IPS-174 On successful completion of the FSA, ownership and responsibility of the following documents are to be handed over to the Customer:

1) All Technical Publications covered by Section 4.10;
2) All Training Materials covered by Section 4.11.5;
3) The Bill Of Materials (BoM) for all nodes and equipment therein, delivered by the Contractor to Customer, inclusive of PFE.

IPS-175 The Contractor shall ensure all documents transferred to the Customer are labellled with the appropriate protective marking.

5 DOCUMENTATION

[140] This Section addresses the documentation requirements of the project. The purpose of these requirements is to ensure that the Contractor develops and provides high quality, comprehensive documentation. This covers all documentation to be provided under the Contract.

DOC-1 The Contractor shall ensure that all project documentation shall be compliant with the requirements identified in the SOW below.

5.1 DOCUMENTATION PLAN

DOC-2 As part of the PIP, the Contractor shall submit a Documentation Plan (DP). The DP shall explain in detail how the Contractor shall fulfil all documentation requirements in this Contract. The DP shall include:

1) List of all documentation deliverables to be provided and defined in this Contract and it's annexes (including SOW, SRS) , in the form of a Contract Data Requirements List (CDRL) and organised according to the Contract Line Item Number (CLIN) structure of the Schedule of Supplies and Services (SSS);
2) Schedule of release of all CDRL items, including draft versions (for review) and final versions (for the purpose of acceptance);
3) Detailed description of the file naming convention in accordance with the requirements in this Section;
4) Detailed description of the document review process in accordance with the requirements in this Section;
5) Detailed description of the change control and version control processes through which the Contractor proposes to manage and control change during the life cycle of each documentation deliverable.

DOC-3 Any deviation from the CDRL shall be coordinated with and requires approval by the Purchaser.

DOC-4 Should it be found that there are documentation requirements within the SOW and Annexes, that are not identified in the CDRL, the CDRL shall be updated to reflect this.

5.2 DOCUMENTATION FORMAT

DOC-5 The Contractor shall ensure that non-COTS documentation shall neither be marked with corporate logos nor contain warnings limiting the rights to use or reproduction.

DOC-6 The Purchaser reserves the right to make additional copies of any documentation (including the training documentation) provided under this Contract for their internal use.

DOC-7 All contractual documentation (e.g., change proposals, invoices, etc.) shall be delivered by the Contractor in electronic format unless specified otherwise by the Purchaser Contracting Officer. The Purchaser reserves the right to request printed versions of any project documentation.

DOC-8 Every document shall include a hyperlinked index.

DOC-9 The Contractor shall ensure that the default software packages for managing projects and processing documentation deliverables are the versions which will be decided at Contract Award by the Purchaser:

1) Microsoft Office Professional;

2) Microsoft Project;

3) Microsoft Visio Enterprise.

DOC-10 The Contractor shall submit documentation, intended for review by the Purchaser in electronic format:

1) In the native format compatible with the Purchaser's software packages above; or

2) All project management documentation (e.g., plans, schedules, reports, etc.) shall be delivered by the Contractor as electronic, editable copies in MS Office format. This format shall be agreed with the Purchaser.

DOC-11 The Contractor shall submit documentation, intended for review by the Purchaser, with each modification identified through the change tracking feature.

DOC-12 The Contractor shall submit all final and accepted versions of documentation deliverables in electronic format, as PDF with Optical Character Recognition enabled (OCR), accompanied with a Microsoft Office version for editing purposes.

DOC-13 The Contractor shall ensure that all documents produced under this Contract shall use sans-serif fonts (e.g. Arial, Helvetica, Calibri, etc.), and obey the following principles:

1) Headings shall be numbered and use bold font-types of sizes higher than the body text (the higher the Heading in the document hierarchy, the larger the font-sizes);

2) No document shall use Headings below level 6 (i.e. 1.1.1.2.3.1 Heading Text);

3) Body text (under the headings) shall not use fonts smaller than Arial 10 pt. (or equivalent size if another font type(s) is (are) selected);

4) Any graphic material generated under this Contract, including network diagrams, shall not use font sizes smaller than Arial 8 (or equivalent size if another font type(s) is (are) selected).

DOC-14 Larger font sizes other than those specified above shall be selected if the corresponding text or drawing is to be reduced in size when embedded in the document, in order to guarantee that the PDF output keeps the font s ise as specified.

DOC-15 Every page shall include a header and footer indicating the highest classification of content in that document using one of the following labels: NATO CONFID*NTIAL, NATO R*STRICT*D (sensitive information identifying e.g. a named location or security assessment), or NATO UNCLASSIFIED.

DOC-16 The Contractor shall ensure that all documentation produced under this contract shall adhere to the same presentation style (cover pages, approval pages, headers, footers, headings and paragraphs, font types and s ises within headings and paragraphs), irrespective of the source of the document within the Contractor's team, including any except COTS equipment documentation.

DOC-17 The Contractor shall ensure that one set of printed System Administrator Guides (SAG) printed on water-proofed paper shall be delivered for each Node and these shall contain any deployment aspects for the Node and Trailer. In addition, all COTS Documentation, manuals and drawings shall be provided in electronical format, both in PDF (OCR) format and, for non-COTS documentation, in an editable Microsoft Office/Visio format.

DOC-18 The Contractor shall ensure that Manuals shall take into consideration the information gained through the Training Needs Analysis (TNA) to ensure that all operation and maintenance tasks are identified and covered by the documentation.

DOC-19 Manuals and As-built drawings shall be provided for all CIS-components, CIS ancillaries and software, such as tents, power distribution, HVAC, BC filters, compressors, and generators, but NOT on PFE (crypto equipment, general use software, etc.). Manuals on PFE will be delivered as PFE manuals together with the PFE. However, manuals and drawings shall cover all the system specific interfaces to/from PFE or any external asset.

DOC-20 All electronic copies shall be delivered in a format which is best suited for review and maintenance by the Purchaser (e.g., Project Master Schedule in MS Project format, Project Progress Reports in MS Word). In general the following guidelines shall be used:

1) Microsoft Word shall be used for generating text document;
2) Microsoft Excel shall be used for tabular or matrix data;
3) Microsoft Visio shall be used for drawings;
4) Microsoft Project shall be used for schedule;
5) Microsoft PowerPoint shall be used for briefings;
6) The rest of deliverables will be furnished as electronic copy of the agreed tools/media used.

DOC-21 All documentation, such as COTS documentation, manuals, drawings and training materials shall be provided in English.

DOC-22 The Contractor shall ensure that documentation convention follows:

1) For numbers appearing in textual documents shall be a comma to be the thousands separator and a period to be the decimal separator (e.g., 1,365,276.24).
2) That dates appearing in free text (e.g., quoting dates of meetings) shall be day-month-year and not month-day-year.
3) The first page shall show the document title, project title, contract number as well as version number and issue date, if applicable, and which shall also be shown on each subsequent page bottom.
4) Developed documentation shall contain a Table of Contents. It shall be noted that depending on the type of document, a Table of Content might not be required. This shall be agreed between the Purchaser and Contractor beforehand.
5) Documents shall contain a preface, containing details of related documents and information on how to navigate the document.
6) Where documents contain many complex special ised or strongly domain oriented terminologies these shall be defined in a glossary.

DOC-23 Each document shall contain the following information for identification:

1) Version of the document and version history;
2) Due date;
3) Delivery date;
4) CLIN number;
5) Status (e.g., accepted/approved/draft).

DOC-24 The Contractor shall remain responsible for updating the documentation that is affected by the changes in the system requirements, design, or support arrangements throughout the project.

DOC-25 The Contractor shall use filenames for all documentation deliverables in compliance with the following filename convention:

a. [NU|NR]_[Contract number]_[Contract Line Item number]_[Name of deliverable.[filename extension]

DOC-26 Example of a compliant filename:

a. NU_CO-14760-TDCIS_3.2.1_QA Plan.pdf.

DOC-27 The fields used in the filename convention shall be used as follows:

1) [NU|NR] is the classification of the document: NATO Unclassified or NATO Restricted;
2) [Contract number] is the official Purchaser contract number “CO-14760-TDCIS”;
3) [Contract Line Item number] is the CLIN used to identify the deliverable in the Schedule of Supplies and Services (SSS);
4) [Name of deliverable] is the Contractor proposed, Purchaser agreed designation of the deliverable;
5) [filename extension] is the standard filename extension, but “.zip” may be used to aggregate multiple files.

DOC-28 The Contractor shall ensure that COTS documents, such as a vendor supplied user manual, shall retain their original filenames and shall hence not be renamed according to the above filename convention.

5.3 DOCUMENT ACCEPTANCE PROCESS

DOC-29 All documentation shall be subject to Purchaser approval.

DOC-30 Documentation shall be distributed as follows:

1) For all documents unless otherwise instructed: an electronic copy to the Purchaser’s Project Manager;
2) For contractual documents: in addition to one hard copy and an electronic copy to the Purchaser’s Contracting Office;
3) With the exception of contractual documents, an electronic copy to the Collaborative Environment.

Table 5-1 Documentation Review Process

Actors Time	Contractor	Purchaser
T = 0	Submit document to Purchaser	
T + 2 wks		Review & send any comments to Contractor: otherwise document finalised.
T + 4 wks	Update document based on Purchaser comments	
T + 5 wks		Document updates either finalized or if necessary further minor comments returned to Contractor
T + 6 wks	Further updates if required	
T + 7 wks		Accepts minor comments and document accepted and finalised.

DOC-31 "One week" and multiples thereof shall be understood as 5 working days, Monday - Friday. This mainly applies to the period of Purchaser's review of a document, from the time the document is uploaded or delivered by the Contractor and vice versa.

DOC-32 Approval of a document or other deliverable shall not be interpreted to imply any Purchaser endorsement of the content. It shall remain the sole responsibility of the Contractor to meet the full system performance requirements and to prove such performance through the regime of testing and other assurance mechanisms set forth in the Contract and it shall be the sole responsibility of the Contractor to remedy any performance shortfall in the event of any identified deficiency in terms of the contract functional and/or performance requirements. The Contractor’s responsibility in this regard extends beyond FSA through warranty, responsibility for any latent defects.

DOC-33 All the documentation within the scope of this project shall be consistent in terms of content. Any inconsistencies that are detected between documents at any time until the end of this project shall be corrected upon Purchaser notification.

DOC-34 The Contractor shall provide a first draft (version 0.1) of each deliverable for Purchaser review by the date specified in the Schedule of Supplies and Services or as agreed between the Purchaser and Contractor.

DOC-35 The first draft shall be substantially complete and correct, and delivered in accordance with the delivery dates specified in the Work Package and the Schedule of Supplies and Services. To ensure the completeness and correctness, the Contractor shall complete the internal review cycle between the related functions before presenting a version to the Purchaser.

DOC-36 The Purchaser reserves the right to return without review a document that has significant deficiencies.

DOC-37 The Contractor shall not rely on the Purchaser review to fill in deficiencies or obtain missing Purchaser information.

DOC-38 The Contractor shall resubmit the document as a revised draft incorporating the Purchaser’s comments within two weeks after receipt, unless specified differently in the Work Package.

DOC-39 The Purchaser shall provide comments, corrections, and suggested changes to the Contractor within two weeks of receipt, unless specified differently in the Work Package. If the Contractor submits more than one document (or more than 400 pages of content in total) for review at the same time, the Purchaser will reserve the right to extend the review period accordingly.

DOC-40 The Contractor shall provide the Final (version 1.0) document within two weeks of receipt of the Purchaser's comments on the revised draft, unless specified differently in the Work Package.

DOC-41 The Contractor shall include and integrate all document review and acceptance activities in the overall Project Master Schedule (PMS) of the PMP in the PIP.

5.4 DRAWINGS

DOC-42 The Contractor shall provide **Engineering Drawings** of all Computer Aided Design (CAD) drawings employed in the procurement and, or manufacture the following of TDCIS associated items:

1) Equipment and rack mounting brackets;
2) Mechanical equipment interfaces;
3) Proprietary cable sections;
4) Proprietary mechanical cable connections and interfaces.

DOC-43 The Contractor shall provide **As-Built Installation Drawings** that reflect the complete installation conducted by the Contractor for each type of system, they shall comprise:

1) Layout Plans showing the locations of all Contractor installed assets;
2) Cabling Plans showing all Contractor installed cabling, per security classification, clearly identifying the location and labelling of each cable, together with the terminations at both ends and the use of the cable;
3) Rack Layout Plans for all Contractor installed racks;
4) System Configuration Plan showing all installed assets with all their interfaces and interconnections, both internal and external;
5) Cross-referenced and consistent with each other and with any other documents provided under this Contract, such as manuals and training material.
6) Representing technical networking and service configuration diagrams shall use layered views, as follows:
7) One layer shall be created for the physical view, covering hardware, ports and cable-connections and associated identification markings (including also signal flow, electrical power and grounding);
   a. One layer for the logical view, covering VLANs, virtual servers, logical links;
   b. One layer for the addressing and routing information;
   c. Service view schematics.

DOC-44 Technical Installation drawings shall be precise, detailed and scaled drawing in accordance with applicable international norms (i.e. ISO 128, ISO 129, ISO 5455, inter alia).

DOC-45 The technical drawings shall include elevations, plans, sections and 3D views. Dimensions and identification of most significant features are mandatory, and shall:

1) Provide the necessary drawings/schematics, specifications, wiring diagrams, etc., to allow the operators to troubleshoot, and fully understand, the design and operation of the particular equipment;

2) Supplement but do not substitute User Manuals and/or Maintenance Manuals and thus be expected to be referenced in the latter as a way of providing specific details on a particular piece of equipment.

6 CONFIGURATION MANAGEMENT

[141] This Section addresses the Configuration Management (CM) requirements of the project. The purpose of these requirements is to ensure that the Contractor establishes and executes NATO-compliant and effective configuration management during the execution of the project until the end of Warranty.

CMG-1 The Contractor shall establish and maintain an effective Configuration Management (CM) organization to implement the CM program and manage the CM functions (configuration identification and documentation, configuration control, configuration status accounting, configuration audits) throughout the duration of the Contract.

CMG-2 The Contractor shall establish and maintain the CM policies, processes and practices/procedures in conformance with [STANAG 4427 Ed.3] “Configuration Management in System Life Cycle Management” and underpinning ACMPs (ACMP-2000, ACMP-2009, ACMP-2100) and [ISO 10007:2017] “Quality Management System – Guidelines for Configuration Management”.

CMG-3 The Contractor shall implement the CM activities for any HardWare (HW), SoftWare (SW) including FirmWare (FW) delivered, integrated, tested and/or customized and document provided, used or defined in the frame of the project and shall fully integrate the COTS elements-data in order to implement a unique CM framework.

CMG-4 The Contractor shall provide the required CM deliveries in accordance with the following schedule that shall be included in the contractor’s Project Master Schedule (PMS) of the PMP in the PIP

Table 6-1 IPS Deliverables

Title	Iss	Due date
Configuration Management Plan (CMP)	Draft	EDC + 2w
	Final Draft	PDR - 4w
	Final	CDR + 4w
Functional Baseline (FBL)	Draft	SRR – 4w
	Final	SRR + 4w
Allocated Baseline (ABL)	Draft	PDR – 4w
	Final	CDR - 4w
Product Baseline (PBL)	Draft	CDR + 4w
	Final	FAT - 4w
Operational Baseline (OBL)	Draft	FSA – 4w
	Final	FSA + 4w
Configuration Management Database (CMDB)	Draft	Design review – 4w
	Final	Design review + 4w
FCA Report		SAT + 4w
PCA Report		FAT + 4w

6.1 CONFIGURATION MANAGEMENT PLAN

CMG-5 The Contractor shall provide, execute, and maintain an effective Configuration Management Plan (CMP) as a living document throughout the duration of the Contract. The Contractor shall organize review meetings for CM progress starting from the first draft of CMP.

CMG-6 The CMP shall identify, document and justify the organizational structure, roles and responsibilities, tasks, milestones and procedures to be used by the Contractor to implement the CMP and fulfil the requirements of this Contract.

CMG-7 The CMP shall assure the establishment and maintenance of configuration item records, configuration item life cycle records, and baselines throughout the duration of the contract and provide assurance that all changes to the baselines are performed through a formal change control process once a baseline has been established and agreed.

CMG-8 The CMP shall be structured following the requirements set in the [ACMP-2009-SRD-40.1 ref. # 4.3.C] and subject to revisions and updates, as required.

CMG-9 The Contractor shall provide in the CMP the rationale and criteria for the CI identification and CI numbering for the Purchaser approval, based on the criteria for selection of CIs detailed in [NATO ACMP 2009, 2017] “Guidance on Configuration Management”.

6.2 CONFIGURATION IDENTIFICATION

6.2.1 ITEM IDENTIFICATION

CMG-10 The Contractor shall identify and describe HW, SW (including FW) and documentation Configuration Items (CI’s) as defined in [NATO ACMP 2009, 2017].

CMG-11 The Contractor shall also identify any PFEs and PFSs provided for implementation as Configuration Items (CI’s) and integrate them within their CM and related part of the CI structure.

6.2.2 BASELINES

[142] The Purchaser reserves the right to modify the CI structure prior to its baselining.

CMG-12 The Contractor shall define the CI trees (Baselines), hierarchically structured, clearly defining each node/leaf as Configuration Item (CI), Hardware Configuration Item (HWCI), Computer Software Configuration item (CSCI), Hardware Parts (HWP) or Computer Software Component (CSC) in accordance with the guidelines provided in the above defined ACMPs and ISO.

CMG-13 The Contractor shall provide and maintain Baselines throughout the duration of the Contract.

CMG-14 The Contractor shall provide the following baselines:

1) Functional Baseline (FBL);
2) Allocated Baseline (ABL);
3) Product Baseline (PBL); and
4) Operational Baseline (OBL).

CMG-15 The Contractor shall be responsible for the consistency between the baselines throughout the project. Any update or change shall be introduced formally and revision controlled.

CMG-16 The Contractor shall develop, maintain and fully document all the baselines in the Contractor's Product Lifecycle Management (PLM) tool.

CMG-17 The Contractor shall export the baselines in the form of CMDBs for each Baseline and relevant modifications, in accordance with the Change Request (CR), Engineering Change Proposal (ECP) and Engineering Change Order (ECO) processes, covering as a minimum the following relationships:

1) Contract functional/non-functional requirements to Functional elements of the FBL;

2) Functional Elements of the FBL to Major CIs of the ABL;

3) Major CIs of the ABL to Full CIs (CIs, HWCIs, CSCIs, HWPs, CSCs) tree (PBL); and

4) Major CIs of the PBL to Services/Sub-Services delivered by the System (mapping of CIs vs Services and vice versa).

CMG-18 The Contractor shall incorporate in the baselines, under a unique hierarchical tree, all the information relevant to the OEMs/COTS HW, SW and FW used and integrated in the System including PFEs and PFSs.

6.2.2.1 FUNCTIONAL BASELINE

[143] The Functional Baseline (FBL) is a set of documents that specifies the functional and non-functional requirements of a service or product and that is used as the approved basis for comparison.

CMG-19 The Contractor shall provide the final version of the FBL for Purchaser approval following the approval of Final SRR Report. Any changes on the approved FBL shall be requested through ECP.

CMG-20 The Contractor's design in the FBL shall be derived from the SRS.

CMG-21 The Contractor shall use an industry recognised requirements management tool to support requirements management.

CMG-22 The Contractor shall provide access to the Requirements Management tool if requested by Purchaser to have an overview of the requirements management system of the Contractor.

CMG-23 The Contractor shall provide the exported requirements lists from the Requirements Management tool in FBL documentation.

CMG-24 The Contractor shall propose the format of FBL in the CMP for Purchaser's approval.

6.2.2.2 ALLOCATED BASELINE

[144] The Allocated Baseline (ABL) is a set of documents that specifies the design of a service or product and is used as the approved basis for comparison. The ABL starts to be developed at the beginning of the design phase (PDR) and it is established and “frozen” at the end of the design phase (at CDR) - it is also known as “as-designed” baseline.

CMG-25 The Contractor's design in the ABL shall meet the functional and non-functional requirements allocated in the FBL.

CMG-26 The Contractor shall provide ABL, with incremental contents, using the NCI Agency template [AI 16.32.04] - ABL Template

6.2.2.3 PRODUCT BASELINE

[145] The Product Baseline (PBL) is a set of products and/or services, including supporting documents, which is used as the approved basis for comparison. The PBL starts to be developed at the beginning of the production phase. It is established and "frozen" at the end of the production phase (at factory integration/test) - it is also known as "as-built" baseline.

CMG-27 The Contractor's design in the PBL shall meet the functional and non-functional requirements allocated in the FBL and the design of the ABL.

CMG-28 The Contractor shall provide PBL, with incremental contents, using the NCI Agency template [AI 16.32.05] - PBL Template

CMG-29 Each element of the PBL shall include as minimum (but not be limited to) the following pieces of information (in accordance with the type of item):

1) Position in the structure (hierarchical level or indenture code);
2) Physical location (Reference Designator or similar positional code) coherent with the As-Built Drawings and manuals;
3) Type of Configuration Item (CI, HWCI, CSCI, HWP, CSC);
4) Type of MRI/MSI, coherent with the LBS/PBS;
5) Item identifiers (Part Number – P/N, Cage Code, Nomenclature, revision/issue, release etc.) coherent with the Contractor's defined CM numbering system, including OEMs/COTS data and their propagation in the CM tree;
6) Asset Data (SMR Code, Price, Price UOM, MOQ, start of warranty/licence validity etc.);
7) Inventory Data (Serial Number - S/N or Licence number if applicable etc.);
8) CI documentation:
    a. For HWCIs/HWPs: specifications, datasheet, Certificates of Conformity (CoC), Declaration of Conformity (DoC), Items Setting Documents (ISD – how to configure hardware, software and firmware) etc.;
    b. For HWCIs/CIs: interconnection diagrams, interface specifications/control documents, test procedures, test records, integration data, customization/setting procedures etc.; and
    c. For CSCIs/CSCs: software Release Notes (SRN), software test data records, software metrics (type of language, Line of Code, number of function points etc.), software Source Code (if specifically generated or modified/adapted/customised in the frame of the project), software Installation files, software Version Description Documents (VDDs), software installation/customization procedures, software settings, software operating manual etc..
    d. Alternative (P/N, Cage Code, Nomenclature, revision/issue, release etc.); and

e. NATO Stock Number (NSN).

CMG-30 The Contractor shall provide the CMDB to reflect the PBL with all related documentation, software, hardware, configuration files, services and any other related information or deliverable necessary to establish the PBL completely.

6.2.2.4 Operational Baseline

CMG-31 The Contractor's developed Operational Baseline (OBL) shall be initially established after successful completion of the PSA and then finally established after successful completion of FSA. It reflects the "as-deployed" ("as-delivered") configuration of the system.

CMG-32 The Contractor shall provide the CMDB to reflect the OBL upon completion of FSA.

6.3 Change Control

CMG-33 The Contractor shall be fully responsible for the Configuration Change Control of all CI's and baselines throughout the duration of the Contract and in accordance with [NATO ACMP 2009, 2017].

CMG-34 The Contractor shall be responsible for issuing in a timely manner, as required by this SOW, all approved changes and revisions to all baseline documents included in the Contract. This includes changes originated both by the Contractor and the Purchaser.

CMG-35 The Contractor shall ensure that the change is properly reflected in all baseline documents affected by that change where a change affects more than one document, or affects documents previously approved and delivered.

CMG-36 The Contractor shall define the Configuration Baseline Change procedures and shall submit Notice of Revision or Requests for Concession when required and approved by the Purchaser. All proposed changes to the baselines (FBL, ABL, PBL, OBL) shall be submitted to the contractor's Configuration Control Board (CCB) prior to the submission to the Purchaser for approval. The Contractor's internal CCB process shall be defined in the CM Plan. Additionally, the Contractor shall propose an external CCB process to communicate and discuss the changes with Purchaser before officially presenting the changes for approval.

CMG-37 The Contractor shall submit change requests in the form of Engineering Change Proposals (ECP) or Request for Deviations/Waivers (RFD/W), when required. All requests shall be captured and logged in a change request register to be identified in CMP. Forms based on ACMP requirements designed by the Contractor for this purpose shall be submitted for approval by the Purchaser prior to use.

CMG-38 The Contractor shall use the instructions and templates provided by the purchaser to issue any ECPs and RFD/Ws in accordance with the following:

- [AI 16.32.02] – Preparation of ECP forms and relevant annex; and
- [AI 16.32.03] – Preparation of RFD/W forms and relevant annex.

6.3.1 Engineering Change Proposals

CMG-39 The Contractor shall assign a priority rating of Emergency, Urgent or Routine Extensions to the target times for processing when submitting ECPs. Changes to the Contractor's baselined Cis shall be processed as:

1) Class I ECPs: these shall have to be mutually agreed upon by the Contractor and Purchaser. Extensions to the target times for processing Class I ECPs shall be mutually agreed upon by the Contractor and Purchaser.
2) Class II ECPs: these shall be submitted by the Contractor to the Purchaser for review and classification concurrence prior to implementation.

CMG-40 If the Purchaser's representative does not concur in the classification, Class I ECP procedures shall be applied by the Contractor and the ECP and then formally submitted to the Purchaser for approval or rejection.

CMG-41 Any ECP shall include, as a minimum, the following information:

1) Reference Number;
2) requirement affected;
3) nature of change;
4) rationale for the change;
5) impact of change / CIs affected;
6) Description of how the change will be reflected in the delivered system's cost, schedule, and/or performance. This description shall include any trade-offs that shall be considered;
7) Status; and
8) Priority.

CMG-42 All design changes shall be appropriately reflected in the technical documentation by the issue of appropriate changes or revisions. Changes/revisions shall be provided for consideration and approval to the Purchaser by the Contractor in accordance with ECP procedures.

CMG-43 Any ECP affecting FBL shall be submitted by the Contractor to the Purchaser for review, classification concurrence and approval. No Class I ECP affecting the FBL, including a change to a baseline document shall be implemented until it has been approved by the Purchaser.

6.3.2 Request for Deviations/Waivers

CMG-44 If required, the Contractor shall prepare, handle, and submit for Purchaser's approval, Request for Deviations/Waivers (RFD/W).

CMG-45 The Contractor shall be aware that permanent departures from a baseline shall be accomplished by ECP action rather than by RFD/W.

6.3.3 Deficiency Reports

CMG-46 The Contractor shall establish and maintain a process for reporting, tracking, and resolving deficiencies in the relevant Baselines. Deficiency Reports (DRs) shall document problems during the design, configuration, implementation, or operation of the system.

CMG-47 DRs shall be closed when the identified problem is resolved through procedure or other action that does not affect the system baselines, or when a corresponding Change Request is opened to correct the deficiency through a change to a baseline.

CMG-48 The **Deficiency Report** shall contain the following information:

1) A serial number for each deficiency;

2) Description of the deficiency;

3) Test and test case or event under which the deficiency was first observed (e.g.: FAT);

4) Date of the observation of the deficiency and expected date of its correction;

5) The personnel raising and endorsing the observation;

6) Any clearance action taken such as repair and testing, notification, receipt of a written reply from the Contractor;

7) The authorized personnel endorsing the correction, and the date of correction;

8) The Contractor's proposed way forward, in case the deficiency remains, with target dates and description of the intended resolution strategy.

CMG-49 The Deficiency Log shall be first created at the time of First Article Acceptance Testing, and shall remain updated at PSA and then until FSA.

CMG-50 It shall be noted that during testing or other inspection procedures, the Purchaser may observe perceived deficiencies. These Purchaser observations shall be included in the Contractor's Deficiency Log, and appropriately documented.

CMG-51 The Contractor shall include and provide its Deficiency Report data as part of the Configuration Management Database (CMDB) throughout the duration of the Contract.

6.4 CONFIGURATION STATUS ACCOUNTING

CMG-52 The Contractor shall be fully responsible for the Configuration Status Accounting (CSA) for all baselines and CIs throughout the duration of the Contract and in accordance with [NATO ACMP 2009, 2017].

CMG-53 The Contractor shall propose the format of CSA Report in the CMP for Purchaser's approval.

CMG-54 The Contractor shall include and provide its CSA data as part of the Configuration Management Database (CMDB) throughout the duration of the Contract.

6.5 CONFIGURATION AUDITING

6.5.1 FUNCTIONAL CONFIGURATION AUDITS (FCA)

[146] Functional Configuration Audit (FCA): this is a formal examination to verify that a configuration item has achieved the functional and performance characteristics specified in its product configuration information. It is the Purchaser's formal audit of the equipment performance with regard to the contract's specifications

CMG-55 The Contractor shall organize and support at least one Functional Configuration Audit (FCA), to occur between FDR and the PSA.

CMG-56 The FCA shall be conducted upon the delivery of the first of each configuration type to be delivered by the Contractor.

CMG-57 The Contractor shall provide the Purchaser with all baseline documentation required to perform the FCA. At each audit, the Contractor shall make available the technical personnel capable of answering questions from the Purchaser's auditor.

CMG-58 The Contractor shall demonstrate by means of the system design and test documentation that each of the technical requirements have been satisfied.

CMG-59 The Contractor shall demonstrate, before each testing activity and after the changes based on the tests, the configuration documented is the same with the configuration installed in the physical system. This shall entail the demonstration of HW and SW/FW configuration.

CMG-60 The Contractor shall undergo the FCA not later than 2 weeks after successful SAT. The outcome of the FCA shall be documented in the FCA report, to be delivered not later than 4 weeks after successful SAT.

6.5.2 PHYSICAL CONFIGURATION AUDITS (PCA)

[147] Physical Configuration Audit (PCA): this is a formal examination to verify that a configuration item has achieved the physical characteristics specified in its product configuration information.

CMG-61 The Contractor shall organize and execute Physical Configuration Audits (PCA) on site at each location, to occur before PSA. The PCA shall be witnessed by the Purchaser.

CMG-62 The PCA shall include:

1) A full inventory check of all equipment ,software and documentation delivered on site, including auditing of equipment and cable labelling and marking, safety marking and warnings, part numbers and serial numbers;
2) Verification of manuals and training material to assess consistency between documentation and equipment and software found on site;
3) Verification of design configuration specification against equipment and software found on site; and
4) Verification of all change requests against equipment and software found on site.

CMG-63 The Contractor shall provide the Purchaser with all baseline documentation required to perform the PCA. At each audit, the Contractor shall make available the technical personnel capable of answering questions from the Purchaser’s auditor.

CMG-64 The Contractor shall solve any deficiencies found during a PCA within the agreed timeframe and update the baseline accordingly.

CMG-65 The Contractor shall undergo the PCA not later than 2 weeks after successful FAT. The outcome of each PCA shall be documented in the PCA report, to be delivered not later than 4 weeks after successful FAT.

CMG-66 The Contractor shall draft and deliver a PCA Report after each PCA, summarizing the results of the audit and for the Purchaser’s approval not later than two weeks after the PCA.

6.6 CONFIGURATION MANAGEMENT DATABASE

CMG-67 The Contractor shall employ a Configuration Management System (CMS) incorporating the Configuration Management Database (CMDB).

CMG-68 The Contractor shall allow the Purchaser access to its CMDB and to the status of all baselines, Configuration Items, Configuration Item Records and Change Records at all times during the execution of the contract.

CMG-69 The Contractor shall deliver a fully populated CMDB to the Purchaser before each design review and before PSA and FSA. The CMDB shall be in a non-proprietary format, unless otherwise stated by the Purchaser, and free of any use restrictions to the Purchaser.

CMG-70 The Contractor shall provide its entire CMDB file set for Purchaser to be able to import to its CMDB tools and databases products if requested by the Contractor.

CMG-71 The Contractor shall ensure that the CMDB can manage Configuration Items that are operational and Configuration Items that are non-operational or in development (i.e.: OBL vs. PBL, respectively).

7 QUALITY ASSURANCE AND CONTROL

7.1 OVERVIEW

[148] This Section addresses the Quality Assurance (QA) and Quality Control (QC) requirements of the project. The purpose of these requirements is to ensure that the Supplier provides all deliverables on time and at the required level of quality by utilising a professional, best practice quality assurance framework and through internal quality control independent from the Supplier’s project organisation. A second objective is to minimise the duration of the review cycles and decrease the review workload by ensuring that the Supplier provides mature deliverables only.

[149] Quality Assurance (QA) is a process and set of procedures intended to ensure that a product or service, during its definition, design, development, test and deployment phases will meet specified requirements.

[150] Quality Control (QC) is a process and set of procedures intended to ensure that a manufactured product or performed service adheres to a defined set of quality criteria and meets the requirements of the customer.

[151] Under this contract the “QA process” is intended as Quality Assurance and Control Process. The term Quality Assurance will include also the Quality Control process.

[152] The Purchaser reserves the right to perform Reviews and Quality audits at any of the Contractor (or Sub-Contractor(s)) facilities. Audit activities at Sub-Contractor’s facilities do not relieve the Contractor and Sub-Contractor from any contractual quality responsibilities.

[153] Unless otherwise specified in the SOW, STANAG 4107 and underpinning AQAPs, ISO 9000:2015, PRINCE2 and ITIL definitions shall apply.

[154] A “Project document” is a document developed and maintained to help in the management of the project. Typically the plans (amongst which, the Quality Assurance Plan (QAP)) are project documents.

[155] The term "NATO Quality Assurance Representative" (NQAR) shall apply to any of the Purchaser appointed Quality Assurance Representative.

[156] The term "Contractor Quality Assurance Representative" (CQAR) shall apply to any of the Contractor appointed Quality Assurance Representative.

QAP-1 The Contractor’s shall comply to its internal Quality Assurance process and systems with STANAG 4107 “Mutual Acceptance of Government Quality Assurance and usage of the Allied Quality Assurance Publications (AQAP)”.

QAP-2 If any sub-contracted quality resources are used, the Contractor’s Quality Assurance Process shall describe the controls and processes in place for monitoring the sub-Contractor’s work against agreed timelines and levels of quality.

QAP-3 The Contractor shall transfer to the Purchaser’s auditors all information deemed necessary to perform the activities, on his own initiative or on request by Purchaser’s auditors.

QAP-4 A non-exhaustive list of information that the Contractor shall transfer to the Purchaser’s auditors includes minutes of meetings, planning documents, source code, requirements documents, and database, design, test and other technical documentation.

QAP-5 Based on the Audit results if there are any disconformities or irregularities with the contract requirements, The Contractor shall immediately make necessary corrections and take necessary precautions to ensure the satisfaction of the requirements.

QAP-6 The Contractor shall ensure that all QA activities and milestones are identified and included in the Project Master Schedule (PMS) of the PIP.

QAP-7 The Contractor shall establish, execute, document and maintain an effective Quality Assurance (QA) programme throughout the Contract's lifetime.

QAP-8 QA programme shall apply both the contractual requirements and the NATO requirements for quality identified by AQAP 2110, AQAP 2210 and AQAP 2310 and AQAP 2105, to provide confidence in the Contractor's ability to deliver products that conform to the Contractual requirements.

QAP-9 If any inconsistency exists between the SOW requirements and the references, the SOW requirements shall prevail.

QAP-10 The Contractor‘s QA effort shall apply to all services and products (both management and specialist) to be provided under the Contract. This includes all hardware, software, firmware and documentation being developed, designed, acquired, integrated, maintained, or used under the Contract (including deliverable and non-deliverable items like test and support hardware and software), without limitation.

QAP-11 The Contractor‘s QA efforts shall ensure that procedures are developed, implemented and maintained to adequately control the design, development, production, purchasing, installation, inspection, testing, configuration management and customer support of all services and all products, in accordance with the requirements of this Contract.

7.2 Roles and Responsibilities

[157] During the entire Contract implementation, the NQAR(s) assures the Contractor's and Sub-Contractor's compliance with all Quality related contractual requirements. The Purchaser, through its NQAR(s), is the authority concerning all Quality related matters.

QAP-12 The Contractor shall be responsible for assurance and control of quality for all deliverables and associated Contractual products, processes and services through the life-cycle of the Contract.

QAP-13 The CQAR shall be accountable for the provision of the QA Plan and the compliance to the defined QA process.

QAP-14 The CQAR(s) shall define the major quality checkpoints that will be implemented while executing the project and the quality process to be used at each checkpoint.

QAP-15 The CQAR(s) shall be responsible for assessing that the Contractual requirements have been complied with, prior proposing the Contractual services and products.

QAP-16 The CQAR shall report to a distinct manager within the Contractor's organisation at a level equivalent to or higher than the Project Manager.

QAP-17 The CQAR shall be the point of contact for interface with and resolution of quality matters raised by the NCI Agency or its delegated NQAR.

QAP-18 The Contractor shall support any NCI Agency or its delegated NQAR activity focused on monitoring Contractor activities at Contractor's facilities or other sites related to the development, testing and implementation. In particular, the Contractor shall; a) Make himself/herself available to answer questions and provide information related to the project, b) Allow the Purchaser representatives to inspect and monitor testing activities, and management, technical and quality processes applicable to the project, and c) Transfer to the Purchaser representatives all information deemed necessary to perform the QA activities, on his/her own initiative or on request by the Purchaser representative.

QAP-19 The Contractor shall ensure that CQAR(s) have the required qualifications, knowledge, skills, ability, practical experience and training for performing their tasks.

QAP-20 The CQAR(s) shall have sufficient responsibility, resources, authority and independence to review and evaluate activities, identify problems and initiate or recommend appropriate corrective actions.

QAP-21 The CQAR(s) shall participate in the early planning and development stages to ensure that all quality related requirements are specified in plans, standards, specifications and documentation.

QAP-22 After establishment of attributes, controls and procedures, the CQAR(s) shall ensure that all elements of the QA Process are properly executed, including inspections, tests, analysis, reviews and audits.

QAP-23 The Contractor, through its CQAR(s), shall be responsible for product quality control and for submitting to Purchaser acceptance products, supplies and services which conform to contractual requirements only.

QAP-24 The Contractor shall maintain and, when required, deliver objective evidence of this conformance.

QAP-25 The Contractor shall give written notice to the NQAR(s) at least four weeks in advance that the services and/or products are being presented for review, testing, verification, validation and acceptance.

QAP-26 Testing shall only be permitted by using test procedures and plans approved by the Purchaser.

7.3 QUALITY MANAGEMENT SYSTEM (QMS)

QAP-27 The Contractor shall establish, document and maintain a Quality Management System in accordance with the requirements of ISO 9001:2015.

QAP-28 The Contractor’s and Sub-Contractor’s QMS relevant to performance under the Contract shall be subject to continuous review and surveillance by the cognizant NQAR(s).

QAP-29 The Contractor shall include in orders placed with its Sub-Contractor(s) and Supplier(s), the QMS requirements necessary to ensure the supplies and services covered by the Sub-Contract(s) and/or Purchase Orders conform to the requirements of the prime Contract.

QAP-30 The Contractor shall specify in each order placed with its Sub-Contractor(s) and Supplier(s), the Purchaser's and its NQAR(s) rights of access to all premises where contractual work is performed, in order to carry out audits, inspections, tests and other functions as may be required by the NQAR(s).

QAP-31 If sub-contracted quality resources are used, the Contractor's Quality Management process shall describe the controls and processes in place for monitoring the Sub-Contractor's work against agreed timelines and levels of quality.

7.4 QUALITY ASSURANCE PLAN

QAP-32 The Contractor shall establish, execute, and maintain as a living document an effective Quality Assurance Plan (QAP) throughout the period of performance of this Contract. The Contractor's QA Process shall be described in the QA Plan. The process is subject to approval by the Purchaser, or its delegated representative (NQARs), whenever it does not meet the Quality Assurance requirements that are stated in this contract.

QAP-33 The Contractor shall provide the QAP for review to the Purchaser in accordance with the requirements identified in the AQAP-2105 and the SOW requirements.

QAP-34 The acceptance of the QAP by the Purchaser only means that the Purchaser agrees to the Contractor's approach in meeting the requirements. This acceptance in no way relieves the Contractor from its responsibilities to meet the requirements stated in this Contract.

QAP-35 The Contractor shall organise QA Review meetings starting from the first draft of QAP.

QAP-36 The Contractor shall review his QA programme periodically and audit it for adequacy, compliance and effectiveness.

QAP-37 The Contractor shall ensure that all contractual requirements, including NATO supplements, are included in internal audits.

QAP-38 The Contractor shall inform the NQAR(s) of deficiencies identified during internal audit unless otherwise agreed between the NQAR and/or the Purchaser and the Contractor.

QAP-39 The Contractor shall maintain a QA Logbook during the lifetime of the project in which records are kept accounting for all QA-activities, most notably all QA reviews. All accounting shall be done through dating and sign off by the responsible QA person. The QA Logbook shall enable the Purchaser to verify if and when a deliverable has been QA reviewed and by whom and with what result.

QAP-40 The Contractor shall establish and maintain an effective QA organisation to implement the QAP and manage the QA independently of the management of the project.

QAP-41 The Contractor's designated Quality Assurance Manager shall ensure that all required roles, responsibilities, processes and control mechanisms are identified and implemented to make sure that all the functional, non-functional requirements within the scope of the contract are analyzed, planned and satisfied.

QAP-42 The QAP shall describe the Contractor's QA organisation, QA programme, roles and responsibilities and procedures to ensure that all activities are performed in accordance with the requirements of this Contract.

QAP-43 The QAP shall reference or document and explain the Contractor's QA procedures for analysis, software support, development, design, production, installation, configuration management, control of Purchaser furnished property, documentation, records, programming standards and coding conventions, library controls, reviews and audits, testing, corrective action and certification as specifically related to this project.

QAP-44 The QAP shall apply to all hardware, software, documentation, activities, services and supplies that are designed, developed, acquired, maintained or used, including deliverable and non-deliverable items.

QAP-45 The QAP shall also ensure that the exchange of deliverables from the Supplier to the Purchaser shall be adequately controlled, and that no deliverables shall be presented by the Supplier without adequate quality control and sign-off by the Supplier's QA Manager.

QAP-46 The QAP shall be compatible and consistent with all other plans, specifications, standards, documents and schedules, which are utilized under this Contract.

QAP-47 All Contractor's procedures referenced in the QA Plan shall either be submitted with the plan, or described in the plan and made available for review by the Purchaser upon demand.

QAP-48 The QAP and all related QA procedures, and all their versions/revisions, shall be subject to the Purchaser approval based on an agreed checklist.

QAP-49 The Contractor shall include a risk management section within the QAP including the risks connected to the sub-Contractors of the Contractor.

QAP-50 The Contractor shall maintain a QA log during the lifetime of the project in which records are kept accounting for all QA-activities, most notably all QA reviews. All accounting shall be done through dating and sign off by the responsible QA person. The QA log shall enable the Purchaser to verify if and when a deliverable has been QA reviewed and by whom and with what result.

QAP-51 The Contractor shall make its quality records, and those of its Sub-Contractors, available for evaluation by the NQAR(s) throughout the duration of the Contract.

QAP-52 The Contractor shall update the document, as required, from the delivery date of the initial QAP through FSA, under Configuration control. The Contractor shall provide a copy of each new version of the QAP to the Purchaser for review and approval.

7.5 QUALITY ASSURANCE PROCESS

QAP-53 The Quality Assurance (QA) implemented by the Contractor shall apply to all hardware, software (including firmware) and documentation being developed, designed, acquired, integrated, maintained, or used under the Contract. This includes non-deliverable test and support hardware and software.

QAP-54 The Contractor's QA Process shall ensure that procedures are developed, implemented and maintained to adequately control the development, design, production, testing and configuration of all deliverables.

QAP-55 The requirements for these processes shall be derived from the Contract, the QMS, the applicable AQAPs and referenced best practices, in that sequence of priority.

QAP-56 The Contractor shall prepare, perform and document System Requirements Review (SRR), Preliminary Design Review (PDR) and Critical Design Review (CDR) according to the contractual requirements and IEEE 15288.2:2014.

QAP-57 The Contractor shall perform verification and validation of the Contractual deliverables before proposing them for the Purchaser review and approval.

QAP-58 Personnel performing QA functions shall have specific documented definitions of their assigned duties. In no case shall the QA personnel managing or performing

QA functions be the same personnel responsible for performing other tasks that are reviewed by QA.

QAP-59 The Contractor shall demonstrate, with the Quality Assurance process, that the processes set up for design, develop, produce and maintain the product will assure the product will meet all the requirements.

QAP-60 If sub-contracted quality resources are used, the Contractor's Quality Management Process shall describe the controls and processes in place for monitoring the sub-Contractor's work against agreed timelines and levels of quality.

QAP-61 The Contractor shall assure that all the test and procedure used to demonstrate the requirements will be monitored and controlled under the QA process.

QAP-62 The Contractor shall document all the identified risks in accordance with Risk Management.

QAP-63 The Contractor shall periodically review the QA process and audit it for adequacy, compliance and effectiveness, and report any changes to the Purchaser POC.

QAP-64 The Contractor shall on request provide the Purchaser with a copy of any subcontracts or orders for products related to the contract.

QAP-65 The Contractor shall notify Purchaser if a subcontract or order has been identified as constituting or involving risk.

QAP-66 The Contractor shall flow down the applicable contractual requirements to Sub-Contractors by referencing the stated contractual requirement, including relevant AQAP(s).

QAP-67 The Contractor shall be responsible for ensuring that the procedures and processes required to fulfil contract requirements are fully implemented at the Sub-Contractor's facilities.

QAP-68 The Contractor shall periodically review the QA process and audit it for adequacy, compliance and effectiveness, and report any changes to the Purchaser NQAR(s).

QAP-69 The Contractor shall ensure that all contractual requirements, including NATO supplements, are included in internal audits.

7.6 AUDITING OF CONTRACTOR PERFORMANCE

QAP-70 The Purchaser reserves the right to perform Reviews and Quality audits at any of the Contractor (or Sub-Contractor(s)) facilities.

QAP-71 Audit activities at Sub-supplier's facilities do not relieve the Contractor and Subcontractors from any contractual quality responsibilities.

QAP-72 The Purchaser may engage auditors to evaluate the performance of the Contractor (or Sub-Contractor(s)) and verify, validate Contractor (or Sub-Contractor(s)) deliverables. The auditors can also monitor, assess, and report any perceived problem areas.

QAP-73 The auditors may be requested by the Purchaser to monitor Contractor activities at Contractors' facilities or other sites related to the development, testing and implementation of the contract. The Contractor shall fully support such activities and in particular:

5) Host inspection visits by Purchaser's auditors;

6) Make himself available for answering questions and furnishing all the information related to the project;

7) Allow the Purchaser's auditors to inspect and monitor testing activities; and

8) Allow the Purchaser's auditors to inspect and monitor the Contractor's processes and tools applicable to this project.

QAP-74 The Contractor shall transfer to the Purchaser's auditors all information deemed necessary to perform the activities, on his own initiative or on request by Purchaser's auditors.

QAP-75 A non-exhaustive list of information that the Contractor shall transfer to the Purchaser's auditors includes minutes of meetings, planning documents, source code, requirements documents, and database, design, test and other technical documentation.

QAP-76 Based on the Audit results if there are any disconformities or irregularities with the contract requirements, The Contractor shall immediately make necessary corrections and take necessary precautions to ensure the satisfaction of the requirements.

7.7 QUALITY FOR PROJECT DOCUMENTS

QAP-77 A formal change management process shall be applied to all project documents, including documents naming conventions as defined by the Purchaser and coordinated with the Contractor.

QAP-78 Project documents shall be configuration controlled. Each version of a project document is subject to Purchaser approval (unless otherwise specified).

QAP-79 The Contractor shall ensure that any change related to the project documents are controlled, with the identity, approval status, version and date of issue are clearly identified.

QAP-80 Project documents file names shall not contain any variable part, like version number, reviewer initials or maturity status. Version numbers and maturity status shall be marked in the document content and/or attributes.

7.8 SUPPORTING TOOLS

QAP-81 All tools used by the Contractor in the context of project execution shall be available for demonstration to the Purchaser, upon Purchaser request.

QAP-82 The Contractor shall also make available to the Purchaser for review upon request, associated records and documentation, including but not limited to, control, authorization for use, calibration, validation, qualification, as applicable, per respective Contract requirement.

7.9 CERTIFICATES OF CONFORMITY

[158] A Certificate of Conformity (CoC) is a document, signed by the Supplier, Vendor of the Product or Contractor, stating that the product conforms to contractual requirements and regulations. A Certificate of Conformity template is available in AQAP-2070.

[159] The CoC, provides evidence that the items produced or shipped comply with test procedures and quality specifications prescribed by the customer. It presents data derived from quality management information.

QAP-83 The Contractor shall be solely responsible for the conformance to requirements of products provided to the Purchaser.

QAP-84 The Contractor shall deliver all the Certificates of Conformity (CoCs) for all HW and SW released products, all COTS SW (including firmware) and all HW released by the COTS Vendors.

QAP-85 Any CoC delivered by the Contractor shall be part of the acceptance data package of the product and shall be provided to the Purchaser before the start of any Site Acceptance Tests.

QAP-86 The Contractor shall ensure that as an enabler for CoC, the qualification testing regime includes, as a minimum, the following:

1) TEMPEST Testing;
2) Electro-Magnetic Compatibility (EMC) Testing;
3) General Environmental Testing;
4) Water/Dust Ingress Testing;
5) Operational Robustness Testing;
6) Mechanical Environmental Testing;
7) Environmental Control Testing;
8) Biological & Chemical Testing;
9) Transportation Testing;
10) Physical Functional System Testing;
11) Product Safety Testing;
12) User Interface Testing.

8 TEST, VERIFICATION & VALIDATION

8.1 INTRODUCTION

[160] This Section details the Test, Verification, Validation (TV&V) principles, activities, processes and requirements to be applied and performed under the Contract, which are required for the verification and validation of the requirements set forth under the Contract by the Purchaser.

[161] All Contract-related deliverables supplied by the Contractor will be verified and validated to ensure they meet the requirements of this Contract. Both fitness-for-use and fitness-for-purpose will be assessed using a quality-based approach.

[162] The verification and validation approach will not only involve delivered equipment, but also interfaces and interoperability with existing NATO and/or national equipment, here considered as Purchaser Furnished Equipment (PFE).

[163] The verification and validation of PFE is out of the scope of the Contract.

[164] In this document, the term “deficiency” is considered to be an inadequacy or incompleteness process definition or execution, while the term “defect” is an error, a fault or a malfunction inside a Configuration Item.

[165] Requirements verification methods, as defined in ISO/IEC/IEEE 29148, will be used in order to obtain evidence(s) that requirements have been fulfilled.

[166] The project requires a set of TV&V activities to verify its compliance with the Contractual requirements set forth in the SOW and in the SRS (Annex to the SOW).

8.2 TEST, VERIFICATION & VALIDATION ACTIVITIES

TVV-1. For each requirement, the Contractor shall select a verification method, which shall be approved by the Purchaser.

TVV-2. All information items used during the verification and validation activities are to be handled according to their security classification. Guidance is provided in this SoW, under the security Section.

TVV-3. The Contractor shall have the overall responsibility for meeting the TV&V requirements and conducting all related activities. This includes the development of all TV&V documentation required under the Contract, the conduct of all independent verification, validation and assurance events, and the evaluation and documentation of the results.

TVV-4. All deliverables supplied by the Contractor under the Contract shall be verified and validated to meet the requirements of this contract.

TVV-5. All document-based deliverables shall be produced in a manner compliant with the templates provided by the Purchaser.

TVV-6. In particular the Contractor shall:

1) Perform the verification activities within each iteration and for each target environment (Contractor and Purchaser);
2) Perform verification to confirm that each element properly reflects the specified requirements, design, code, integration and documentation;
3) Support Purchaser led Validation Activities to confirm that the solution is fit for purpose.

TVV-7. The Contractor shall be responsible for the planning, execution and follow-up of all TV&V events.

[167] The Purchaser will assist in preparations by reviewing and providing feedback on all Contractor produced configuration items. The Purchaser will also provide testing and engineering Subject Matter Expertise (SME) during all TV&V events to witness and assist with these events.

TVV-8. The Contractor shall demonstrate to the Purchaser that there is a testing process in place for the project, supported by Contractor Quality Assurance (QA).

TVV-9. Where requested by the Purchaser, the Contractor shall provide test data to support all TV&V activities.

TVV-10. The Contractor shall follow the Purchaser defined TV&V processes.

TVV-11. If the Contractor wishes to propose a modification to the process, the proposal shall be approved by the Purchaser and documented accordingly.

TVV-12. The Contractor shall ensure that rigorous testing, including regression testing when required, is performed at every stage of the Project lifecycle in order to identify and correct defects as early as possible and minimise impact on cost and schedule.

TVV-13. All test, verification and validation material developed and used under the Contract shall be delivered to the Purchaser.

TVV-14. The Contractor shall strictly follow the test process, document templates and guidance provided by the Purchaser unless officially agreed by the Purchaser.

TVV-15. The Contractor shall provide an overall project Test Director for the phases defined in Table 8-1, who will work closely with the Purchaser's assigned TV&V Manager and NATO Quality Assurance Representative (NQAR). Table 5 defines the test phases considered. It deemed necessary, the project may split the test phases defined in Table 5 into multiple events.

[168] The Purchaser will provide subject matter experts (SME) during each test event, as well as TV&V Test Engineers and an NQAR.

TVV-16. The Contractor shall use Key Performance Indicators (KPIs) to identify opportunities for quality improvement, provide solutions and update the plans, the achievement of defined objectives like coverage of risks, requirements, supported configurations, supported operational scenarios, etc.

TVV-17. The Contractor shall have the overall responsibility for meeting the TV&V requirements and conducting all related activities defined in the Table 1-1Table 8-1 below, describing TV&V phases. Each phase may have one or more events to complete the full scope.

Table 8-1 TV&V Phases

TV&V Phases	Scope	Purchaser Involvement
Engineering Phase	Internal contractor activities executed during development phase of the system to ensure the system/software conforms to their design specifications.	**Review**: Test Reports for Unit, Integration and System tests. Inspections
Qualification Phase	Activities executed to verify the design and manufacturing process, ensure the system meets necessary design requirements, and	**Review**: Event Test Plan, Test Cases/Scripts, Test Report, Test Data, Test Environment Baseline,

TV&V Phases	Scope	Purchaser Involvement
	provide a baseline for subsequent acceptance tests. *Activities:* *TEMPEST Testing* *Electro-Magnetic Compatibility (EMC) Testing* *General Environmental Testing* *Water/Dust Ingress Testing* *Operational Robustness Testing* *Mechanical Environmental Testing* *Environmental Control Testing* *Biological & Chemical Testing* *Transportation Testing* *Physical Functional System Testing* *Product Safety Testing* *User Interface Testing* *Component Testing* *Interface Testing* *Security Testing* *Integration Testing (internal to the project deliverables)*	Existing defects. Demonstrations. Inspections **Participate**: Test Readiness Review (TRR), Test Execution, Event Review Meeting (ERM) **Provide:** Test Event Assurance Reports
Factory Acceptance Phase	To verify that production units comply with the requirement/design specifications and production can start. Confirm that all required engineering-level testing activities have been completed in accordance with the SOW. Determine if project deliverables are ready for subsequent TV&V activities.	**Review**: Event Test Plan, Test Cases/Scripts, Test Report, Test Data, Test Environment Baseline, Existing defects. Dry Run results. Certification **Participate**: Dry Run (Optional Purchaser participation), TRR, Test Execution, Event Review Meeting (ERM)
TV&V Assessment Phase	Independent assessment performed with Purchaser and led by Contractor to determine whether or not a system satisfies user needs, functionality, requirements, and user workflow processes etc. before it gets into operation. To ensure verification of quality criteria defined in figure 1 Product Quality Criteria, for the following tests: - **System Integration Test (SIT**) – Requirements based testing, focused on verifying integration of the different components together and with any external interface as defined by the SOW	**Review**: Event Test Plan, Security Test and Verification Plan (STVP), Test Cases/Scripts, Test Report, Test Data, Test Environment Baseline, Existing defects and Analysis thereof **Participate**: TRR, Test Execution, Event Review Meeting (ERM). User Reviews (including internal users)

TV&V Phases	Scope	Purchaser Involvement
	- **User Acceptance Test (UAT)** – Scenario based testing, focused on validating the system as per user needs. - **Security Tests** – Tests focused on ensuring the security criteria are met. - **System Acceptance Test (SAT)** – Tests focused on ensuring compliance with the requirements outlined in the SOW. - **RFC Evaluation** – Review by Agency Change Managers and execution of any additional evaluation as requested by Change Managers. Under normal circumstances, all required inputs are generated from TV&V activities	
Site Acceptance Phase (SiAT)	To ensure that the specific site/node is installed properly per site/node installation plan and the service meets the requirements stated in the SRS. Site Acceptance Testing is also to ensure compatibility and integration of the product with the site environment. Migration related tests are also covered under this tests. This includes integration with PFE.	**Review**: Event Test Plan, Test Cases/Scripts, Test Report, Test Data, Test Environment Baseline, Existing defects. Demonstration. Analysis. **Participate**: TRR, Test Execution, Event Review Meeting (ERM)
Operational Test and Evaluation	To ensure that all the Operational Acceptance Criteria (OAC) such as performance and availability have been successfully implemented. Sites are successfully integrated and tested on the network level. Demonstrate that all components of the System/Application have been integrated (including other systems) to meet all OACs as well as all security requirements defined in the Security Accreditation Documentation Package. Ensure end to end delivered system works as expected and can interoperate with other Purchaser equipment	**Review**: Event Test Plan, Test Cases/Scripts, Test Report, Test Data, Test Environment Baseline, Existing defects. Demonstrations. Analysis **Participate**: TRR, Test Execution, Event Review Meeting (ERM)

[169] The Purchaser reserves the right to monitor and inspect the Contractor’s TV&V activities to verify their compliance with the requirements set forth in this Contract.

[170] The Contractor shall ensure that their System Verification methodology and strategy of acceptance aligns to ISO/IEC/IEEE 29148 and the th e following verification methods:

a. Inspection - an examination of the item against applicable documentation to confirm compliance with requirements. Inspection is used to verify properties best determined by examination and observation (e.g., - paint colour, weight, etc.). Inspection is generally non-destructive and typically includes the use of sight, hearing, smell, touch, and taste; simple physical manipulation; mechanical and electrical gauging; and measurement. The pass/fail criteria are simple accept/reject indications and shall be based on the visual inspection results or information content of the documentation. Inspection is conducted by experts in product design (i.e., software designers, hardware designers, test team members), who are not directly related to the development of the product being inspected. Inspection of certificates is considered another form of inspection. The Contractor is responsible for obtaining certificates from the relevant independent authorities, who are recognised and, or accredited by NATO, demonstrating that the equipment delivered under this project has been built and set-up in accordance with this SOW and applicable International and European norms. Certificates shall identify the equipment's approving independent authority and list the requirements against which it has been validated. All necessary TDCIS compliancy criteria, shall be validated using this method;

b. Analysis - use of analytical data or simulations under defined conditions to show theoretical compliance. Used where testing to realistic conditions cannot be achieved or is not cost-effective. Analysis (including simulation) may be used when such means establish that the appropriate requirement, specification, or derived requirement is met by the proposed solution. Analysis may also be based on 'similarity' by reviewing a similar item's prior verification and confirming that its verification status can legitimately be transferred to the present system element. Similarity can only be used if the items are similar in design, manufacture, and use; equivalent or more stringent verification specifications were used for the similar system element; and the intended operational environment is identical to or less rigorous then the similar system element. Pass/fail criteria are objective and based on the analytical/simulation/analysis results versus the stated requirements and associated tolerances. Verification by analysis is applicable were demonstration or test is not feasible or economically viable;

c. Demonstration - a qualitative exhibition of functional performance, usually accomplished with no or minimal instrumentation or test equipment. Demonstration uses a set of test activities with system stimuli selected by the supplier to show that system or system element response to stimuli is suitable or to show that operators can perform their allocated functions when using the system. Observations are made and compared with predetermined responses. Demonstration may be appropriate when requirements or specifications are given in statistical terms (e.g., mean time to repair, average power consumption, etc.). This method is used to demonstrate a capability to be provided by the requirement. Test procedures and their test cases will contain test steps which define specifically the inputs and pre-conditions necessary for verification of the subject requirement. Pass/fail criteria are simple yes/no indications of functional performance since no quantitative values are specified. The Contractor shows the performance of a product, service, system or feature in use, be they representative or operational conditions. The execution of these tests requires the presence of the Purchaser, and possibly accompanied by Customer representative;

d. Testing - an action by which the operability, supportability, or performance capability of an item is quantitatively verified when subjected to controlled conditions that are real or simulated. These verifications often use special test equipment or instrumentation to obtain very accurate quantitative data for analysis. This method is used when it is possible to make direct or indirect measurement of a specific numerical parameter to verify compliance with a stated requirement. Actual measured values are recorded, and pass/fail is determined by comparing the measured value with the specified value. Input data and results are provided in the test procedures. Controlled condition, configurations, and inputs are used in order to observe the response. Results are quantified and analyzed. This method can be used where user interaction is involved and when computations with input data are necessary. Two basic test approaches are black box and white box testing. In black box testing, the inner structure and design of the test object is unknown or not considered and the test cases are derived from the specification. White box techniques are based in the knowledge of the inner structure of the test object, require that the source code were available and flow-oriented test cases will be identified. In practice, these approaches are used to complement each other because they tend to detect different classes of errors. Black box techniques are useful for finding incorrect or missing functions, interface errors, errors in data structure, performance errors and initialization and termination errors. Black box techniques miss many other errors because they ignore important properties of items that are due to design and implementation factors and incomplete requirement descriptions. White box testing focuses on such errors. Test comprises the emulation and, or simulation of the operational environment in which a product, service or system, under a specific configuration, is expected to operate. Test procedures shall follow standards referred to with the TDCIS System Requirements Statements (SRS) document. Test execution requires the presence of the Purchaser. The Contractor shall submit respective test reports for review to, and approval by the Purchaser;

e. Certification. The Contractor is responsible for obtaining certificates from the relevant independent authorities, who are recognised and, or accredited by NATO, demonstrating that the equipment delivered under this project has been built and set-up in accordance with this SOW and applicable International and European norms. Certificates shall identify the equipment's approving independent authority and list the requirements against which it has been validated. All necessary TDCIS compliancy criteria, shall be validated using this method.

TVV-18. The Contractor shall only proceed to the next formal TV&V activity, after the successful completion of the previous TV&V activity and after the agreement/approval by the Purchaser of it being fit for use and, or purpose.

8.3 DELIVERABLES

TVV-19. The Contractor shall provide a System Test Documentation Package, following documentation templates provided by the Purchaser, that is comprised of the following documents:

Table 8-2 Test Documentation

Work Product Name	First Draft	Sent to Review/Approve
The Master Test Plan (MTP)	During Bid	4 weeks after Contract award
Defect Reporting and Management Plan	During Bid	4 weeks after Contract award
Event Test Plans for individual test events (ETP)	During Bid (example)	4 weeks before TV&V event
The Security Test & Verification Plans (STVP)		as required per the NSAB
Any submitted test Waivers together with supporting material		4 weeks before TV&V event
The Test Cases/Scripts/Steps	During Bid (example)	4 weeks before TV&V event. First draft 4 weeks after Contract award
Status Reports		Periodically (to be defined in the MTP)
Test Completion Report		1 week after TV&V event
System under-test Documentation		2 weeks before TV&V event
The Requirements Traceability Matrix (RTM) updated with test-related information	During Bid	First with MTP and update per test event

TVV-20. If applicable, the Contractor shall develop and validate any Test Harnesses, simulators and stubs, including all script/code/data/tools required to execute the planned functional and non-functional tests in the Test Environment. The Test Harnesses for PFE will be provided by the Purchaser.

TVV-21. Modification of inaccurate or inadequate TV&V deliverables and any subsequent work arising as a result shall be carried out at the Contractor's expense.

TVV-22. Templates provided by the Purchaser are to be utilized by the Contractor as structure guides and for the content the Purchaser expects to be detailed. If the Contractor would like to propose a modification of the templates, it shall be approved by the Purchaser.

TVV-23. All deliverables shall undergo as many review cycles are required, and shall be approved once all deficiencies have been corrected.

8.3.1 MASTER TEST PLAN (MTP)

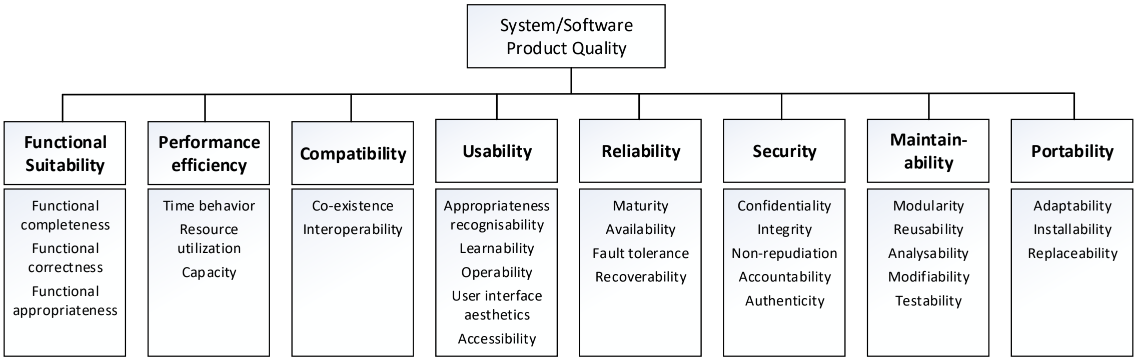
TVV-24. The Contractor shall identify and describe in the Master Test Plan (MTP) which best practices and international standards will be applied and how.

TVV-25. The Contractor shall produce a Master Test Plan (MTP) to address the plans for each TV&V activities listed in this document. The Purchaser will monitor and inspect the Contractor’s MTP activities to ensure compliance.

TVV-26. The Contractor shall keep the MTP always up to date.

TVV-27. The Contractor shall describe how the Quality Based Testing is addressed and implemented in the MTP. is based on ISO 25010 and should be used as product quality criteria model.

Figure 8-1 Product Quality Criteria



TVV-28. The Contractor shall describe all formal TV&V activities in the MTP with a testing methodology and strategy that fit the development methodology chosen by the project.

TVV-29. The Contractor proposed testing methodology shall describe the method of achieving all the test phases, defined in Table 8-1 successfully.

TVV-30. The Contractor shall describe in the MTP how the following objectives will be met:

1) Compliance with the requirements of the Contract;
2) Verification that the design produces the capability required;
3) Compatibility among internal system components;
4) Compliance with the SRS requirements;
5) Compliance with external system interfaces and/or systems;
6) Confidence that system defects are detected early and tracked through to correction, including re-test and regression approach;
7) Compliance with Purchaser policy and guidance (i.e. security regulations, etc.);
8) Operational readiness and suitability;
9) Product Quality Criteria (Figure 8-1).

TVV-31. The Contractor shall describe the Contractor’s test organization and its relationship with the Contractor’s Project Management Office and Quality Assurance (QA) functions in the MTP.

TVV-32. The Contractor shall describe in the MTP “Entry and “Exit” criteria for each of the formal TV&V events. The Contractor shall seek approval of all criteria related to an event not later than the TRR of the event

TVV-33. The Contractor shall provide in the MTP the schedule, location and scope for all the events to be run, specifying to which phase they belong. When the contractor identifies that multiple events are required for a phase, this shall also be specified in the MTP.

TVV-34. Together with the MTP, the contractor shall provide a defect reporting and management process to be applied during the TV&V activities.

TVV-35. The Contractor shall describe how defects/non-conformances encountered during TV&V events will be reported, managed and remedied.

TVV-36. The MTP shall include the Contractor's approach to Test Reviews including Test Readiness Reviews and Event Review Meetings for each TV&V event.

8.3.2 TEST CASES AND TEST PROCEDURES

TVV-37. Any updates required from the execution of test cases during each phase shall be incorporated into the relevant test cases by the Contractor for use during independent verification, validation and acceptance. If only certain sections are affected, then it shall be sufficient to up-date and re-issue those Section plus cover sheet with amendment instructions. Should major changes in contents or page re-numbering be needed, then the complete Section shall be re-issued by the Contractor. All changes shall be made with the agreement and approval of the Purchaser.

TVV-38. The Contractor shall submit the draft test cases for the TV&V event to the Purchaser for approval no later than four (4) weeks prior to the execution of the tests, unless differently stated in a work package. The Purchaser shall provide comments or approval within four (4) weeks of receipt. The purchaser must have the final version of the test cases and Event Test Plan available one (1) week prior to the TRR for a specific TV&V event.

TVV-39. The contractor shall develop test and use cases to verify and validate all requirements in the SOW, requirements specifications and final design. The test cases shall follow the template provided by the purchaser.

8.3.3 EVENT TEST PLAN

TVV-40. The contractor shall create an Event Test Plan (ETP) per each event detailing all the information required for that event. The ETP shall follow the template provided by the Purchaser.

TVV-41. The Contractor shall describe in the event test plan what training (if any) will be provided prior to formal TV&V events.

TVV-42. The Contractor shall identify, in the ETP, which environment(s) to be used at each TV&V event and the responsibilities for configuration control, operation and maintenance of the environment.

TVV-43. The ETP shall describe when an agreement shall be reached between the Contractor and the Purchaser on the defect categorization and defect priority of failures encountered, as well as a way forward (if either at the end of each day of a TV&V event or at the Event Review Meeting). If agreement is not reached, the disputed items shall be escalated to the Purchaser's and Contractors' Project Managers.

8.3.4 REQUIREMENTS ACCEPTANCE CRITERIA

TVV-44. Requirement Acceptance criteria represent a condition that states whether the specified SRS requirements are fulfilled or not. Written in simple language, the Acceptance Criteria is complementary to each contractual requirement in the SRS and provides the basis of a shared understanding for what is to be delivered and what is required as objective evidence to assess that a requirement has been met. Acceptance Criteria for requirements with V&V Method of Test and Demonstration for instance can be written in “Given/When/Then” format. It is meant to provide a logical description which actions would lead to meeting the requirements. It is not meant to provide detailed input or physical description (as this is the actual Test Case/Script).

TVV-45. The Contractor shall translate each requirement in the SRS, in an acceptance criteria that will clearly detail how the requirement will be fully met (clear pass/fail or yes/no outcome).

TVV-46. The Contractor shall address the Purchaser's comments and update the Acceptance Criteria accordingly.

TVV-47. The Acceptance Criteria shall be agreed by both contractor and puchaser prior to the creation of the Test Cases/ Scripts.

TVV-48. The agreed Acceptance Criteria shall be translated into Test Cases to provide details of full requirements coverage.

8.3.5 Requirement Traceability Matrix

TVV-49. The Contractor shall produce and maintain the Requirement Traceability Matrix (RTM), which includes all functional and non-functional requirements, to track the TV&V status of all requirements throughout the Contract execution (especially during the TV&V activities).The RTM shall also trace the requirements to the design. It shall also define how the requirements will be validated or verified at each of the TV&V activities:

1) The verification method: Inspection, Analysis, Test or Demonstration;
2) Correspondent TV&V phase(s) for each requirement;
3) Coverage Status.

[171] The Purchaser will review and approve the proposed RTM.

TVV-50. The contractor shall maintain the RTM updated during the project lifecycle.

TVV-51. The RTM shall map the applicable Operational Acceptance Criteria (OAC) to the SoW and SRS requirements. The Contractor shall establish the OAC traceability at the requirements analysis stage and approve at design stage.

TVV-52. The RTM shall be provided and maintain as an appendix to the SDS, extend this matrix to the Developmental Baseline, Product Baseline and the Management Test Plan (MTP) to ensure verification thought the project.

TVV-53. The RTM shall guarantee the two way link between requirements (SRS) and technical specifications.

TVV-54. The Contractor shall provide the Purchaser with updates (via the tools) to the RTM daily during the execution of an event, and following the conclusion of each event defined in the MTP. A workflow for updating the RTM shall be proposed by the Contractor and approved by the Purchaser.

TVV-55. If the verification method per requirement is not provided beforehand, the verification method shall be test. Any deviation to this requirement is subject to Purchaser approval.

8.3.6 SECURITY TESTING VERIFICATION PLAN

TVV-56. The Contractor shall produce an STVP, to ensure that the Security testing, including verification of compliance with NATO CIS security regulations is applied. This is an integral part of the TV&V process.

TVV-57. The STVP shall support the accreditation of the System Platform. This document shall be approved by NATO Office of Security.

8.3.7 TEST COMPLETION REPORT

TVV-58. The Test Completion Report provides a summary of the testing performed during the Test Event.

TVV-59. The Contractor shall provide, in the Test Completion Report, a log/record of the event, including but not limited to individual test results, defects found (with a way forward for the ones remaining open), requirement coverage (planned and executed), test execution durations, deviations during execution and sign-off for each result by both the Contractor and Purchaser.

8.4 TOOLS

TVV-60. The Contractor shall generate and deliver automated test procedures/cases compatible with Purchaser test management and automation tools.

TVV-61. The Contractor shall make use of automated testing and supporting testing tools (test management, requirement coverage, defect management, etc.) to the maximum applicable extent, for all system development, implementation, internal and formal tests. The process and proposed supportive tools shall be described in the Master Test Plan (MTP). In areas where the Purchaser already uses specific tools, the Contractor shall make use of the tools in use by the Purchaser.

TVV-62. Tools supporting requirements coverage, defect management and test management shall be selected and hosted by the Purchaser and used by the Contractor. For any internal work, the Contractor may use their own internal tools, but the tools used for the contractor's internal work shall be able to natively interface with the tools selected and hosted by the Purchaser in order to keep all TV&V related data for the project in the Purchaser tools.

8.5 TEST VERIFICATION & VALIDATION EVENTS AND RESULTS

TVV-63. The Contractor shall conduct testing during the Project lifecycle compliant with the following requirements:

TVV-64. The Contractor is responsible for conducting all testing during the Project lifecycle. The contractor shall provide evidence to the Purchaser of the results of these testing activities. The Contractor shall respond to any Purchaser clarification requests regarding test results or performance within two working days

TVV-65. The Contractor shall conduct all testing activities for any architectural changes.

TVV-66. The Contractor shall support post go-live activities during the Operational Acceptance phase, to evaluate the project capability performance and establish benchmarks for future enhancements, including any changes made to fulfil the requirements.

TVV-67. The Contractor shall provide status reports to the Purchaser regarding verification and validation activities during the planning/design and development phases, via the use of a dashboard report within the test management tool set and through meetings. The Contractor shall provide report(s) to the Purchaser following the completion of any TV&V event.

[172] The Purchaser will approve the report and its findings within two business days.

TVV-68. Progress and result measurement shall be approved by the Purchaser and focused on KPIs.

TVV-69. Test results shall be recorded in the test management tool set. All results of all formal acceptance testing performed during a given day must be recorded in the test management tool. The Contractor shall provide these test results for any given day by the starting of the next business day (0800 AM), but as a minimum not later than 24 hours following the execution of any test.

8.5.1 TEST READINESS REVIEW (TRR)

TVV-70. The Contractor shall conduct a Test Readiness Review (TRR) meeting at least one week prior to the events defined in the MTP. The TRR shall ensure that all entry criteria for the events have been met. Documentation that requires review by the Purchaser prior to a TRR, as defined in the Event Test Plan (ETP), shall be provided no less than 2 weeks prior to TRR.

TVV-71. The Purchaser has the right to cancel the TRR and/or any formal test event if the evidence demonstrates that execution of the test event will not be effective.

TVV-72. The Contractor shall demonstrate that all the internal tests and dry runs are successful with test reports and results delivered to the Purchaser at least 2 weeks prior to start of any Contractual test activities.

8.5.2 EVENT REVIEW MEETING

TVV-73. The start and/or ending of any test session shall be subject to the Purchaser approval. In the event that critical issues are encountered which impact the process of the testing or if the other functions depends on the failed test cases, the Purchaser has the right to stop the testing for Contractor's investigation. The tests can only re-start if Purchaser agrees to continue testing from the point of failure or re-start testing from the beginning.

TVV-74. The Contractor shall convene an Event Review Meeting (ERM) as defined in the ETP. The ERM shall ensure that the event results, defect categorization and a way forward to fixing the defects (if required) is agreed upon the Contractor and the Purchaser,. If agreement is not reached, the disputed items shall be escalated to the Purchaser's and Contractors' Project Managers.

8.5.3 TV&V EVENT

TVV-75. An event starts with the Test Readiness Review (TRR) and finishes off with the Event Review Meeting (ERM).

TVV-76. During formal TV&V phases, a daily progress debrief shall be scheduled. Participation to the daily progress debrief will be agreed between Purchaser and Contractor. The aim of the debrief is to get a common understanding on what tests were run, which passed, which failed, and whatever defects were reported during the day.

TVV-77. For each TV&V event, the Contractor shall provide log/record of the event, including but not limited to individual test results, defects found, requirement coverage, test execution durations, deviations during execution and sign-off for each result by both the Contractor and Purchaser.

TVV-78. At the end of the project, the Contractor shall provide the final version of all artefacts (regardless of format) created during the execution of all TV&V activities.

8.5.4 Test Waivers

TVV-79. The Contractor may request a Test Waiver if the Contractor has previously successfully completed qualification testing to national, or international standards for assemblies, subassemblies components or parts. The Purchaser, after review of test waivers and analysis of their impact, reserves the right to require test and certification of the modified equipment at no cost to the Purchaser. The Purchaser has the right to reject any test Waiver.

TVV-80. In respect to a requested waiver, the Contractor shall certify that the test environment to be implemented is identical to that which was originally used for testing, or advise the Purchaser of design/construction changes which affect form, fit or function.

TVV-81. The Contractor shall record and log all waiver requests along with their resolution submitted for the Purchaser's approval.

8.5.5 Failed events

TVV-82. In the event of failed TV&V event and the need to return to a site for re-testing; travel and per diem expenses of NATO personnel shall be borne by the Contractor

8.6 Test Defect Categorisation

TVV-83. The Contractor shall use the Purchasers' categorization nomenclature for all defects and non-compliances

TVV-84. Should a failure be identified during a TV&V event/activity, a defect shall be recorded in the Agency's' test management and defect management systems. Once the event has concluded, the defect shall be reviewed during the event review meeting to agree on the severity, priority and category. The event test report shall then report the disposition of all defects recorded during the event and the defect management system shall be updated accordingly. Classification shall follow the definitions in Table 8-3:

Table 8-3 Definitions for Defect Categorization

Attribute s	Definition
Severity	The severity of a defect is the degree of impact that the failure has on the development or operation of a component, a system or a user function.

	The severity shall initially be proposed by the tester but shall officially be set in agreement with all the stakeholders. When agreement cannot be reached, the Purchaser's PM will set the severity.
Priority	The priority of a defect defines the order in which defects shall be resolved. The priority of the defect shall initially be proposed by the tester but shall officially be set in agreement with all the stakeholders. When agreement cannot be reached, the Purchase's PM will set the priority.
Category	The type of observation identified during the execution of a test case.

8.6.1 SEVERITY

TVV-85. According to their severity, defects shall be classified as one of the following in Table 8-4:

Table 8-4 Classification of defects based on severity

Severity	Definition
Critical	The failure of testing of a requirement. The failure results in the termination of the complete system or one or more component of the system. The failure causes extensive corruption of data. The failed function is unusable and there is no acceptable alternative method to achieve the required results
Major	A significant failure that causes severely impaired functions but does not prevent operational processing. Applies to conditions under which the complete system or one or more component of the system are partially inoperative, but are still usable by the users. A work around may be available, but it may require manual intervention. Examples: * Absence of expected modules/ object or Unit * failure of business operational process that affects a large group of users * complete failure of a module

Severity	Definition
Moderate	The failure does not result in the termination and all functions are available but causes the system to produce incorrect, incomplete or inconsistent results. When resources are available and budgeted, should be resolved.
Minor	The failure does not result in termination and does not damage the functioning of the system. The desired results can be easily obtained by working around the failure.
Cosmetic	The failure is related to the look and feel of the application, typos in a document or user interfaces (amongst others), and not part of the immediate usability or contractual requirements. The failure does not adversely affect the overall system operation.

8.6.2 PRIORITY

TVV-86. According to their priority, defects shall be classified as one of the following in Table 8-5:

Table 8-5 Priority Classes for Defect Classification

Priority Class	Description
Urgent	The defect shall be resolved as soon as possible. Required to complete independent verification and validation activities.
Medium	The defect shall be resolved in the normal course of development activities. It can wait until a new build or version is created.
Low	The defect is an irritant which should be repaired, but repair can be deferred until after more serious defects have been fixed.

8.6.3 CATEGORY

TVV-87. According to their category, deficiencies shall be classified with one of the values defined in Table 8-6:

Table 8-6 Deficiency Categories

Category	Description
Defect	An imperfection or deficiency in a work product where it does not meet its requirements or specifications. This category of defect could drive to the creation a Class II (Product Correction) Engineering Change Proposal (ECP).

Category	Description
Enhancement	This type of defect is used to record an Improvement to the product baseline. This category of defect would typically drive to the creation of a Class I (Product enhancement) ECP.
Document	This category is used to record deficiencies encountered in the system documentation (test cases, test procedures, RTM, test plan, manuals, design, procedures…).
Clarification	This category is used to record deficiencies encountered during the test execution, which must be clarified.
Waiver	This category is used to record when a waiver is required to address a specific observation or deficiency.

9 Security Accreditation

9.1 INTRODUCTION

[173] The Tactical Deployable CIS (TDCIS) needs to achieve security accreditation in order to be granted the authorisation for operational use at S*CR*T level. Therefore, the security accreditation process established by the appropriate Customer and Purchaser Security Accreditation Authorities (SAA) are to be followed.

[174] The primary objective of security accreditation is to ensure that an adequate level of protection is achieved and maintained throughout the life cycle of the TDCIS. This includes ensuring that the TDCIS conforms to NATO Security Policies and Directives identified and SRD listed in this SoW.

[175] The security accreditation of the TDCIS DCIS is to follow a structured process based on the high level requirements established in the Management Directive on CIS Security (ref. 9), as detailed in this document. Deviations from this structured process are to always be documented and can only be authorised by the appropriate SAA.

[176] The Security accreditation is to be granted by the Purchaser's SAA for the TDCIS to store, process and/or transmit NATO information in its desired environment.

9.2 SECURITY ACCREDITATION REQUIREMENTS

[177] This Section defines the requirements pertaining to the execution of WP3. This Section also describes the security accreditation process for the TDCIS project, in accordance with the current NATO Security Policies and Directives.

[178] Security Accreditation for NATO Communications and Information Systems (CIS) is a structured process to ensure that an adequate level of protection is achieved and maintained throughout the life cycle of the CIS.

SEC-1. Security Accreditation Process for TDCIS, as described in the NATO Security Policies and Directives shall be strictly followed by the Contractor and shall encompass overall development, production and implementation of the TDCIS DCIS.

SEC-2. A verification that security measures (personnel security, physical security, security of information, CIS security controls), including security baselines identified in the respective System-specific Security Requirement Statements (SSRS) and SecOPs have been properly implemented in accordance with the requirements of the SAA is one of the primary bases for the security accreditation for the TDCIS.

SEC-3. This verification is carried out by the SAA and typically supported by appropriate results of security testing conducted based upon agreed Security Test and Verification Plan (STVP) which is to cover all security requirements identified and approved in form of System-specific Security Requirement Statement (SSRS).

SEC-4. Due to the TDCIS architecture and its operational purpose (DCIS), Electronic Security Environment (ESE) assessment process is to be decoupled from the assessment provided for the Global Security Environment (GSE) and Local Security Environment (LSE). This is because for the TDCIS, being deployable CIS, both target GSE and LSE are unknown and cannot be addressed in advance. As the opposite, appropriate evaluation of ESE for the TDCIS will be done before any deployment.

SEC-5. It is the overall responsibility of the Contractor to develop an appropriate TDCIS system design and security-related documentation in order to achieve security accreditation of the TDCIS. The design and the SRD deliverables shall be compliant with Security Policies and Directives in this SoW.

SEC-6. In support of producing the deliverables the Contractor shall closely engage directly with representatives of the Purchaser and/or SAA (through the Purchaser) in order to discuss particular security-related requirements but also to clarify and/or enhance the documentation to be provided as part of the Security Related Documentation.

SEC-7. This process shall be organised in the form of one or several workshops that shall be attended by the Contractor and by representatives of the Purchaser. Location of the meetings and workshops will be defined by the Purchaser and will typically take place at a facility located in the Purchaser. The Contractor may be invited to provide briefings and/or technical expertise for meeting(s) with the SAA.

SEC-8. The SAA may provide advice and instructions to the Contractor on any security implication, or any proposed change based on the findings and results of the assessments and/or security tests. The advice, instructions and guidance from the SAA shall be considered by the Contractor. The Contractor shall take action(s) to follow, carry out the necessary work and to implement the advice, instructions and guidance given by the SAA.

SEC-9. The Contractor shall recognise the NATO Security Policies and supporting Directives, in order to take into account all related requirements in the resulting TDCIS system design and installation thereof.

SEC-10. The Contractor shall take into account the NATO CIS security requirements for the implementation and support of three security domains in the deployed environment, NATO S*CR*T (NS), Mission S*CR*T (MS), and NATO Unclassified (NU) respectively.

SEC-11. The Contractor shall be responsible to develop and implement the TDCIS system in accordance with the NATO CIS security requirements and provide all required security-related documentation for TDCIS system (in English language) in order to achieve security accreditation of the TDCIS DCIS.

[179] Security accreditation for TDCIS needs to be achieved before the system is to be put into the operation(s).

[180] When there will be a requirement to test specific TDCIS node(s) or elements therof, before use in the final operational environment, the SAA may grant an Approval for Testing (AfT) with caveats to be applied to its use. These caveats could include the scope of tests, the classification of information involved in the testing, the test plan and the timeframe for the AfT, etc.

SEC-12. The Contractor shall coordinate with the Purchaser, all AfT requirements and provide filled AfT Request (based on the Purchaser provided template (ref. 9)) to the Purchaser as required. The Purchaser shall coordinate this request with SAA.

[181] Approval for Testing is typically required (but not limited) to conduct necessary security testing in accordance with Security Test and Verification Plan (STVP).

[182] Depending on the infrastructure involved, functional testing of TDCIS may also require AfT to be issued by the SAA.

9.3 SECURITY-RELATED DOCUMENTATION

SEC-13. The Security-related Documentation (SRD) in support of the accreditation process, comprised of the following deliverables in English language, shall be provided by the Contractor:

1) CIS Description;
2) Security Accreditation Plan (SAP);
3) Security Risk Assessment (SRA);
4) System Specific Security Requirement Statement (SSRS);
5) Generic System Interconnection Security Requirement Statement (SISRS);
6) Security Operating Procedures (SecOPs);
7) Security Test and Verification Plan (STVP);
8) Security Test and Verification Report (STVR); and
9) Electronic Security Environment (ESE) Conformance Statement (ESECS).

SEC-14. The Contractor shall produce key security-related documentation or inputs to documents in support of the TDCIS security accreditation, as detailed below.

SEC-15. The Contractor shall produce required documentation or inputs to documents using templates, provided by the Purchaser, as listed in the Appendix B, Section B.2.8. These will be provided after contract award.

9.4 SECURITY ACCREDITATION PLAN (SAP)

[183] The Security Accreditation Plan describes the steps to be taken to achieve security accreditation for TDCIS.

SEC-16. Initial version of the Security Accreditation Plan for the TDCIS shall be developed by the Contractor and presented for the approval to the SAA.

SEC-17. The Contractor shall deliver its Security Accreditation Plan (SAP) as a part of the initial Project Implementation Plan (PIP). All activities related with the security accreditation process shall be identified in the respective Project Implementation Plan (PIP) and in the Project Management Plan (PMP).

SEC-18. The Contractor shall ensure the SAP describes:

1) How the Contractor shall meet all the guidelines and principles of Section 6;
2) How the Contractor shall carry out its Site Survey Reports specific to Security;
3) Clearly and succinctly, a description of the TDCIS;
4) How the Security Accreditation process is to be pursued for this particular system;
5) Facilitate and chair its security workshops and meetings;
6) What adaptations are required based on NATO approved templates;
7) All planning for dates, milestones and deliverables;
8) Security descriptions.

SEC-19. The Contractor shall ensure that the SAP is available for Purchaser review by PDR noting that the PDR will serve to outline the documentation to be produced in relation to the security accreditation objective.

SEC-20. Timeline specified in the SAP shall be maintained by the Contractor during the project to address changes in the PIP and PMP.

SEC-21. Any other changes required by the Purchaser to be incorporated into the SAP shall be addressed by the Contractor and provided to the Purchaser who will coordinate this with SAA.

SEC-22. The Contractor shall strictly adhere to the security accreditation activities described in the SAP as approved by the SAA. All activities related with the security accreditation process shall be identified in the respective Project Implementation Plan (PIP) and in the Project Management Plan (PMP).

SEC-23. Timeline specified in the SAP shall be maintained by the Contractor during the project to address changes in the PIP and PMP.

SEC-24. Any other changes required by the Purchaser to be incorporated into the SAP shall be addressed by the Contractor and provided to the Purchaser who will coordinate this with SAA.

9.5 CIS DESCRIPTION

[184] The CIS Description for TDCIS is the first document in support to security accreditation to be developed after contract award.

SEC-25. The CIS Description for TDCIS shall be developed by the Contractor based on Purchaser's provided template (Appendix B - A.2.7) and shall be approved by the SAA (through the Purchaser).

SEC-26. The CIS Description shall be formulated at the earliest stage of the project (TDCIS planning stage) and shall be further enhanced as the project develops.

SEC-27. The CIS Description document shall at a minimum include the following information:

1) Detailed technical description showing the main components and the high level as well as detailed information flows, and how these are protected, inclusive of any data flow from leveraged networks/infrastructure (if any);
2) Description of all internal and external connections of the system;
3) List of hardware and software components used;
4) Overview of the security mechanism which are going to be implemented in the TDCIS DCIS and all its components.

SEC-28. The Contractor developed CIS Description shall be submitted to the Purchaser for review before they will be provided to the SAA for approval.

SEC-29. The Contractor shall take into account any comments from the reviewers and SAA and shall update the CIS Description document as many times as necessary in order to obtain SAA approval.

SEC-30. The Contractor shall maintain and keep the CIS Description document up to date throughout the project.

9.6 SECURITY RISK ASSESSMENT

[185] The Security risk assessment is the process of identifying security risks, i.e. the threats and vulnerabilities to the CIS, determining their magnitude and identifying

areas needing countermeasures. Security risk assessment serves to identify the risks that exist, identify the current security posture of the CIS in respect to handling information, and then assemble the information necessary for the selection of effective security countermeasures, based upon NATO Security Policy and supporting Directives and Guidance.

[186] The Security risk assessment contributes to the decision on which security measures are be required, and how the apportionment between technical and alternative security measures can be achieved, and gives an unbiased assessment of the residual risk.

SEC-31. The Security Risk Assessment (SRA) for the TDCIS shall be conducted by the Contractor based on the information provided in the CIS Description document. SRA is to be approved by the SAA.

SEC-32. SRA shall be conducted in accordance with AC/35-D/1017. Refer to Table 2-1, Section 2.3.5.

SEC-33. The Contractor shall use the SRA application PILAR 8.1 version minimum (and utilising MAGERIT methodology) with the NATO profile for producing the Security Risk Assessment for the TDCIS.

[187] Note access to the NATO Pilar application, with the NATO profile can be made available for the Contractor to produce the TDCIS SRA, if required.

SEC-34. The Contractor shall use the NATO template "SRA Report (PILAR) Template", as listed in the Appendix B, Section B.2.8, to document the results of the SRAs.

[188] Objective of the SRA is to define the security objectives of confidentiality, availability and integrity/authenticity of the designed TDCIS systems according/in tandem to the particular services to be provided by the resulting TDCIS system, the values of the traffic and information stored and transported over the TDCIS system, and the nature and levels of the particular threats being identified.

SEC-35. The Contractor shall organise SRA workshop(s) at Purchaser facility. Respective Purchaser's Subject Matter Experts (SMEs) shall be invited to support proper assessment. It has been anticipated that at least 2 (two) up to 5 (five) days SRA workshops will be required.

SEC-36. The Security Risk Assessment process for the TDCIS shall include the following stages:

1) Identification of the scope and objective of the security risk assessment (which shall be agreed with the Purchaser plus National and NATO SAA);
2) Determination of the physical, personnel and information assets which contribute to the fulfilment of the mission of the TDCIS;
3) Determination of the value of the physical and personnel assets;
4) Determination of the value of the information assets against the following impacts: disclosure, modification, unavailability and destruction;
5) Identification of the threats and vulnerabilities to the risk environment and their level;
6) Identification of existing countermeasures;
7) Determination of the necessary countermeasures and a comparison with existing measures; identifying those countermeasures which are already installed and identifying those countermeasures which are recommended.

SEC-37. Based on the results of the Security Risk Assessment SRA, the Contractor shall identify areas of TDCIS DCIS requiring safeguards and countermeasures to comply with NATO Security Policy and supporting Directives. The decision on specific security mechanisms shall be based on evidence(s) and results produced by the Security Risk Assessment.

SEC-38. Where the implementation of security measures results in the modification of the design (without introducing additional components), other documentation requirements, and changes to configuration of components, the Contractor shall consider these changes to be within the technical and financial scope of this Contract; no Engineering Change Proposal (ECP) shall be generated.

SEC-39. Where the implementation of security measures results in a requirement for additional components to be procured for implementation that could not be reasonably foreseen beforehand, an ECP shall be raised by the Contractor.

SEC-40. The Contractor shall take into account any comments from the SAA (provided to the Contractor through the Purchaser) and shall conducts update of SRA document as many times as necessary in order to obtain SAA approval.

SEC-41. The SRA for the TDCIS shall be composed as a standalone document.

9.7 SYSTEMS-SPECIFIC SECURITY REQUIREMENT STATEMENT

[189] The System-specific Security Requirement Statement (SSRS) is a complete and explicit statement of the security principles to be observed ands of the detailed security requirements to be met.

[190] SSRS specifies how security is be achieved, managed and checked.

SEC-42. The SSRS for TDCIS DCIS shall be developed by the Contractor based on Purchaser’s provided template (Appendix B) and shall be approved by the SAA (through the Purchaser).

SEC-43. The SSRS shall be formulated at the earliest stage of the project (TDCIS planning stage) and shall be further developed and enhanced as the project develops.

SEC-44. The Contractor’s developed SSRS shall:

1) Describe the minimum levels of security deemed necessary to countermeasure the risk(s) identified in a risk assessment;
2) Have an unique identifier for each security requirement;
3) Indicate mandatory and recommended Security Mechanisms (SMs).

SEC-45. SSRS shall be based on NATO Security Policy and supporting Directives and the Security Risk Assessment. The SSRS for TDCIS shall also take into consideration parameters covering the operational environment such as the lowest level of personnel security clearance, the highest classification of information handled, the security mode of operation and other Purchaser’s specific requirements.

SEC-46. The Contractor shall take into account any comments from the SAA (provided to the Contractor through the Purchaser) and shall conduct update of SSRS document as many times as necessary in order to obtain SAA approval.

9.8 SYSTEM INTERCONNECTION SECURITY REQUIREMENT STATEMENT

SEC-47. The Contractor shall develop a generic SISRS for TDCIS DICS in order to cover security requirements for the interconnection of the TDCIS DCIS with other CIS (based on scenario types provided be the Purchaser).

SEC-48. The generic SISRS shall covered all identified interfaces to other system(s).

SEC-49. The generic SISRS for TDCIS DCIS shall be developed by the Contractor based on Purchaser's provided template, as listed in the Appendix B, Section B.2.8, and shall be approved by the SAA (through the Purchaser).

SEC-50. The Contractor shall take into account any comments from the SAA (provided to the Contractor through the Purchaser) and shall conduct update of the generic SISRS document as many times as necessary in order to obtain SAA approval.

9.9 SECURITY OPERATING PROCEDURES

[191] Security Operating Procedures (SecOPs) are a description of the implementation of the security measures to be adopted, the operating procedures to be followed and the responsibilities of the personnel.

SEC-51. SecOPs for TDCIS DCIS shall be developed by the Contractor based on Purchaser's provided template (shall be approved by the SAA (through the Purchaser).

SEC-52. SecOPs for the TDCIS shall contain separate chapters for personnel performing security management as well as administrative functions (e.g. Core Administrators, Local Administrators, and CIS Security Officer) and TDCIS users[16].

SEC-53. SecOPs for the TDCIS, as a minimum, shall include following sections:

1) Administration and organisation of security, including points of contact;
2) Personnel security, physical security, security of information;
3) CIS Security;
4) Incident and emergency procedures;
5) Configuration management;
6) Acceptable use policy.

SEC-54. SecOPs shall also cover all security requirements identified in the SRA and SSRS which are not fully fulfilled by technical countermeasures. For example, following security procedures should be addressed (not exhaustive list) :

1) System configuration and maintenance;
2) System backup;
3) System recovery, etc.

SEC-55. The Contractor shall take into account any comments from the SAA (provided to the Contractor through the Purchaser) and shall conduct update of SecOPs document as many times as necessary in order to obtain SAA approval.

SEC-56. While the remainder of the TDCIS documentation is to be in English language, the

[16] If required separate SecOPs for different groups of users might be developed.

Contractor shall take into account that the SecOPs is a user/admin facing official document, that must be signed by users and administrators prior to their operation of the TDCIS. Therefore, the Contractor shall offer a bilingual approach to the development of the SecOPs, wherein both the English and Portuguese languages will be used.

9.10 SECURITY TEST AND VERIFICATION PLAN (STVP)

[192] A Security Test and Verification Plan (STVP) is a description of the security testing and verification of the CIS Security measures to be implemented for the TDCIS.

SEC-57. The STVP for TDCIS DCIS shall be developed by the Contractor based on Purchaser's provided template and shall be approved by the SAA (through the Purchaser).

SEC-58. The STVP shall describe in details the tests which will demonstrate compliance with the security requirements for the TDCIS DCIS identified in the respective SSRS, generic SISRS and SecOPs.

SEC-59. The Contractor shall ensure that the STVP defines a complete and detailed sequence of steps to be followed to prove that the security mechanisms designed into TDCIS enforce the security requirements identified in the TDCIS SSRS.

SEC-60. For each security test the following details shall be identified:

4) The objective of the security test;

5) An outline description of the security test;

6) A description of the execution of the security test (too include technical instructions how to conduct the test);

7) The pass criteria for the security test.

SEC-61. The Contractor shall ensure that each and every security test is cross-referenced to the corresponding security requirements from the TDCIS SSRS (identified by the unique identifier) as well as to the tested security mechanisms (SMs).

SEC-62. The Contractor shall ensure all security requirements and security mechanisms identified for the TDCIS are planned for testing.

SEC-63. The Contractor shall execute the STVP for the TDCIS DCIS and develop respective Security Test and Verification Report (STVR).

SEC-64. Execution of STVP conducted at Purchaser's shall be witnessed by the Subject Matter Expert (SME) designated by the Purchaser. He/She is to countersign respective STVR(s).

SEC-65. The Contractor shall also develop, provide and maintain the initial and any updated Security Implementation Verification Procedures (SIVP) for the TDCIS DCIS as part of Security Tests.

SEC-66. These procedures shall consist of a set of software scripts and inspection procedures that shall allow a CIS Security Officer to verify that all components of the TDCIS DCIS have been installed and configured property and comply with the SSRS and SecOPs.

SEC-67. The Contractor shall take into account any comments from the SAA (provided to the Contractor through the Purchaser) and shall conduct update of STVP and/or SIVP documents as many times as necessary in order to obtain SAA approval.

9.11 SECURITY TEST AND VERIFICATION REPORT (STVR)

[193] A Security Test and Verification Report (STVR) is a description of the results for the every instance of security testing conducted based on STVP.

SEC-68. The Contractor shall develop STVR for every instance of security testing conducted based on STVP.

SEC-69. The STVR template for the TDCIS DCIS shall be developed by the Contractor.

SEC-70. For each security test the following details shall be identified in the STVR:

1) Test ID;
2) An outline description of the security test;
3) The pass criteria for the security test;
4) The results of the security tests;
5) Test status (e.g. in progress, passed, failed)
6) Test completion (in per cent);
7) Failure severity (e.g. critical, high, medium, low, none);
8) Test date;
9) An info about who conducted the test;
10) An information about who witness the test.

SEC-71. STVR shall contain overall test summary details:

1) Identification of the element under tests (TDCIS deployable kit(s));
2) Tests starting date;
3) Tests finishing date;
4) Amount of all tests to be conducted;
5) Amount of tests executed;
6) Tests passed;
7) Tests failed;
8) Tests still in progress;
9) Amount of findings with clear distinguish of their severity (e.g. critical, serious, major, less important).

SEC-72. As the part of the STVR preparation, the Contractor shall also fill the Electronic Security Environment (ESE) Conformance Statement (ESECS) based on the Purchaser provided template, as listed in the Appendix B, Section B.2.8. ESECS after the Purchaser approval (signature) will be provided together with the test results (in form of the STVR) to the SAA as required for Deployable CIS.

SEC-73. Detailed TDCIS deployable kit configuration shall be depicted in the associated ESECS. If virtual infrastructure is to be used, all deployed virtual machines shall be also identified.

SEC-74. A separate ESECS shall be filled be the Contractor for each TDCIS kit.

SEC-75. The Contractor shall take into account any comments from the SAA (provided to the Contractor through the Purchaser) and shall conduct update of STVR (this might require some security tests to be re-conducted) and ESECS as many times as necessary in order to obtain SAA approval.

10 SYSTEM ACCEPTANCE

10.1 PROVISIONAL SYSTEM ACCEPTANCE (PSA)

[194] The concept of Provisional System Acceptance (PSA) is based upon the knowledge that complex and technically sophisticated systems may not be delivered without some deficiencies in the compliance with the totality of the Contract requirements.

SAC-1 To progress to PSA the Contractor shall have to have successfully completed all of WPs 1 to 7; see Section 2.

SAC-2 Should there be any outstanding deficiencies, the Contractor shall be handle these as detailed in Section 6.3.3.

SAC-3 The Contractor shall identify, document and maintain a complete Deficiency Log, listing of all deficiencies discovered during the testing leading up to its request for PSA and those which otherwise may exist at the time that the systems are offered to the Purchaser for PSA.

SAC-4 In order to request PSA of the systems delivered under this Contract, the Contractor shall have completed the following actions:

1) All deliverables under the Contract, have been supplied;
2) Approval of the SAT reports by the Purchaser;
3) The training courses and delivery of all training materials;
4) The delivery of all required special tools and test equipment, all spares and consumable items;
5) The delivery of all required documentation;
6) A deliverables inventory has been provided which details all the deliverables to be supplied under the terms of the contract;
7) The design documents have been supplied with updates to accurately reflect the “As Built” configuration and verification of the accuracy of the Documentation has taken place;
8) Certificates of Conformity (CoC) have been supplied that the equipment conforms to the contractual standards and applicable manufacturing standards;
9) A complete list of cryptographic keys, such as activation keys, feature keys, password lists and any other password and/or codes necessary for the Purchaser to operate the system from day to day, has been supplied to the Purchaser.

SAC-5 At such time as the Contractor has completed the prerequisites defined above, he shall notify the Purchaser in writing that the systems are offered for PSA.

SAC-6 This notification shall be accompanied by the PSA Report for the systems being offered.

[195] The process of PSA review starts with the delivery of the PSA Report.

SAC-7 The PSA Reports submitted to the Purchaser for PSA (one report for each of the systems delivered under this Contract, i.e. Operational (Batch 1) and shall include the following information:

10) Status of each individual equipment, sub-systems i.e. installation, integration, notification, operation;

11) Complete test reports, for each of the all testing and acceptance events leading to PSA;

12) Reliability Maintainability and Availability (RMA) Analysis Report;

13) Status of inventory;

14) Status of documentation relevant to the acceptance e.g. as-built drawings, handbooks, quality assurance reports;

15) Status of codification action;

16) Status of training package;

17) The Deficiency Log, listing all the open deficiencies, and describing the resolution strategies and target dates, as agreed with the Purchaser.

[196] Within 4 weeks of receipt of the PSA Report, the Purchaser will schedule a PSA Review Meeting.

SAC-8 The PSA Meeting will be chaired by the Purchaser with the objectives of:

1) providing a review of the status of each system, specifically reviewing and discussing the status of all observed deficiencies, as listed in the system's specific Deficiency Log;

2) establishing a list of all observed deficiencies which have yet to be corrected by the Contractor;

3) evaluating the list of outstanding deficiencies in relation to their combined effect on the suitability of the system for hand-over for actual operation, service delivery;

4) Providing an initial determination as to whether PSA may be granted. If PSA is not granted, establishing the basis for such determination. If PSA is granted, establishing the final list of deficiencies which shall be corrected by the Contractor prior to Final System Acceptance and a schedule for such corrections to take place.

SAC-9 The Contractor shall prepare a written record of the PSA Review in the form of PSA Meeting minutes and submit to the Purchaser, within 1 week of the meeting.

SAC-10 This PSA Review minutes shall be completed and signed by the representatives of the Contractor and Purchaser respectively.

SAC-11 The PSA Review Minutes shall be forwarded to the Purchaser's Contracting Authority who will formal ise the decisions of the PSA Meeting in writing and officially notify the Contractor of such decisions within two (2) weeks of receipt of the PSA Minutes.

SAC-12 The Contractor shall note that any Certificate of Conformity provided at the time of the PSA meeting is considered to also be provisional pending correction of noted deficiencies before Final System Acceptance.

10.2 FINAL SYSTEM ACCEPTANCE (FSA)

[197] Final System Acceptance (FSA) is the act by which the Purchaser has evaluated and determined that the implemented TDCIS System meets the requirements of the Contract, and that the Contractor has fully delivered all requirements.

SAC-13 To achieve FSA, the Contractor shall demonstrate the following:

1) The Contractor has met all of the PSA milestone requirements to be implemented under this contract;

2) The Customer has successfully completed OpTEval, with Contractor support;

3) The Contractor has executed all milestones and all implementation activities in accordance with this document to be implemented under this contract;

4) The Contractor has delivered a complete and updated set of documents;

5) The Contractor has executed all agreed test cases, and all tests shall have a status “PASS”;

6) All the identified deficiencies are either fixed or waived by the Purchaser;

7) All training sessions have been conducted to the satisfaction of the Purchaser’s staff participating in the sessions;

8) Any regression testing of any changes resulting from OpTEval activities has been completed;

9) The Contractor has delivered all deliverables, and conduct all activities, as specified in this contract;

10) The Contractor shall close to the satisfaction of the Purchaser all outstanding issues, failures, and deficiencies;

11) The Contractor shall update the training material as required, based on the Training Evaluation report and the training feedback from the OpTEval.

[198] A FSA meeting will be conveyed and chaired by the Purchaser when he considers that the deliverables are ready for Final Acceptance.

[199] The achievement of FSA is subject to the Purchaser approval.

SAC-14 The FSA Report shall include the following documentation:

1) FSA Meeting Agenda;

2) OpTEval Report;

3) FSA Observations sheet;

4) Final In-Service Support Plan (ISSP);

5) Final Support case;

6) Final System Inventories;

7) Final Software Distribution List (SWDL);

8) Final Quality Assurance Log;

9) Final Configuration Status Accounting (CSA) Reports;

10) Configuration Management Database (CMDB), containing the Final Baseline Configuration (FBC), down to component-level configuration files (part of the TDCIS OBL);

11) Complete Requirements Management Database, in electronic form (e.g. USB or CD/DVD).

SAC-15 The FSA Observations sheet shall be the log of any discrepancies and omissions carried over from PSAs and/or raised during the OpTEval, and not qualifying as off-specifications. These shall be listed together with a statement on the proposed resolution and resolution timeline (for discrepancies) or rationale for accepting them (for omissions), prior to declaring FSA.

APPENDIX A REFERENCE DOCUMENTS

A.1 APPLICABLE DOCUMENTS

A.1.1 INTEGRATED PRODUCT SUPPORT

The Contractor shall apply policies and standards contained within following documents in matters relating to the project's Integrated Product Support (IPS).

1) STANAG 4728 System Life Cycle Management – Ed.2 (2015).
2) AAP-20 NATO Programme Management Framework (NATO Life Cycle Model) – Ed.C, Ver.1 (2015)
3) AAP-48 NATO System Life Cycle Processes – Ed.B, Ver.1 (2013)
4) STANAG 4597 Obsolescence management – Ed.2 (2010)
5) STANAG 6001 Language Proficiency Levels – Ed.5 (2014)
6) STANAG 4280 NATO Levels of Packaging - Ed.2 (1999)
7) STANAG 4281 NATO Standard Marking for Shipment and Storage - Ed.3 (2016)
8) STANAG 4329 NATO Standard Bar Code Symbologies – AAP-44(A) – Ed.4 (2010)
9) STANAG 4329 NATO Standard Bar Code Symbologies – AAP-44(A) – Ed.4 (2010)

A.1.2 CONFIGURATION MANAGEMENT

The Contractor shall apply policies and standards contained within following documents matters relating to the project's Configuration Management (CM).

1) STANAG 4427 Configuration Management in System Life Cycle Management – Ed.3 (2014)
2) ACMP-2000 Policy on configuration management – Ed.A, Ver.2 (2017)
3) ACMP-2009 Guidance on Configuration Management – Ed.A, Ver.2 (2017)
4) ACMP-2100 The Core Set of Configuration Management Contractual Requirements – Ed.A, Ver.2 (2017)
5) ISO 10007:2003 Quality Management System – Guidelines for Configuration Management. Second edition, 2003

A.1.3 QUALITY MANAGEMENT

The Contractor shall apply policies and standards contained within following documents in matters relating to the project's Quality Assurance (QA).

1) AQAP-169 NATO Guidance on the Use of AQAP-160 Edition 1, Edition 1, July 2001, NU
2) AQAP-160 NATO Integrated Quality Requirements for Software throughout the Life Cycle, Edition 1, July 2001, NU

3) STANAG 4107, Ed.11 Mutual Acceptance of Government Quality Assurance and Usage of the Allied Quality Assurance Publications. Ed.11, 2019
4) AQAP-4107 Mutual Acceptance of Government Quality Assurance and Usage of the Allied Quality Assurance Publications (AQAP). Ed. A, Ver.2, 2018
5) STANAG 4107, Ed.11 Mutual Acceptance of Government Quality Assurance and Usage of the Allied Quality Assurance Publications. Ed.11, 2019
6) AQAP-4107 Mutual Acceptance of Government Quality Assurance and Usage of the Allied Quality Assurance Publications (AQAP). Ed. A, Ver.2, 2018
7) NATO AQAP-2009 NATO – Allied Quality Assurance Publication 2009, "NATO guidance on the use of the AQAP 2000 series", Edition 3, 2010
8) AQAP-2070 NATO Mutual Government Quality Assurance (GQA). Ed.B, Ver.3, 2015
9) AQAP-2105 NATO Requirements for Quality Plans. Ed.C, Ver.1, 2019
10) AQAP-2110 NATO Quality Assurance Requirements for Design, Development and Production. Ed.D, Ver.1, 2016
11) NATO AQAP-2120 NATO – Allied Quality Assurance Publication 2120, "NATO QA requirements for production", Edition 3, 2010
12) AQAP-2131 NATO Quality Assurance Requirements for Final Inspection and Test. Ed.C, Ver.1, 2017
13) AQAP-2210 NATO Supplementary Software Quality Assurance Requirements to AQAP-2110 or AQAP-2310. Ed.A, Ver.2, 2015
14) AQAP-2310 NATO Quality Assurance Requirements for Aviation, Space and Defence Contractors. Ed.B, Ver.1, 2017
15) IEEE 12207 Systems and Software Engineering – Software Life Cycle Processes International Standard For Software Lifecycle Processes
16) IEEE 15288.2-2014 Standard for Technical Reviews and Audits on Defence Programs

A.1.4 DCIS CUBE ARCHITECTURE

The Contractor shall apply policies and standards contained within following documents in matters relating to the project's DCIS Cube Architecture.

1) DCIS Cube ADD Main, 2018 DCIS Cube Architecture Definition Document", Version 1.0, NCIA/TR/2018/02530, NCI Agency, The Hague, Netherlands, 8 May 2018
2) DCIS Cube ADD Annexes, 2018 DCIS Cube Architecture – Annexes, DCIS Cube CBB and Dependencies on External ABB, Version 1.0, Annex to NCIA/TR/2018/02530, NCI Agency, The Hague, Netherlands, 8 May 201

A.1.5 VM WARE SECURITY

The Contractor shall apply policies and standards contained within following document in matters relating to the project's Security.

1) Vmware ESXi 6.5 Security Settings, 2018 Security Settings for VMware ESXi 6.5 Description and Values, Version 1.0, June 2018, NCI Agency, Mons, Belgium (NATO Unclassified)

A.2 REFERENCE DOCUMENTS

A.2.1 INTEGRATED PRODUCT SUPPORT

The Contractor shall refer to guidance and instructions contained within following documents in matters relating to the project's IPS.

1) ISO/IEC 15288, 2015, Systems and software engineering -- System life cycle processes
2) ISO/IEC 12207, 2008, Systems and software engineering -- Software life cycle processes
3) ISO/IEC 25010, 2011, Systems and software engineering — Systems and Software Quality Requirements and Evaluation (SQuaRE) — System and software quality models
4) IEC 60050, International Electrotechnical Vocabulary (IEV) (www.electropedia.org)
5) IEC 61078:2016, Reliability Block Diagrams
6) IEC 60706-3:2006, Maintainability of equipment - Part 3: Verification and collection, analysis and presentation of data
7) IEC 60812:2018, Failure modes and effects analysis (FMEA and FMECA)
8) IEC 62550:2017, Spare parts provisioning
9) AIA/ASD SX000i, International specification for Integrated Product Support (IPS) – Issue 3.0 (2021)
10) AIA/ASD S3000L, International procedure specification for Logistics Support Analysis (LSA) – Issue 2.0 (2021)
11) AIA/ASD S2000M, International Specification for Material Management. Issue 7.0 (2021)
12) AIA/ASD S1000D, International Specification for Technical Publications. Issue 4.0.1 (2009)
13) MIL-HDBK-338B, Electronic Reliability Design Handbook
14) MIL-STD-756B, Reliability Modeling and Prediction
15) MIL-HDBK-470A, Designing and Developing Maintainable Products and Systems
16) MIL–STD–1629A, Procedures for performing a Failure Mode, Effects and Criticality Analysis
17) Telcordia SR-332, Reliability Prediction Procedure for Electronic Equipment
18) HDBK-217Plus, Reliability Prediction Models
19) ANSI VITA51, Reliability Prediction MIL-HDBK-217F2 Subsidiary Specification
20) ASME Y14.44 - 2008, Reference Designations for Electrical and Electronics Parts and Equipment
21) Bi-SC Directive 075-003, Collective Training and Exercise Directive, 02 October 2013, NU

22) Bi-SC Directive 075-007, Education and Individual Training Directive, 10 September 2015, NU
23) NATO C3 Taxonomy Enclosure 1 to AC/322-D(2016)0017, “C3 Taxonomy Baseline 2.0”, 10 November 2015
24) AI 16.31.10, NCIA Agency Instruction – Spare parts provisioning
25) AI 16.31.07, NCIA Agency Instruction – Guidance Document (GD) for ASD-AIA-ATA S1000D Technical Publications, with the associated S1000D Issue 4.0.1 Business Rules Decision Points (BRDP) Index
26) AI 16.31.12, NCIA Agency Instruction – Writing Style Guide (WSG) for ASD/AIA/ATA S1000D Technical publications
27) AI 16.31.13, NCIA Agency Instruction – Illustration Style Guide (ISG) for ASD/AIA/ATA S1000D Technical publications

A.2.2 APPROVED FIELDED PRODUCT LIST

The Contractor shall refer to guidance and instructions contained within following documents in matters relating to the project’s Approved Fielded Products.

1) AFPL, Approved Fielded Product List, relevant to the NGCS (also known as NGCS AFPL), “NGCS AFPL 06 July 2022.xls”.

2) AAP-44(A), NATO Standard Bar Code Handbook, September 2010, NATO non-classified

A.2.3 TESTING

1) ISO/IEC/IEEE 29119-1:2013, Software and systems engineering — Software testing — Part 1: Concepts and definitions
2) ISO/IEC/IEEE 29119-2:2013, Software and systems engineering — Software testing — Part 2: Test processes
3) ISO/IEC/IEEE 29119-3:2013, Software and systems engineering — Software testing — Part 3: Test documentation
4) ISO/IEC/IEEE 29119-4:2015, Software and systems engineering — Software testing — Part 4: Test techniques
5) ISO/IEC 25010-2011, Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models
6) IEEE Standard 15288.2:2014, IEEE Standard for Technical Reviews and Audits on Defense Programs
7) IEEE Standard 1016-2009, IEEE Standard for information technology - systems design - software design descriptions

A.2.4 CONFIGURATION MANAGEMENT

The Contractor shall refer to guidance and instructions contained within following documents in matters relating to the project’s CM.

1) SAE ANSI/EIA-649C, Configuration Management Standard (2019-02-07)
2) AI 16.32.04, NCIA Agency Instruction – ABL Template
3) AI 16.32.05, NCIA Agency Instruction – PBL Template
4) AI 16.32.02, NCIA Agency Instruction – Preparation of ECP forms and relevant annex
5) AI 16.32.03, NCIA Agency Instruction – Preparation of RFD/W forms and relevant annex

A.2.5 TRAINING

The Contractor shall refer to guidance and instructions contained within following documents in matters relating to the project's Training Products.

1) Bi-SC Directive 075-003, Collective Training and Exercise Directive, 02 October 2013, NU
2) Bi-SC Directive 075-007, Education and Individual Training Directive, 10 September 2015, NU
3) NATO C3 Taxonomy, Enclosure 1 to AC/322-D(2016)0017, "C3 Taxonomy Baseline 2.0", 10 November 2015

A.2.6 NATO SECURITY

The following NATO Security documents shall be applicable:

1) Security within the North Atlantic Treaty Organisation (C-M(2002)49), COR 12, dated 14 September 2015;
2) Directive on Personnel Security (AC/35–D/2000–REV7), dated 07 January 2013;
3) Directive on Physical Security (AC/35–D/2001–REV2), dated 07 January 2008;
4) Directive on Security of Information (AC/35–D/2002–REV4), dated 17 January 2012;
5) Directive on Classified Project and Industrial Security (AC/35–D/2003–REV5), dated 13 May 2015;;
6) Primary Directive on CIS Security (AC/35-D/2004-REV3), dated 15 November 2013
7) Management Directive on CIS Security (AC/35-D/2005-REV3), dated 12 October 2015;
8) INFOSEC Technical & Implementation Directive on Cryptographic Security and Cryptographic Mechanisms (AC/322-D/0047-REV2 (INV), NATO RESTRICTED, dated 11 March 2009;
9) INFOSEC Technical & Implementation Directive for Computer and Local Area network (LAN) Security (AC/322-D/0048-REV3), NATO RESTRICTED, 18 November 2019;
10) INFOSEC Technical & Implementation Directive on Emission Security (AC/322-D(2007)0036), NATO RESTRICTED, dated 12 July 2007;
11) Guidelines for the Security Accreditation of CIS (AC/35-D/1021-REV3), dated 31 January 2003;

12) Guidelines for Security Risk Management (SRM) of Communication and Information Systems (CIS) (AC/35-D/1017-REV3), dated 29 June 2017;
13) Guidelines for the Development of Security Requirement Statements (SRSs) (AC/35-D1015–REV3), NATO RESTRICTED, 31 January 2012;
14) Guidelines for the Structure and Content of Security Operating Procedures (SecOPs) for CIS (AC/35-D/1014-REV3), dated 31 January 2012;
15) Guidelines for the Security Evaluation and Certification of Communication and Information Systems (CIS) (AC/35-D/1019-REV1), dated 12 December 2008;
16) INFOSEC Technical & Implementation Directive for the Interconnection of Communication and Information Systems (CIS) (AC/322-D/0030-REV5), NATO RESTRICTED, dated 23 February 2011;
17) INFOSEC Technical & Implementation Guidance for the Interconnection of Communication and Information Systems (CIS) (AC/322-D(2005)0040), dated 17 October 2005;
18) INFOSEC Technical and Implementation Directive on the requirement for, and the Selection, Approval and Implementation of Security Tools (AC/322-D(2004)0030, NATO RESTRICTED, dated 17 May 2004;
19) INFOSEC Technical and Implementation Guidance for the Protection of CIS from Malicious Software (AC/322-D(2004)0019(INV), dated 09 March 2004;
20) INFOSEC Technical and Implementation guidance on Identification and Authentication (AC/322-D(2005)0044), NATO RESTRICTED, dated 26 October 2005;
21) INFOSEC Technical & Implementation Directive for Transmission Security (AC/322-D/0049), NATO RESTRICTED, dated 29 April 2002;
22) INFOSEC Technical and Implementation Guidance for Electronic Labelling of NATO Information (AC/322-D(2004)0021), dated 16 March 2004;
23) NATO Public Key Infrastructure (NPKI) Certificate Policy (AC/322-D(2004)0024-REV2-AS1), dated 18 January 2008;
24) Security Configuration Catalogue, NCI Agency Cyber Security Service Line, v.1.10, dated April 2018[17];
25) NATO S*CR*T CIS Security Reference Baseline, Security Mechanisms (SMs) Requirements for Core and Site Services, version 2.0, dated 05 July 2017.

A.2.7 NATO TEMPLATES

The following NATO Templates are applicable:

1) Security Accreditation Plan Template, version 4.0, dated 08 July 2016;
2) CIS Description Template, version 2.1, dated 02 May 2017;
3) Security Risk Assessment (SRA) Report (NATO PILAR) Template, version 1.0, dated January 2013;

[17] New version might be provided upon contract award if available.

4) System Security Requirements Statement (SSRS) Template, version 5.0, dated 12 January 2018;
5) Abbreviated System Interconnection Security Requirements Statement (A-SISRS) Template, version 1.0, dated 19 September 2017;
6) Secure AIS Generic SecOPs, version 1.0 dated 20.05.2014;
7) Generic Security Test & Verification Plan, version 1.0, dated 17 February 2014;
8) Electronic Security Environment Conformance Statement (ESECS) Template, dated 05.02.2018;
9) Approval for Test Request Template, dated 23.01.2017.

APPENDIX B PURCHASER FURNISHED EQUIPMENT

Table Annex 14 – Equipment to be provided to the Contractor – **Refer to Annex A herein**

Table Annex 15 - Antenna to be provided to the Contractor – **Refer to Annex A herein**

[1] The design, production, testing and acceptance phases will include the integration of, and the interaction with, Purchaser Furnished Equipment (PFE) equipment.

[2] PFE is the general term used throughout this document. PFE includes Purchaser Furnished:

a. Equipment;

b. Information;

c. Software;

d. Configuration;

e. Connectivity;

f. SMEs (Access to); and

g. Facilities (e.g. Office space during CCT).

[3] Two classes of PFE are considered:

a. PFE that is handed over by the Purchaser to the Contractor, for integration INTO systems delivered under this contract.;

b. PFE staged and operated by the Purchaser, in the context of FAT, IV&V Assessment, SAT and OpTEval, for integration WITH the system delivered under this contract.

[4] The following table provides the list of PFE. The following paragraphs provide additional details on the integration aspects (for both the INTO and WITH variants described above)

Appendix Table 1 PFE Integration Approach

PFE	Parent System	Integration	Remarks
IP crypto	CNM	INTO	Integrated prior to FAT and after delivery of Batch 1 and Batch 2
End User Phones	UAM	WITH	Phones other than System Administrator Phones
End User Workstations	UAM	WITH	Workstations other than

PFE	Parent System	Integration	Remarks
			System Administrator Workstations
Military SATCOM bandwidth	Military SATCOM	WITH	Provides SATCOM connectivity for SAT and OpTEval
Commercial SATCOM bandwidth	Commercial SATCOM	WITH	Provides SATCOM connectivity for SAT and OpTEval
Business Support Services (applications)	ISM	INTO	SRS identified PFE Applications to be loaded into the ISM
COI Services (applications)	ISM	INTO	SRS identified PFE Applications to be loaded into the ISM
CIS Security Services (applications)	ISM SysAdmin Workstations	INTO	SRS identified PFE Applications to be loaded into the ISM and SysAdmin Laptops
Transport Vehicles	All	WITH	Includes motor vehicles and pallets, containers. Includes OLRT vehicle.
Iridium PTT integration station	Nodes appointed in the SRS	INTO	N/A
IP HF Radio	Nodes appointed in the SRS	INTO	Including anciliaries
CNR Radio	Nodes appointed in the SRS	INTO	Including ancilliaries

B.1 INTEGRATION OF PFE

[5] Delivery and integration of PFE crypto devices will occur over the life of the Project;

a. Upon CDR approval, for PFE integration into the First Articles subject of Qualification Testing (QT) and Factory Acceptance Testing (FAT);

b. Upon approval of the FAT, for PFE integration into Batch 1 and Batch 2 units, for Site Acceptance Testing (SAT) and Operational Test and Evaluation (OpTEval).

B.2 INTEGRATION WITH PFE

[6] Integration of the systems delivered under this Contract with PFE systems configured and operated by the Purchaser is required for verification of system-level interfaces, encompassing physical connectivity and end-to-end connectivity.

[7] System-level integration and verification of end-to-end connectivity with or over the PFE systems shall be sought with the following:

a. PRT National Anchor Station;

b. The NATO Deployable Operations Gateway (DOG), to terminate links from the NS Kit;

c. All end user appliances (NU, NS and MS), all equipped with 1 GbE interfaces.

B.3 ACCESS TO DCIS SMES

[8] The Purchaser will enable knowledge transfer process during the CCAP sessions, by providing access to PRT and NCIA Subject Matter Experts (SME), and to documentation.

[9] Coordination for the provision of the PFE – SMEs, shall be agreed with the Purchaser.

B.4 ACCESS TO IVV TOOLS

[10] Requirements Coverage, Defect Management and Test Management tools to be used in this project will be hosted by the Purchaser.

[11] The Purchaser will grant access to the above tools to an agreed number of individuals nominated by the Contractor.

[12] Details of the tools will be made available after Contract Award.

APPENDIX C MAINTENANCE AND SUPPORT CONCEPTS

C.1 MAINTENANCE CONCEPT AND MAINTENANCE LEVELS DEFINITION

C.1.1 Definitions

In accordance with [ASD SX000i], Maintenance is an activity that retains or restores a physical item to a specified condition or level of performance.

Training is linked to the Logistic Support Analysis (LSA) discipline through the Operational Task Analysis (OTA) and Maintenance Task Analysis (MTA), the former being determined by the Concept of Operation (CONOPS) and the latter being determined by the Maintenance Concept applicable to the specific product under acquisition.

A maintenance concept is a statement of maintenance considerations, constraints, and strategy for the operational support that governs the maintenance levels and type of maintenance activities to be carried out for the product under analysis. The maintenance concept is generated in the IPS element, "Maintenance".

The Maintenance concept, in turn, is derived from the Concept of Operations (CONOPS, see paragraph 6.4) and is a major driver in product design and support.

In accordance with [IEC 60050]:

1) Level of maintenance/maintenance level: set of maintenance actions to be carried out at a specified indenture level;
2) Indenture level: level of sub-division within a system hierarchy.

Maintenance, maintenance levels and maintenance tasks are product-related (linked to the system hierarchy[18]) and are defined in accordance with the complexity of the task, the required resources and tools, independently from the maintenance organization.

Maintenance supports (sustains) operation: any action required to restore the operation of a system or to ensure operational status can be maintained over time is a maintenance task; a maintenance task becomes a support task when it is associated to an organizational element of the support organization in charge of that task at the defined level.

Further definitions follow (IEC 60050):

1) Maintenance – (191-07-01): The combination of all technical and administrative actions, including supervision actions, intended to retain an item in, or restore it to, a state in which it can perform a required function.
2) Maintenance policy – (191-07-03): A description of the interrelationship between the maintenance echelons, the indenture levels and the levels of maintenance to be applied for the maintenance of an item.
3) Indenture level – (191-07-05): Level of sub-division within a system hierarchy from the point of view of a maintenance action. E.g.: System, subsystem, assembly, and component (see

[18] The different types of systems' hierarchies (physical, functional, hybrid) are defined in [ASD S3000L] as Product Breakdown Structures (PBS).

also MIL-HDBK-505). [Note: from the maintenance perspective, the indenture level depends upon various factors, including the complexity of the item's construction, the accessibility of sub items, skill level of maintenance personnel, test equipment facilities, and safety considerations.]

4) Maintenance echelon or line of maintenance – (191-07-04): A position in an organization where specified levels of maintenance are to be carried out on an item.
5) Level of maintenance or maintenance level – (191-07-06): Set of maintenance actions to be carried out at a specified indenture level

C.1.2 Maintenance Concept

A Maintenance Concept is a definition of the maintenance objectives, line of maintenance, indenture levels, maintenance levels, maintenance support and their interrelationships.

A Maintenance Concept is applied for both HardWare (HW) and SoftWare (SW) and produces maintenance tasks that will be performed on site, at civil or military maintenance facilities, at industry (Original Equipment Manufacturer, Contractor) maintenance facilities.

The Maintenance Concept identifies who-does-what-at-what-level in accordance with the maintenance levels and definitions defined below.

Maintenance levels, indenture levels, maintenance echelons (etc.) are always product-related.

C.1.3 Maintenance echelon (line of maintenance)

A Maintenance echelon is the position in an organization where specified levels of maintenance are to be carried out. The line of maintenance is characterized by the skill level of the personnel, the facilities and tools provided, the location, etc.

Four (4) maintenance echelons are generally defined to ensure the highest possible availability of the Product.

1) Level 1: implies fast and easy activities on MSIs/MRIs (see [ASD S3000L]) performed on-site for preventative or corrective actions on the acquired System/Capability;
    a. Typology: without the need to remove the item from its existing installations on the Product;
    b. Accessibility: easy (e.g.: general visual inspection for hardware, launch of common routines or macros for software);
    c. Location: operating location (e.g. on-site, deployed location, on-ship);
    d. Tools: common hand tools and/or common test equipment;
    e. Facility: nil.
2) Level 2: implies more complex activities on MSIs/MRIs performed on-site including the replacement of modules using standard and special-to-type tools, BITE, limited troubleshooting on the acquired System/Capability;
    a. Typology: it may be necessary to remove the item from its existing installation on the Product;

   b. Accessibility: may be difficult (e.g.: rear access or tight plug and unplug for hardware, backup and restore for software);
   c. Location: operating location (e.g. on-site, deployed location, on-ship);
   d. Tools: common hand tools, common support equipment, and/or peculiar support equipment;
   e. Facility: nil

3) Level 3: implies the repair of subassemblies, modules and MSIs/MRIs after their replacement at maintenance Level 1 and Level 2; testing on test-benches or integration tests can be included. This maintenance level can be performed either on product (e.g. on-site) or at specific repair shops/facilities (off-site);
   a. Typology: it is necessary to remove an item from its existing installation on the Product;
   b. Accessibility: item dismounted from its existing installation on the Product and available for any kind of manipulation;
   c. Location: NATO maintenance location that may be either located or not located in proximity of the operating location;
   d. Tools: as required by the NATO maintenance location;
   e. Facility: specialized repair shop, software reference systems, etc

4) Level 4: includes repairs and overhaul activities beyond Level 1 to Level 3 capabilities (e.g.: repair of subassemblies, modules and MSIs/MRIs after their replacement at maintenance Level 1 to Level 3; major modifications to improve the design and/or operational activities will be prepared and, if necessary, embodied at this level). Level 4 is always off-site (generally at OEMs facilities).
   a. Typology: it is necessary to remove an item from its existing installation on the Product;
   b. Accessibility: item dismounted from its existing installation on the Product and available for any kind of manipulation;
   c. Location: Contractor/OEM maintenance location located at Industry premises;
   d. Tools: as required by the Contractor/OEM maintenance location;
   e. Facility: repair centre, software development laboratory, etc.

While performing the Maintenance Task Analysis (MTA), each maintenance task shall be analysed to determine the echelon at which the task shall be performed.

C.1.4 Hardware Maintenance

Hardware maintenance is generally categorised/grouped as follows

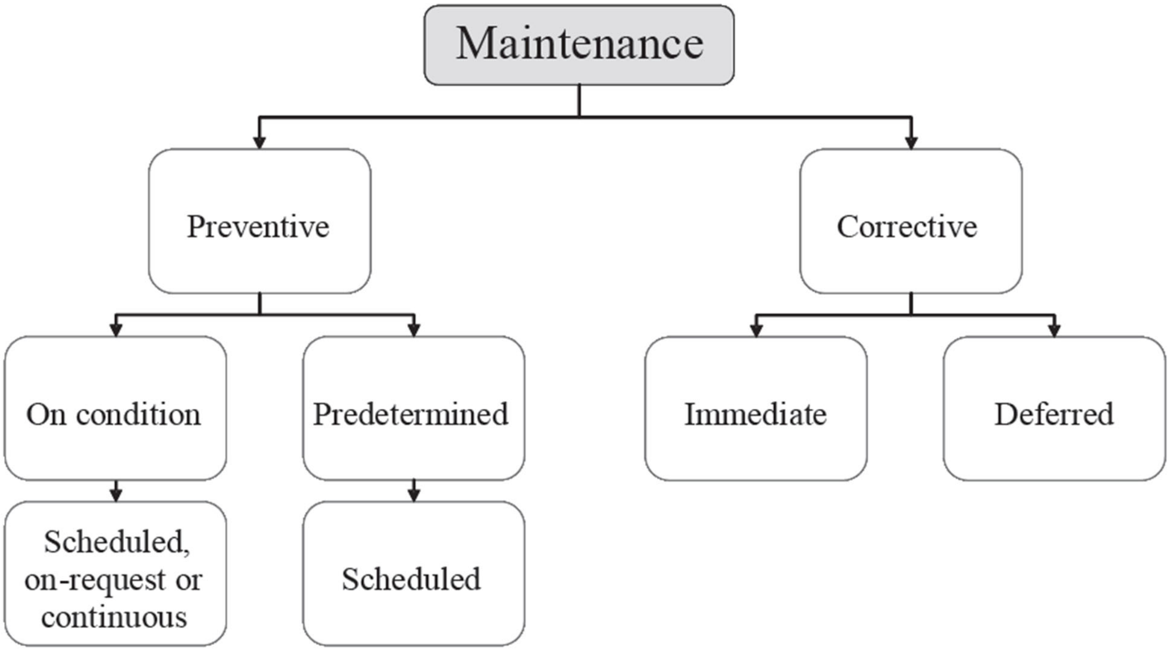


Figure Maintenance types (source: EN 13306:2001)

1) Preventative/Scheduled (HW maintenance):

   a. On-condition: maintenance carried out to mitigate degradation and reduce the probability of failure after analysis of system conditions through defined indicators assessed on a periodic basis.

   b. Scheduled (planned): maintenance carried out on a periodic basis (time-related or number-of-occurrences-related).

2) Corrective/Unscheduled (HW maintenance):

   a. Run-to-failure: maintenance carried out to perform a Remove & Replace action of a faulty item affecting system operation (critical failure). The action is done as soon as all the resources (skills, tools and spares) are available to minimise the System downtime.

   b. Deferred: maintenance carried out to perform a Remove & Replace action of a faulty item not affecting system operation. It is done in a time slot that does not further impact the Operational Availability (e.g. during a schedules maintenance downtime period) or on “live” equipment if this is possible (e.g. when active redundancy or hot stand-by are implemented).

The hardware maintenance is classified in four levels generally known as HL1, HL2 HL3 and HL4.

1) **Hardware Organizational Maintenance Level 1 (HL1)** is Hardware maintenance capable of being carried out:

   a. On-site;

   b. By relatively low technical skill level personnel performing preventive maintenance, and replacing LRUs and IIs on the basis of diagnostic outputs;

c. Using BIT systems for start-up and on-line diagnostics, by referring to main equipment TM;

d. No Special Tools and Test Equipment (TTE) are envisioned to be used;

e. Typical tasks will include visual inspection, preventative maintenance tasks, manual reconfiguration if necessary, external adjustments, removal and replacement of LRUs/IIs;

f. Includes system failure recovery by the application of simple on-line diagnostics or technician initiated restart of the system and the use of off-line diagnostics which do not require external test module support;

g. By generation of equipment failure reports, supply requisitions and other pertinent maintenance and supply records.

2) **Hardware Organizational Maintenance Level 2 (HL2)** is Hardware maintenance capable of being carried out:

a. On-site;

b. By higher technical skill level personnel performing preventive maintenance and replacing LRUs and IIs on the basis of diagnostic outputs;

c. Using BIT systems for start-up and on-line diagnostics, simple TTE (standard and special-to-type) in addition to BIT as a means for on-line and off-line diagnostics, and by referring to main equipment TMs to perform exhaustive fault isolation;

d. Simple either commercial or special-to-type TTE are envisioned to be used (e.g.: screwdrivers, multi-meters, oscilloscope, adapters, peculiar support equipment);

e. Where the fault is beyond the capabilities of HL1 technical support, HL2 activities will be performed by Support Site personnel (through on-site intervention);

f. Where remote fault management is not feasible, technicians from the host site will travel to the remote site hand carrying relevant spares to perform maintenance tasks;

g. By generation of equipment failure reports, supply requisitions and other pertinent maintenance and supply records.

3) **Hardware Intermediate Maintenance Level 3 (HL3)** is Hardware maintenance capable of being carried out:

a. At maintenance facilities and through technical support and assistance or on-site intervention/work by maintenance personnel with skills enabling tasks to be accomplished within the relevant technologies;

b. By higher technical skill level personnel performing:

i. Repairing, testing and calibrating LRU, Shop Replaceable Units (SRU) and Secondary Spare Parts (SSP);

ii. On-site investigations and major scheduled servicing/overhaul, detailed inspection, major equipment repair, major equipment modification, complicated adjustments, system/equipment testing;

iii. Failure trend analysis including reporting to relevant Purchaser authorities and Post Design Services (PDS);

iv. Repair tasks will be performed using Automatic Test Equipment (ATE), general purpose and special-to-type TTE, calibration equipment, any applicable support software, and the necessary equipment TMs and a Technical Data Package (TDP);

v. Where the fault is beyond the capabilities of HL1/2 technical support, HL3 activities will be performed by support site personnel (through on-site intervention) or by the Contractor, depending on the maintenance concept;

vi. It includes generation of equipment failure reports, supply requisitions and other pertinent maintenance and supply records.

4) **Hardware Depot Maintenance Level 4 (HL4)** is Hardware maintenance capable of being carried out:

   a. At maintenance facilities (industry or military, original equipment manufacturers) and through technical support and assistance or on-site intervention/work by maintenance personnel with skills enabling tasks to be accomplished within the relevant technologies;

   b. Where the fault is beyond the capabilities of HL1-3 technical support, HL4 activities will be performed by the Contractor;

   c. It includes generation of equipment failure reports, supply requisitions and other pertinent maintenance and supply records.

C.1.5 Software Maintenance

The software maintenance is a task for the purposes of software fault removal, adaptation to a new environment, or improvement of performance.

The software maintenance for the purposes of software fault avoidance, identification and/or removal can be:

1) **Preventative/Scheduled (SW maintenance)**: it refers to tasks necessitated for detecting potential errors in a software product or anticipate and avoid potential failures (daily checks, DBs clean up/integrity checks, cache cleaning, rebooting/restarting etc.). The task can lead, if latent failures are discovered, to a modification of a software product after delivery to detect and correct latent faults in the software product before they become effective faults (leading to a deferred corrective action).

2) **Corrective/Unscheduled (SW maintenance)**: it refers to tasks necessitated by actual errors in a software product. If the software product

does not meet its requirements, corrective maintenance is performed. It is a Reactive modification of a software product performed after a new version is made available (patch/update) to correct the discovered problem(s). This activity is linked to Configuration Management, change management (contractor initiated Engineering Change Proposals - ECP), new SW release(s) and Product baseline (PBL) change.

The software maintenance for the purposes of software adaptation to a new environment, or improvement of performance is a software change that enhances the software product. These changes are those that were not in the original design specifications or in the originally released software and are subject to purchaser initiated ECP:

1) **Adaptive maintenance**: software maintenance for the purposes of adaptation to a new environment (e.g.: a new environment could be a new type of hardware or a new operating system on which the software is to be run). Adaptive refers to a change necessary to accommodate a changing environment. Adaptive changes include changes to implement new system interface requirements, new system requirements, or new hardware requirements. This is a modification of a software product performed after delivery to keep a software product usable in a changed or changing environment.
2) **Perfective maintenance**: software maintenance performed to improve the performance, maintainability, or other attributes of a computer program (e.g.: maintenance that adds new required functions is often referred to as enhancement). Perfective refers to a change that improves the software product's performance. A perfective change might entail providing new functionality improvements for users or reverse engineering to create maintenance documentation that did not exist previously or to change existing documentation. This is a modification of a software product after delivery to improve performance or maintainability.

The software maintenance is classified in four levels generally known as SL1, SL2 SL3 and SL4.

1) Software Organizational Maintenance Level 1 (SL1) is software maintenance carried out with the same characteristics highlighted for HL1. SL1 are those functions/tasks in support of the on-site software that are within the capabilities of site maintenance personnel. This includes software failure recovery by the application of simple diagnostics, or site maintenance personnel initiated restart.
2) Software Organizational Maintenance Level 2 (SL2) is software maintenance carried out with the same characteristics highlighted for HL2. E.g.: software settings, simple software customizations (per site/instance), software reloading/installation with automated or detailed procedures reported in the TMs, execution of scripts, and management of users/profiles. SL2 are those functions/tasks in support of the on-site software that are within the capabilities of a System Administrator.
3) Software Intermediate Maintenance Level 3 (SL3) is software maintenance carried out with the same characteristics highlighted for HL3. E.g.: software/firmware fine tuning (per site/instance), software/firmware bugs recording and reporting, software/firmware troubleshooting including Operating Systems. SL3 (on-site intervention)

comprises those functions/tasks in support of the on-site software that require specialist intervention (software System architects, SW programmers, experienced Systems' Administrators, Network specialists). The tasks can be performed either by software personnel visiting the site or by remote diagnostics if enabled by the product.

4) Software Depot Maintenance Level 4 (SL4) is software maintenance carried out with the same characteristics highlighted for HL4. E.g. software/firmware debugging, re-coding and testing (both in simulated and emulated environments), software/firmware patches creation and deployment. The tasks can be performed by software engineers in properly configured environments (software development and testing facilities) under strict Configuration Control.

a) HL and SL are generally combined for HW intensive systems: when HW maintenance is required and SW shall be reloaded/set on replaced MSI/MRI, the maintenance level associated to the HW (HL) is also associated to the relevant SW (SL) and the activities are combined, detailed in the TMs and associated to the same personnel in the Support organization.

C.2 Support Concept and Support Levels definition

C.2.1 Definitions

The Support Concept is linked to the Maintenance concept and operation under the constraints dictated by the support organization (e.g. how NCI Agency is organised).

Maintenance concept	Support Concept	Product Support
Product related	Maintenance organization related	Project related
Level of maintenance (HW and SW)	Level of support	Maintenance policy
HL1-4 / SL1-4	*tipically* LoS1-4	
Complexity of the maintenance task related to actions of different technical complexity	Roles and responsibilities of the different support stakeholders	Maintenance levels carried out at different positions of the maintenance organization

The support concept is organization-related operation and maintenance: support and support levels indicate the different roles, skills and tools and the escalation process in place in an organization.

The interrelationship between the support levels/activities (maintenance organization-related) and the maintenance levels/activities (product-related) to be applied for the maintenance of each item into the system is the maintenance policy.

When capabilities are procured, the Contractor is able to design, develop and deliver the relevant system and apportion the maintenance tasks in accordance with their inherent complexity and in accordance with the maintenance concept; this apportionment, driven by the NCI Agency provided maintenance concept, shall then be allocated to NCI Agency support organizational elements.

If the Support Levels are not fully mapped/linked with the Maintenance Levels (e.g. the Contractor provided Maintenance Task Analysis), then “what shall be done by whom” in NCI Agency organization will be unknown.

The allocation of maintenance tasks to the support tasks (and therefore to the support organization at different levels of responsibility) is partially done by the contractor but shall be under the NCI Agency coordination among the main stakeholders involved in the delivery of training services.

Contractors generally define, tailor (design), develop and implement/deliver capabilities based on industry standards and eventually by customising products they have already in their catalogues: the “general” maintenance and operation activities are linked to the complexity of the capability and to the main functions such capability can deliver, therefore Industry is linked to Maintenance and Operation and not to Support and Use.

Being IPS product related, all the aspects relevant to support training (support organization related) will be defined jointly with other NCI Agency organizational elements (e.g. NCI Academy, NCIA Centres) in order to correctly allocate the maintenance tasks to the right support organization teams.

Further definitions follow [IEC 60050]:

1) Support Concept – a description that provides general considerations, constraints, and plans for interim and long-term sustainment of the item under analysis. The support concept is generated in the IPS element, "Product Support Management".
2) Maintenance support performance (execution of support) – 191-02-08: the ability of a maintenance organization, under given conditions, to provide upon demand, the resources required to maintain an item, under a given maintenance policy. [Note: the given conditions are related to the item itself and to the conditions under which the item is used and maintained.]

C.2.2 Support concept

A Support Concept is a definition of the support objectives (scenarios) in relation with maintenance levels, maintenance support and their interrelationships.

The support concept has the scope to translate the product-centric complexity, constraints and limitations into a fully sustainable support organization and System/Capability.

For specific “products”, support organizations might be quite similar if defined and developed following known frameworks (e.g. ITIL) or standards (e.g. ISO 20000); however, support organizations might be quite heterogeneous if the systems/capabilities to be maintained (supported) are of different types (e.g. encompassing the full C4ISR products family).

In addition, even applying consolidated support concepts based on pre-defined support levels, what shall be done in any case is the mapping of the organizational support teams to the support levels that, in turn, shall be mapped with the maintenance levels (see Annex A).

What follows below defines the support levels in accordance with ITIL V.3 framework and ISO 20000 and applies to NCI Agency for IT-intensive (centric) products.

There are four support levels and a level zero performed by the users that normally initiate the troubleshooting for the corrective maintenance.

1) **First level support** (on-site, non-specialised):

i. It consists of simple routine administration and activities. This level is user facing and is the first line of technical support. A single point of contact inside the NCI Agency central Service Desk is provided to customers for the implemented services. The Service Desk will log, categorise, prioritise, diagnose and resolve incidents within the boundaries of their training and permissions. The pertinent NCI Agency CIS Support Units (CSUs) carry out this level of support, in coordination with the NCI Agency Centralised Service Desk.

ii. The 1st Level Support Process implements the Incident Management process in accordance with the ISO/IEC 20000 and ITIL framework or equivalent;

iii. As part of the Incident Management, the Service Desk receives the issue from the user, puts it into a standard format (Trouble Ticket, TT), performs an initial assessment and distributes it to the predefined actors to solve it.

2) Second level support (centralised)

a) It provides escalated technical support to incident investigation and diagnosis. This level delivers advanced expertise to process services related to centralised system operations, fault isolation, system administration, management of maintenance services, system configuration, including reconfiguration of data sources and data connectivity to restore operations, assistance to first level and on-site support. This level performs end-to-end service monitoring and takes actions to resolve the incident and recover the services impacted.

b) The 2nd Level Support Process implements the Problem Management process in accordance with the ISO/IEC 20000 and ITIL framework or equivalent;

c) The Problem Management process receives the TT from the Service Desk and performs the following tasks:

d) Re-evaluation of TT category, criticality and priority,

e) Identification of the root cause of the issue (e.g. by issue replication testing),

f) Identification of workarounds,

g) Identification and initial planning of possible short, medium and long-term solutions (e.g. Workarounds, Patches, or new Baseline or CI Releases),

h) Create Problem Analysis Report and Change Request (CR) incl. schedule of implementation, and synchronisation with the Baseline Maintenance process;

i) Presentation of the Problem Analysis Report and CR to the Change Control Board (CCB) for approval,

j) Monitor and Control the approved CR during implementation,

k) Trigger 3rd Level Support and/or 3rd Level Maintenance process to implement the CR;

l) Perform the post- CR implementation review.

3) Third level support (centralised)

a) consists of central service management, central problem isolation and resolution, system-level maintenance, local repairs or spares provision, and management of deficiencies and warranty cases, beyond the capability of the second level support.

b) The 3rd Level Support Process implements the Deployment and Release Management process in accordance with the ISO/IEC 20000 and ITIL framework or equivalent.

c) The Deployment and Release Management process receives the approved Change Request from the 2nd Level Support and performs the following tasks:

d) Release of the solution (release unit/record)

e) Development of the solution (e.g. new CI Fix, Repair, Replacement, Patch, or Release),

f) Testing of the solution (e.g. Regression testing, issue/deficiency replication testing),

g) Update of Baseline content and status,

h) Delivery and deployment of the solution.

4) Fourth level support (OEM/vendor)

b) It consists of off-site factory/vendor problem resolution and maintenance, beyond the capability of third level support.

C.3 MAINTENANCE POLICY

NCIA and the contractor will contribute to the following mapping to correlate the support levels/activities (maintenance organization-related) and the maintenance levels/activities (product-related) to be applied for the maintenance of each item.

Appendix Table 2 Maintenance vs Support Mapping

System name:	[SystemName]	Support					Use
		Level 1 (L1S)	Level 2 (L2S)	Level 3 (L3S)	Level 4 (L4S)		
		Junior Tech	Senior tech	Sys Admin	OEM		

Operation								
Maintenance	Level 1	Hardware Level 1 (HL1M)						
		Software Level 1 (SL1M)						
	Level 2	Hardware Level 2 (HL2M)						
		Software Level 2 (SL2M)						
	Level 3	Hardware Level 3 (HL3M)						
		Software Level 3 (SL3M)						
	Level 4	Hardware Level 4 (HL4M)						
		Software Level 4 (SL4M)						

C.3.1 Operation and operators

In accordance with (IEC 60050), operation is the combination of all technical and administrative actions intended to enable an item to perform a required function, recognizing necessary adaptation to changes in external conditions.

To this extent operation is an enabling function and not a restoration function (is it not maintenance); in addition operation focuses on the (system/capability) required functions in a changing “environment” therefore it is intended to act on such functions by enabling, disabling, tuning, tweaking, optimising, changing and adapting such functions if and when required to answer, for example, to service demand changes.

So, in general, an operator (implementing the operation role) ensures that a capability is properly delivering its functions by monitoring, controlling, responding and setting the system in accordance with the required functions and current conditions.

In certain organizations (especially IT), this role is often associated to systems Administrators but generally a SysAdmin role is different and falls in the maintenance domain and not in the operation domain: a SysAdmin is able to administer the System and not (necessarily) to work on its functions.

Example: for a Surveillance Radar, the operator is the role responsible for enabling/disabling sectors, changing thresholds, changing operational modes etc. using an operator console (most of the times remoted w.r.t the Radar) where all the functions of the radar can be modified and optimised.

The system/capability operator is quite different from the system/capability user as well. The user benefits (directly or indirectly) from the functions delivered by the capability but is not an operator and might not know anything about the system functions optimization.

Being IPS product related, all the aspects relevant to operators training (system functions related) will be defined jointly with other NCI Agency organizational elements (e.g. NCI Academy, NCI Agency Centres).

C.3.2 Users and users’ needs

Although apparently linked to operators, the main document describing the users’ needs is the CONOPS (Concept of Operations).

A CONOPS "describes the proposed system in terms of the user needs it will fulfil, its relationship to existing systems or procedures, and the ways it will be used. CONOPS can be tailored for many purposes, for example, to obtain consensus among the acquirer, developers, supporters, and user agencies on the operational concept of a proposed system. Additionally, a CONOPS may focus on communicating the user's needs to the developer or the developer's ideas to the user and other interested parties” [Data Item Description DI-IPSC-81430].

CONOPS are complex documents that shall describe one or more systems composing one or more capabilities, their mission, operational scenario, interfaces, constraints, functionalities, quality elements, support organization associated to maintenance concept etc.

Not always a CONOPS is available or can be provided to contractors or is worth to be used by contractors for certain systems (or part of): in these cases, the contractual documents shall either provide an excerpt of the CONOPS or describe the essential elements required by the Contractors for building the right system (fit for use) and not only the system right (fit for purpose).

It shall be noted that there is a clear line of demarcation between operators and users: users are those elements in an organization that take benefit from the services delivered by the capability or benefit from its functions.

Example: for a Surveillance Radar, the Users are the Air Traffic Controllers (ATC) that generally have no knowledge about Radar Operation (e.g. how to set different radar modes, enable/disable functionalities etc.) or Radar maintenance or support.

Being IPS product related, all the aspects relevant to users′ training (doctrinal) will be left to other NCI Agency organizational elements (e.g. NCI Academy).

APPENDIX D KEY PERSONNEL REQUIREMENTS

[1] The table below lists the required certification and minimum experience that is to be met by Suitably Qualified and Experienced Personnel (SQEP) required to fill the Key Roles.

[2] In exceptional circumstances, extensive relevance experience may be considered instead of formal certification.

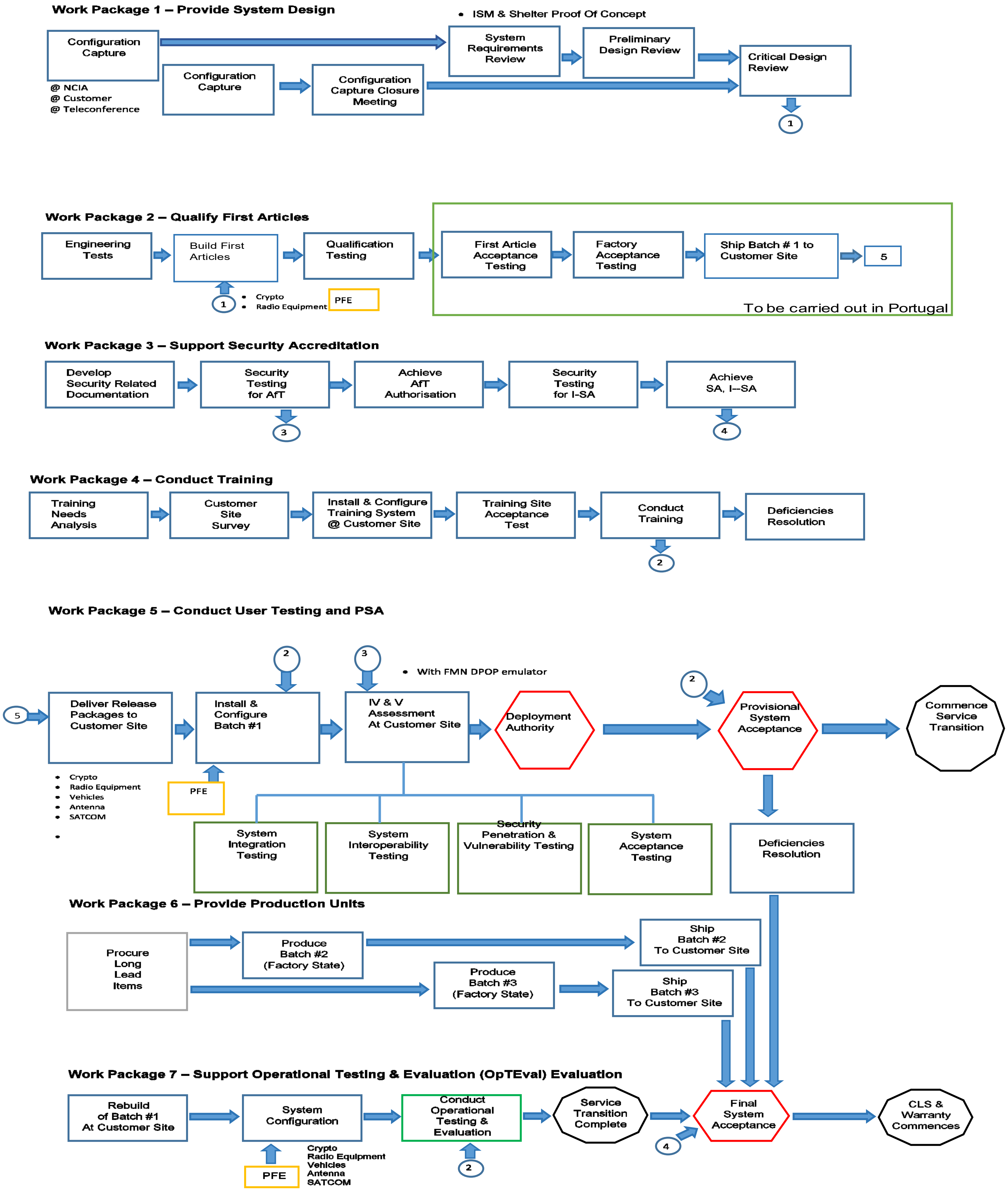
Appendix Table 3 Key Personnel Requirements

SER	KEY PERSONNEL	REQUIREMENTS
1	**Project Manager**	Responsible for project management, performance and completion of tasks and delivery orders. Establishes and monitors project plans and schedules and has full authority to allocate resources to insure that the established and agreed upon plans and schedules are met. Manages costs, technical work, project risks, quality, and corporate performance. Manages the development of designs and prototypes, test and acceptance criteria, and implementation plans. Establishes and maintains contact with Purchaser, Subcontractors, and project team members. Provides administrative oversight, handles contractual matters and serves as a liaison between the Purchaser and corporate management. Ensures that all activities conform to the terms and conditions of the Contract and Work Package procedures.
1.1	Certification	Master's degree in management, engineering, or business administration. Formal certification through Project Management Institute or equivalent source.
1.2	Experience	Must have experience of deployed systems with at least seven years in information systems design and project management. At least two years as the project manager for an effort of similar scope, preferably including the application of a formal project management methodology such as PRINCE2.
2	**Technical Lead**	Performs complex engineering tasks and multiple tasks simultaneously. Assists with or plans major research and engineering tasks or programs of high complexity. Directs and co-ordinates all activities necessary to complete a major, complex engineering program or multiple smaller tasks or programs. Performs advanced engineering research, hardware or software development.
2.1	Certification	Master's degree in engineering
2.2	Experience	Must have experience of deployed systems with at least seven years in engineering positions associated with the review, design, development, evaluation, planning and operation of electrical or electronic components, subsystems, or systems for government or commercial use. Member of recognised professional body.

SER	KEY PERSONNEL	REQUIREMENTS
3	**Test Director**	Directs test planning, design and tools selection. Establishes guidelines for test procedures and reports. Co-ordinates with Purchaser on test support requirements and manages Contractor test resources.
3.1	Certification	Bachelor's degree in engineering.
3.2	Experience	Must have experience of deployed systems with at least seven years in the design and execution of information systems tests.
4	**CIS Security Manager**	Analyses and develops network systems and information security practices to include: operating systems, applications, TCP/IP, security architecture, multi-level security, intrusion detection, virus detection and control, PKI, vulnerability assessment. Documents findings and recommend changes in procedures, configuration, or design.
4.1	Certification	Bachelor's degree.
4.2	Experience	At least three years in information systems security. At least five years in information systems integration, implementation, or operation.
5	**IPS Manager**	Provides support in the development of support documentation to include as a minimum, elements such as support equipment, technical orders, supply support and computer resources support, process of evolving and establishing maintenance/support concepts. Creates, coordinates and helps execute plans for the Integrated Product Support (IPS) of complex systems during the entire life-cycle. Analyses adequacy and effectiveness of current and proposed logistics support provisions. Supervises the efforts of other logistics personnel in the execution of assigned tasks.
5.1	Certification	Bachelor's degree in engineering.
5.2	Experience	Must have experience of deployed systems with at least seven years in supply and support of information systems. At least five years in Integrated Product Support of distributed systems in more than one NATO nation.
6	**Quality Manager**	Expected to develop quality control processes, ensuring deliverables are specified and designed with adherence to contractual requirements, legal and safety standards. Responsible for monitoring and evaluating internal production processes, examining products to determine their quality, engaging with the Purchaser and gathering product feedback. Identify opportunities to improve production efficiencies. Evaluating the quality of final products output and producing statistical reports on standards achieved. Products not achieving necessary standards are to be identified and rejected, prior to delivery to the Purchaser.
6.1	Certification	Bachelor's degree in business or engineering, plus certification with internationally recognised Quality Assurance or Control Institute
6.2	Experience	Must have experience of deployed systems with at least seven years in information systems design and quality management. At least two years as the quality manager for an effort of similar scope.

SER	KEY PERSONNEL	REQUIREMENTS
7	**Training Manager**	Conducts the research necessary to identify training needs based on performance objectives and existing skill sets; prepares training strategies and delivery methodology analyses; and prepares cost/benefit analyses for training facilities and deliverables. Develops training delivery plan, instructional guidelines, and performance standards and assessment mechanisms. Plans and directs the work of training material developers and coordinates activities with system development staff. Supervises the implementation and adaptation of training products to customer requirements. Conducts the research necessary to develop and revise training courses and prepares training plans. Develops instructor (course outline, background material, and training aids) and student materials (course manuals, workbooks, handouts, completion certificates, and course feedback forms). Trains personnel by conducting formal classroom courses, workshops, seminars, and/or computer based/computer-aided training. Provides daily supervision and direction to staff.
7.1	Certification	Bachelor Degree.
7.2	Experience	Must have experience of deployed systems with at least 5 years in the design and development of training for information systems using an Instructional Systems Design approach such as the Systems Approach to Training, Performance-Based Training, Analysis, Design, Development, Implementation, and Evaluation (ADDIE), or Criterion Referenced Instruction.
8	**Configuration Manager**	Establishes and maintains a process for tracking the life cycle development of system design, integration, test, training, and support efforts. Maintains continuity of products while ensuring conformity to Purchaser requirements and commercial standards. Establishes configuration control forms and database.
8.1	Certification	Bachelor’s degree.
8.2	Experience	At least five years’ experience in specifying configuration management requirements, standards, and evaluation criteria in acquisition documents, and in performing configuration identification, control, status accounting, and audits. At least three years in computer and communication systems development, including physical and functional audits and software evaluation, testing and integration.

APPENDIX E PROJECT ACTIVITY FLOW


Work Package 1 – Provide System Design
ISM & Shelter Proof Of Concept
Configuration Capture
@ NCIA
@ Customer
@ Teleconference
Configuration Capture
Configuration Capture Closure Meeting
System Requirements Review
Preliminary Design Review
Critical Design Review
1
Work Package 2 – Qualify First Articles
Engineering Tests
Build First Articles
Qualification Testing
1
Crypto
Radio Equipment
PFE
First Article Acceptance Testing
Factory Acceptance Testing
Ship Batch # 1 to Customer Site
5
To be carried out in Portugal
Work Package 3 – Support Security Accreditation
Develop Security Related Documentation
Security Testing for AfT
3
Achieve AfT Authorisation
Security Testing for I-SA
Achieve SA, I–SA
4
Work Package 4 – Conduct Training
Training Needs Analysis
Customer Site Survey
Install & Configure Training System @ Customer Site
Training Site Acceptance Test
Conduct Training
2
Deficiencies Resolution
Work Package 5 – Conduct User Testing and PSA
5
Deliver Release Packages to Customer Site
Crypto
Radio Equipment
Vehicles
Antenna
SATCOM
2
Install & Configure Batch #1
PFE
3
IV & V Assessment At Customer Site
With FMN DPOP emulator
Deployment Authority
2
Provisional System Acceptance
Commence Service Transition
System Integration Testing
System Interoperability Testing
Security Penetration & Vulnerability Testing
System Acceptance Testing
Deficiencies Resolution
Work Package 6 – Provide Production Units
Procure Long Lead Items
Produce Batch #2 (Factory State)
Ship Batch #2 To Customer Site
Produce Batch #3 (Factory State)
Ship Batch #3 To Customer Site
Work Package 7 – Support Operational Testing & Evaluation (OpTEval) Evaluation
Rebuild of Batch #1 At Customer Site
System Configuration
PFE
Crypto
Radio Equipment
Vehicles
Antenna
SATCOM
Conduct Operational Testing & Evaluation
2
Service Transition Complete
4
Final System Acceptance
CLS & Warranty Commences

APPENDIX F TABLE OF ABBREVIATIONS

Abbreviation	Meaning
GPP	3rd Generation Partnership Project
5G NR	5G New Radio
5GC	5G Core
AAA	Authentication, Authorisation & Accounting
ABB	Architectural Building Blocks
ABD	As Built Drawings
ABL	Allocated Baseline
ABS	Anti-lock Braking System
AC	Alternating Current
ACU	Antenna Control Unit
AD	Active Directory
ADFS	Active Directory Federation Service
AECTP	Allied Environmental Conditions and Test Publications
AES-NI	AES New Instructios
Ai	Intrinsic Availability
AN	Access Node
API	Application Programming Interface
APN	Access Point Name
AQAPs	Allied Quality Assurance Publications
ARM	Availability & Reliability Maintenance

Abbreviation	Meaning
ATE	Automated Test Equipment
ATU	Antenna Tuning Unit
AVR	Automatic Voltage Regulator
BC	Biological and Chemical
BCC	Battalion Communication Centre
BGP	Border Gateway Protocol
BIT	Built In Test
BLK	Black Transport Network
BLOS	Beyond Line of Sight
BMC	Baseboard Management Controller
BMS	Battlefield Management System
BoB	Breakout Box
BPS	Boundary Protection System
C2	Command & Control
C4ISR	Command, Control, Communications, Computers Intelligence, Surveillance and Reconnaissance
CA	Carrier Aggregation
CAC	Call Admission Control
CARC	Chemical Agent Resistant Coating
CAS	Compute and Storage
CAW	Contract Award
CBRN	Chemical, Biological, Radiological and Nuclear

Abbreviation	Meaning
CBT	Computer Based Training
CCA	Coloured Cloud Access
CCAP	Configuration Capturing
CCC	Company Communication Centre
CD	Compact Disc
CDR	Critical Design Review Call Detail Record
CDRL	Contract Deliverables Requirement List
CES	Core Enterprise Service
CI	Configuration Item
CIS	Communication and Information System
CIWG	Capability Integration Working Group
CLIN	Contract Line Item Number
CLS	Contracted Logistic Support
CLSP	Contract Logistics Support Plan
CM	Configuration Management
CMDB	Configuration Management Database
CMP	Configuration Management Plan
CNM	Core Network Module
CNR	Combat Net Radio
CoC	Certificate of Conformity

Abbreviation	Meaning
CoG	Center of Gravity
COI	Community Of Interest
CONEMP	Concept Of Employment
COP	Continuous Operating Power
COTS	Commercial Off The Shelf
CQAR	Contractor Quality Assurance Representative
CR	Change Request
CRP	Change Request Plan
CSA	Configuration Status Accounting
CSC	Computer Support Centre
CSCI	Computer Software Configuration Item
CUBE	Cisco Unified Border Element
CUCM	Cisco Unified Call Manager
DC	Direct Current
DCIS	Deployable Communication and Information System
DCIS CA	DCIS Cube Architecture
DDM	Data Diode Module
DHCP	Dynamic Host Configuration Protocol
DMSMS	Diminishing Manufacturing Sources and Material Shortages
DNS	Domain Name Server
DP	Documentation Plan

Abbreviation	Meaning
DPOP	Deployable Point Of Presence
DR	Deficiency Report
DRACAS	Data Reporting Analysing & Corrective Action System
DRS	Deployable Removable Storage
DSCP	Differentiated Services Code Point
DSMS	Domain Specific Management System
DSS	dismounted soldier situational awareness software
DVD	Digitised Video Disc
DWPD	Drive Writes Per Day
E2E	End-to-End
ECCRP	External Commercial Communication Roof Panel
ECP	Engineering Change Proposals External Communications Panel
ECU	Environmental Control Unit
EDC	Effective Date of Contract
EIRP	Effective Isotropic Radiated Power
ELOSRP	External Line of Sight Roof Panel
EMC	Electro-Magnetic Compatibility
EMI	Electromagnetic Interference
EMM	Element Management Module
EMSEC	Emission Security
EPC	Evolved Packet Core

Abbreviation	Meaning
EPP	External Power Panel
ERFP	External RF Panels
ERM	Event Review Meeting
ES	Engineering Support
ESATRP	External SATCOM Roof Panel
ESP	Encapsulating Security Protocol
ETE	Estimated Time to Empty
ETP	Event Test Plan
EU	European Union
EUD	End User Devices
E-UTRA	Evolved Universal Terrestrial Radio Access
FAAT	First Article Acceptance test
FAS	Functional Application Service Functional Area Service
FAT	Factory Acceptance Test; this is another term for FAAT above
FBL	Functional Baseline
FCA	Functional Control Audits; or Functional Configuration Audit
FD	Fault Detection
FDR	Final Design Review
FfP	Fit for Purpose
FI	Fault Isolation

Abbreviation	Meaning
FIPS	Federal Information Processing Standards
FMECA	Failure Mode Effect & Criticality Analysis
FMN	Federated Mission Network
FO	Fibre Optic
FQDN	Fully Qualified Domain Name
FSA	Final System Acceptance
FTA	Fault Tree Analysis
GAR-T	Tactical Towable Support Group
GRE	Generic Routing Encapsulation
H & S	Health & Safety
HCLOS	High Capacity Line Of Sight
HDS	High Density Switching
HFO	Hydrofluoroolefines
HL	Hardware Level
HLD	High Level Design
HTTP	HyperText Transport Protocol
HW	Hardware
IA	Infromation Assurance
IaaS	Infrastructure as a Service
IATA	International Air Transportation Association
ICAO	International Civil Aviation Organization

Abbreviation	Meaning
IDU	Indoor Unit
IEC	International Electrotechnical Commission
IER	Information Exchange Requirements
IETF	Internet Engineering Task Force
IF	Intermediate Frequency
IGP	Interior Gateway Protocol
IK	Installation Kit
iLO	Integrated Lights-Out
IMP	Issue Management Plan
IMS	Informal Messaging Service
IMT	Industry Maintenance Task International Mobile Telecommunication
IMT-CN	IMT Core Network
IMT-UE	IMT User Equipment
IOPS	Input/output Operations Per Second
IP	Internet Protocol
IPDV	IP packet Delay Variation
IPL	Initial Provisioning List
IPLR	IP packet Loss Rate
IPMI	Intelligent Platform Management Interface
IPS	Integrated Product Support Intrusion Prevention System

Abbreviation	Meaning
IPSP	Integrated Product Support Plan
IPTD	IP packet Transfer Delay
IRFP	Internal RF Panels
IRR	Infra-Red Reflective
ISM	Information Service Module
ISPCP	Initial Spare Parts & Consumables Package
ISS	In Service Support
ISSP	In Service Support Plan
ITS	Issue Tracking System
ITSM	Information Technology Service Management
ITU	International Telecommunication Union
IV&V	Integration Verification & Validation
KOM	Kick Off Meeting
KVM	Keyboard Video Mouse
LAN	Local Area Network
LC2IS	Land Command and Control Information System
LDP	Label Distribution Protocol
LED	Light Emitting Diode
LHCP	Left-Hand Circular Polarization
LLD	Low Level Design
LMM	Local Management Module

Abbreviation	Meaning
LogA	Log Aggregation
LORA	Level Of Repair Analysis
LOS	Line of Sight
Low-PIM	Low Passive Intermodulation
LRU	Line Replaceable Unit
LSA	Logistics Support Analysis
LSP	Label-Switched Path
LTE	Long-Term Evolution
MAN	Metro Area Network
MCU	Multipoint Control Unit
MHE	Material Handling Equipment
MIL-STD	Military Standard
MIMO	Multiple Input Multiple Output
Mini-LOS	Mini-Line of Sight
MLPP	Multi-Level Precedence Pre-emption
MM	Multi-Mode
MMA	Multimedia Access
MNO	Mobile Network Operators
MNP	Mission Network Partner Mission Network Participant
MOU	Memorandum Of Understanding
MP	Maintenance Plan

Abbreviation	Meaning
MPC	Mission Preparation Centre
MPLS-TE	Multiprotocol Label Switching – Traffic Engineering
MPT	Multi-Purpose Tires
MR	Mission RESTRICTED
MS	Mission SECRET
MSDP	Multicast Source Discovery Protocol
MSDS	Material Safety Data Sheet
MTA	Maintenance Task Analysis
MTBCF	Mean Time Between Critical Failures
MTBF	Mean Time Between Failures
MTP/TRP	Media Termination Point / Trusted Relay Point
MTTR	Mean Time To Repair
MTTRS	Mean Time To Restore Service
MTV	Medium Tactical Vehicle
MU	Mission UNCLASSIFIED
NAC	Network Access Control
NATO	North Atlantic Treaty Organisation
Nat-R	National RESTRICTED
Nat-S	National SECRET
Nat-U	National UNCLASSIFIED
NBD	Next Business Day

Abbreviation	Meaning
NCI AGENCY	NATO Communication & Information Agency
NDN	National Defence Network
NIAPC	NATO Information Assurance Product Catalogue
NIC	Network Interface Card
NIDS	Network Intrusion Detection System
NIP	Network Interconnection Point
NMCD	Network Management and Control Device
NQAR	NATO Quality Assurance Representative
NPKI	NATO Public Key Infrastructure
NR	NATO RESTRICTED
NRF	NATO Reaction Force
NS	NATO Secret
NSPA	NATO Supply & Procurement Agency
NTP	Network Time Protocol
NU	NATO Unclassified
OAS	OpenAPI Specification
OBL	Operational Base Line
OCR	Optical Character Recognition
ODU	Outdoor Unit
OEM	Original Equipment Manufacturer
OJT	On Job Training

Abbreviation	Meaning
OpTEval	Operational Technical Evaluation
OS	Operating System
OTA	Over The Air
OTI	Operational Task Inventory
OTS	Off The Shelf
OVA	Online Vulnerability Assessment
P2P	Peer-to-Peer
PBL	Product Base Line
PBR	Policy-Based Routing
PBS	Product Breakdown Structure
PCA	Physical Configuration Auditing Protected Core Access
PCN	Protected Core Network
PDF	Portable Document Format
PDR	Preliminary Design Review
PDU	Power Distribution Units
PE	Provider Edge
PFE	Purchaser Furnished Equipment
PGU	Power Generator Unit
PHST	Packaging Handling Storage & Transportation
PIP	Project Implementation Plan
PKI	Public Key Interface

Abbreviation	Meaning
PM	Project Manager
PMP	Project Management Plan
PMS	Project Master Schedule
PNA	Portuguese National Army
POAP	Plan On A Page
PoC	Point of Contact
PoE	Power over Ethernet
POL	Petroleum, Oil and Lubricant
PoP	Point of Presence
POTS	Plain Old Telephone System
PRM	Project review Meeting
PRT	Portugal Portuguese
PRT MOD	Portuguese Ministry Of Defence
PSA	Preliminary System Acceptance
PSD	Power Spectral Density
PTP	Precision Time Protocol
PTT	Push To Talk
QA	Quality Assurance
QAP	Quality Assurance Plan
QAR	Quality Assurance Representative
QC	Quality Control

Abbreviation	Meaning
QMP	Quality Management Plan
QMS	Quality Management System
QoS	Quality of Service
RAIDO	Risks Assumptions Issues Dependencies Opportunities
RAML	RESTful API Modeling Language
RAMT	Reliability Availability Maintainability Testability
RAN	Radio Access Network
RAP	Radio Access Point
RAT	Radio Access Technology
RBD	Reliability Block Diagram
RCB	Residual Current Breakers
RCIL	Recommended Consumables Items List
RCM	Reliability Centred Maintenance
RDP	Remote Desktop Protocol
RF	Radio Frequency
RFC	Request for Change
RFD	Request For Deviation
RFW	Request For Waiver
RHCP	Right-Hand Circular Polarization
RL	Rear Link
RMP	Risk Management Plan

Abbreviation	Meaning
RNM	Remote Network Module
ROADS	Record of Actions & Decisions
RPL	Repair Price List
Rs	Symbol Rate
RSPCL	Recommended Spare Parts & Consumables List
RT	Real Time
RTM	Requirement Traceability Matrix
RtR	Real Time Replication
RTTL	Recommended Tools & Test Equipment List
RU	Rack Unit
SAG	System Administration Guide
SAN	Storage Area Network
SAT	System Acceptance Test; this is another name for the FAST above
SATCOM	Satellite Communications
SBC	Session Border Controller
SDC	Software Defined Compute
SDDC	Software-Defined Data Centre
SDN	Software Defined Networking
SDS	Software Defined Storage
SFF	Safe Failure Fractions
SFP	Small Form-Factor Pluggable

Abbreviation	Meaning
SFTP	Shielded Foil Twisted Pair
SGS	Satellite Ground Station
SHDSL	Symmetric High speed Digital Subscriber Line
SIC-T	Sistema de Informação e Comunicações - Tático
SIM	Subscriber Identity Module
SIT	System Integration Test
SIVP	Security Implementation Verification Procedure
SL	Software Level
SM	Single Mode
SMB	Server Message Block
SMC	Service Management and Control
SME	Subject Matter Expert
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOC	State of Charge
SOS	System Of Systems
SOW	State Of Work
SPD	Surge Protective Devices
SQEP	Suitably Qualified and Experienced Personnel
SRR	System Requirements Review
SRS	Systems Requirement Specification

Abbreviation	Meaning
SRST	Survivable Remote Site Telephony
SRU	Shop Replaceable Units
SSH	Secure Shell Protocol
SSPP	System Safety Program Plan
SSR	System Safety Review
SSS	Schedule of Supplies & Services
STANAG	Standard NATO Agreement
STE	Special to Type Equipment
STP	Shielded Twisted Pair
STVP	Security Test & Verification Plan
SW	Software
TA	Target Architecture
TAT	Turn Around Time
TB	Terabyte
TBW	TB Written
TCP	Transmission Control Protocol
TD	Test Director
TDCIS	Tactical Deployable Communication and Information System
TDM	Time Division Multiplexing
TFS	Traffic Flow Security
THD	Total Harmonic Distortion

Abbreviation	Meaning
TIWG	Test Integration Working Group
TLS	Through Life Support
TM	Technical Manual
TN	Transit Node
TNA	Training Needs Analysis
TP	Training Plan
TPDP	Technical Publication Development Plan
TPM	Trusted Platform Module
TRR	Test Readiness Review
TSGT	Tactical Satellite Ground Terminal
TTR	Time To Recover
TV&V / TV&V	Test, Verification, Validation
TV&VP / MTP	Test, Verification & Validation Plan. This is another name to the Project Master Test Plan (MTP)
TXT	Trusted Execution Technology
UAM	User Access Module
UAT	User Acceptance Test
UAT(E)	User Acceptance Test of Equipment
UCC	Unified Communication and Collaboration
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
UPS	Uninterrupted Power Supply

Abbreviation	Meaning
UTRAN	UMTS Terrestrial Radio Access Network
UV	Ultra Violet
V2	Voice and Video
vCPU	virtual CPU
VCU	Virtual Crypto Unit
VLAN	Virtual Local Area Network
VM	Virtual Machine
vRAM	virtual RAM
VRF	Virtual Routing and Forwarding
VSWR	Voltage Standing-Wave Ratio
VTC	Video Teleconference
WAN	Wide Area Network
WAP	Wireless Access Point
WBS	Work Breakdown Structure
WGS	Wideband Global SATCOM
WinRM	Windows Remote Management
WLC	Wireless LAN Controller

APPENDIX G GLOSSARY OF TERMS

Attaching Parts	These are the items reported in the Corrective and Preventative Maintenance Procedures and in the Illustrated Parts Breakdown such as screws, gaskets, nuts, bolts, washers etc.
Consumables: Technical	This category of consumables includes (but it's not limited to) Fuses, Bulbs, Lamps, Gaskets, o-rings, EMI/Tempest seals, Surge Protectors, gas dischargers, Batteries and, in general, any other item replaced in case of preventive or corrective maintenance on the System etc.
Consumables: Non-Technical	This category of consumables includes (but it's not limited to) all POLs (Petrol, Oils, Lubricants), adhesive, sealing paste, gas and, in general, any other item replaced in case of preventative or corrective maintenance on the System etc.
Consumables: Generic	This category of consumables includes (but it's not limited to) ink cartridges, toners, printing paper, print ribbons, generic cleaning material and in general all the materials whose consumption cannot be predicted (e.g. is not associated to any preventative or corrective maintenance on the System) etc.
Installation	Attaching facilities and, or equipment to a unit's infrastructure, being installed in robust manner, preventing their subsequent removal or movement within their mount.
Integration	The process of bringing together component sub-systems, or equipment, ensuring their combined functionality in forming a coherent system, meets the expected system requirements.
Level 0 Schedule	A single line representation of a project's lifecycle containing major milestones
Level 1 Schedule	A bar chart representation of the project's lifecycle illustrating major components and associated milestones.
Level 2 Schedule	Major components in the Level 1 schedule are subdivided and shown in a bar chart format, where further milestones are shown also.
Level 3 Schedule	Further sub-divisions are illustrated in a Gantt chart, which is to be used in monitoring and managing the project's execution. This Gantt chart will identify.
Line Replaceable Unit (LRU)	a. Its failure can be detected and indicated by a BIT (Built In Test System) system or by abnormal condition/failure display/alarm, in conjunction with Technical Manuals (TMs) and general-purpose test equipment and troubleshooting procedures b. It is easily accessed for replacement purposes c. It is easy to replace, through the use of a plug-in connector, screwed terminal, nut/bolt fixing or similar connector

	d. It has minimal adjustment/alignment requirements, such as voltage level settings, Software (SW) and Firmware (FW) installations/adaptations etc. e. Adjustments may be carried out with the BIT or with general-purpose Hardware (HW)/ Software (SW) tools and test equipment f. When only one LRU has failed, its replacement returns the system/equipment to full operational status.
Line Replaceable Unit: Statistical (LS)	A category of LRU includes, but not limited to items subject to faults that occur with a statistical probability e.g. IF/RF strips/boards, SBCs, PPCs, Computers/Servers/Workstations and theirs components/peripherals, Networking equipment (Routers, switches), Power Supplies, electric/electronic components in general etc.
Line Replaceable Unit: Limited Life (LL)	This sub-category of LRU includes, but not limited to the items whose faults are due to ageing e.g. TWTs, Rotary Joints, Slip Rings, Engines, T/R switches, Fans and Fan Assemblies, etc
Roadmap	A term applicable to projects and systems. A Project roadmap provides a strategic overview of the major elements of a project, illustrating its objectives, milestones, deliverables, resources, and planned timeline. A system roadmap is a flexible planning technique to support strategic and long-range planning, by matching short-term and long-term goals with specific technology solutions
Service Provision Authority	Being suitably skilled and experienced, this authority ensures that the service provided by a contractor to the end user is as required by a commercial agreement between the two parties. A service's provision may be governed by a Service Level Agreement, outlining the extent and degree of service to be provided by a contractor to the end user.
Support Concept	A definition of the support objectives (scenarios) in relation with maintenance levels, maintenance support and their interrelationships and shall be implemented in conjunction and coordination with the Maintenance Concept. The support concept is the apportionment of maintenance activities: • PRT Maintenance Task (PMT) will be performed by PRT MOD personnel (military or civilian), • Industry Maintenance Task (IMT) will be performed by industry personnel under Warranty or Post Warranty Arrangement. Refer to Appendix H in this document for detailed information regarding Support Concept
Support Scenario: NONO	NATO Owned / NATO Operated. The solution would be procured as a system and would be operated and maintained by NATO. The responsibilities for NATO maintenance levels are defined in the Maintenance Concept.
Support Scenario: COCO	Contractor Owned / Contractor Operated. NATO would have the solution delivered by a contractor as a Service.

Support Scenario: NOCO	NATO Owned / Contractor Operated. With this approach NATO would procure a system, but would “outsource” the Operation and Maintenance of it.
Support Scenario: CONO	Contractor Owned / NATO Operated. This approach exists and is usually called “Final NCI Agency leasing”.
Technical Authority	Technical authorities ensure that engineering documents and drawings are checked, reviewed, and approved by appropriately qualified, competent, and experienced expert engineers, within the NCI Agency and, or the selected contractor. Technical Authorities ensure that the technical decisions made are consistent with the appropriate level of competence, quality and consistency, in order to assure the technical integrity of the final product. NCI Agency will be the Technical Authority for the contract issued to The Contractor selected for the TDCIS project.

NATO OTAN

NATO Communications and Information Agency

NCI AGENCY

NATO Communications and Information Organisation

Portuguese Republic Ministry of Defence Tactical Deployable Communication and Information System

Short Title: PRT TDCIS

Book II - Part IV

Statement of Work (SoW)
Annex A – System Requirements Specification (SRS)

Reference:	RFQ-CO-115363-PRT-TDCIS
Publication Date:	~~24/11/2022~~30/11/2022
Classification:	NATO UNCLASSIFIED
Status:	Final
Version:	2.2~~1~~
No. of pages	321

TABLE OF CONTENTS

INDEX OF FIGURES

INDEX OF TABLES

This page is intentionally left blank.

1 Introduction

NOTE (PRTTDCIS-1108)

~~[1]~~ This System Requirements Specification (SRS) document provides the Functional and Technical requirements, together with the Implementation Constraints for The Tactical Deployable Communication and Information System (TDCIS) for the Portuguese (PRT) Army to be used up to Brigade level, for National, NATO or other multinational deployment scenarios in Portuguese National and/or International territory. TDCIS is designed to operate on military and civilian operational scenarios and to support Joint and/or Combined operations.

SRS (PRTTDCIS-1109)

~~SRS-1~~ This SRS defines the sizing, standards, quality and design requirements, and constraints that shall be adhered to in the design (or modification of a COTS design) and implementation of this project.

NOTE (PRTTDCIS-1110)

~~[2]~~ The SRS does not discuss Node quantities. These are covered under the scope description in the Statement of Work (SOW) Main Body.

NOTE (PRTTDCIS-1667)

~~[3]~~ This SRS is structured as follow:

1) **Introduction** (this chapter) covers the *Purpose* of the document; then,
2) **Conventions and Standards** covers all Conventions, Definitions, NATO and other Standards which are applicable all this document long; then,
3) **High Level Specifications** covers
    1) The TDCIS in *General* and the architecture which supports it,
    2) The *Nodes* and *Housing* elements TDCIS is composed of,
    3) The *Performance Targets* TDCIS has to meet,
    4) The TDCIS level *Implementation Constraints*; then,
4) **Services** covers all services (*Business Support, CIS Security*, etc.) TDCIS has to provide; then,
5) **Modules** covers in details the *Functional* and *Technical Requirements*, together with the *Implementation Constraints* applicable to the different Modules and Subsystems which are used to build the TDCIS; then,
6) **Transmission Systems** covers in details the *Specifications* of all Transmission Systems (such as SATCOM, Radio, etc.) present in TDCIS; then,
7) **Housing Elements** covers in details the *Specifications* of all Housing elements (such as Shelter, Trailer and Casing) present in TDCIS; finally,
8) **User Appliances** covers in details the *Specifications* of all End User Devices (such as Workstations, Phones, etc.) present in TDCIS.

2 Conventions and Standards

2.1 SRS Document

NOTE (PRTTDCIS-1119)

~~[4]~~ Information and requirements contained under a "General" heading are applicable to all the elements covered by the corresponding upper section.

NOTE (PRTTDCIS-1120)

~~[5]~~ All statements are identified with a Unique Reference called the Key.

NOTE (PRTTDCIS-1121)

~~[6]~~ Mandatory requirements are identified as **SRS**.

NOTE (PRTTDCIS-1122)

~~[7]~~ General informational, descriptive text is identified as NOTE.

SRS (PRTTDCIS-1123)

~~SRS-2~~ Statements in numbered lists (i= 1 to n) under a **SRS** requirement shall be considered individual requirements under the "shall" statement of the parent requirement.

NOTE (PRTTDCIS-3041)

~~[8]~~ The acronyms and abbreviations used in this SRS are defined in in the applicable Annex or Appendix of the SOW.

NOTE (PRTTDCIS-3042)

~~[9]~~ No meaning is associated with the order of serial numbering. There could be gaps in numbering and requirement identifiers in a group do not have to be sequential.

NOTE (PRTTDCIS-3247)

~~[10]~~ All Conventions defined in the SOW are equally applicable to the SRS.

2.2 Definitions

NOTE (PRTTDCIS-1124)

~~[11]~~ "-xx" is the generic suffix denoting either:

- Black Transport Network (BLK); or
- NATO Unclassified (NU);
- Mission Unclassified (MU);
- National Unclassified (Nat-U);
- NATO Restricted (NR);
- Mission Restricted (MR);
- National Restricted (Nat-R);
- NATO Secret (NS);
- Mission Secret (MS); or,
- National Secret (Nat-S).

NOTE (PRTTDCIS-3089)

~~[12]~~ "-xU" is the generic suffix denoting both NU and/or MU and/or Nat-U.

NOTE (PRTTDCIS-3088)

~~[13]~~ "-xR" is the generic suffix denoting both NR and/or MR and/or Nat-R.

NOTE (PRTTDCIS-1125)

~~[14]~~ "-xS" is the generic suffix denoting both NS and/or MS and/or Nat-S.

SRS (PRTTDCIS-1126)

~~SRS-3~~ Requirements stating a capability to be "supported" (i.e. "shall support") shall be understood as the ability of the Purchaser to configure the capability to be active or not active at his discretion. This means that the capability is not necessary implemented upon delivery, but shall be available in its full extent, without restrictions.

SRS (PRTTDCIS-1127)

~~SRS-4~~ Requirements stating a capability to be "implemented" (i.e. "shall implement") shall be understood as requiring the capability to be implemented and configured for use in the delivered system.

SRS (PRTTDCIS-1128)

~~SRS-5~~ Requirements stating to be supported or implemented "fully conformant" to an architecture shall be understood as requiring full correspondence between architecture specification and implementation, where all features of this specific requirement are implemented in accordance with the architecture specification and there are no features of this specific requirement implemented that are not covered by the architecture specification.

NOTE (PRTTDCIS-1129)

~~[15]~~ The term "including" is never meant to be limiting - the list that follows is always non-exhaustive.

SRS (PRTTDCIS-1130)

~~SRS-6~~ Any requirements using the term "target" shall be interpreted as hard constraints to be respected during the design process, with any deviation being subject of agreement by the Purchaser. Any such constraints are currently motivated by:

1) Compliance with the DCIS TA; or
2) Federated Mission Network (FMN) compliance; or
3) Interoperability; or
4) Lessons Learned; or
5) Specific operational constraints.

NOTE (PRTTDCIS-1131)

~~[16]~~ The DCIS TA is neither an Applicable nor a Reference document in this SRS. The interpretation of the TA and its translation into requirements in the specification is the responsibility of the Purchaser.

NOTE (PRTTDCIS-1133)

~~[17]~~ The use of the term "notional" is to be interpreted as guidance only.

SRS (PRTTDCIS-1134)

~~SRS-7~~ When specifications and/or quantities are specified as "Design Driven", it shall be understood as being subject to design decisions and thus not prescribed by this specification.

NOTE (PRTTDCIS-1135)

~~[18]~~ Availability requirements are formulated in terms of Operational Availability. Assumptions are made for mean logistics delays based on positioning spares locally, at intermediate depots, or at centralized depots.

SRS (PRTTDCIS-4025)

~~SRS-8~~ The term "Withstand" shall be understood as that the equipment under specified climatic and environmental conditions is stored, transported, handled and shall operate without suffering degradation of system performance (gain, pattern type, sensitivity, etc.) and without suffering permanent mechanical damages.

SRS (PRTTDCIS-1523)

~~SRS-9~~ The term "enable" (or enabled) shall be understood as an enabling function; i.e. the capability needs to be implemented for, but no CIS equipment is to be installed or delivered. For example, if a rack needs to be "enabled" for the integration of a Radio Transmitter, it means that the rack is equipped with the radio transmitter integration kit (cabling, mounting shelves...), but the radio transmitter itself is not to be delivered.

SRS (PRTTDCIS-1846)

~~SRS-10~~ "Open" shall be understood as enabling the basic functionality to be modified or extended through mechanisms such as API and plugins without any proprietary constraints.

NOTE (PRTTDCIS-2109)

~~[19]~~ Housing elements are defined as the Non-CIS assets hosting the CIS components. Shelters, Cases (transit and transport) and Trailers are housing elements.

NOTE (PRTTDCIS-2917)

~~[20]~~ The term "User" refers to any personnel member accessing the DPOP and consuming its Services.

NOTE (PRTTDCIS-2918)

~~[21]~~ The term "End User" refers to any personnel member accessing the DPOP and consuming its Services and who is not a System Administrator.

SRS (PRTTDCIS-3235)

~~SRS-11~~ End-User Devices (EUD) is a naming convention and shall be understood as a generic term to refer to any user (End User or System Administrator) appliance such as Workstations, Phones, Printer, etc.

SRS (PRTTDCIS-3844)

~~SRS-12~~ The acronym HDD (Hard Disk Drive) shall be understood as a generic term to define a storage device, irrelevantly of the technology it is implemented with (e.g. Solid State).

NOTE (PRTTDCIS-3120)

~~[22]~~ The implementation of any given DPOP information security domains is called a Colour Cloud.

2.3 Architecture

NOTE (PRTTDCIS-2309)

~~[23]~~ All architecture diagrams are modeled using Archimate 3.1 modelling language.

NOTE (PRTTDCIS-1111)

~~[24]~~ The infrastructure supporting the DCIS capability is a system-of-systems and is broken down as follows:

1) *Deployable Point Of Presence (DPOP)* is a collection of Nodes; and,
2) *Node* is a collection of Modules built into Housing Elements, associated with Transmission Systems and User Appliances; and,
3) *Module* is a collection of Subsystems; and,
4) *Subsystem*, is a Functional blocks which provides Services; and,
5) *Components*, are the building blocks of the Subsystems; and,
6) *Element* is a generic term which can refer to any of blocks described above.

SRS (PRTTDCIS-1112)

~~SRS-13~~ The detailed system design shall adhere to, and shall be structured around, the system breakdown structure presented in the following figure.

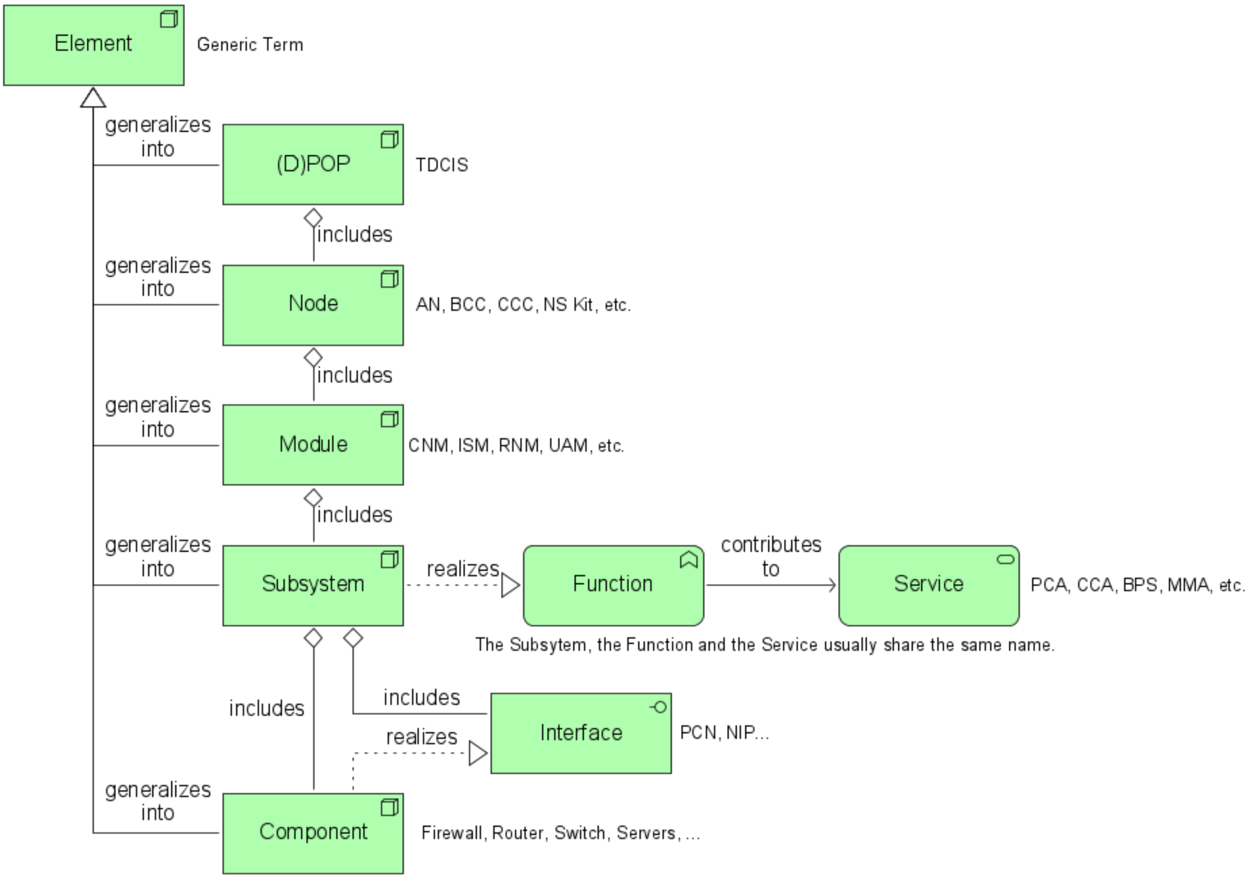


Figure 1 - Architecture Taxonomy

NOTE (PRTTDCIS-1113)

~~[25]~~ The TDCIS Nodes are built from Modules, Transmission Systems, and Housing elements.

NOTE (PRTTDCIS-1163)

~~[26]~~ The TDCIS System is considered as a DPOP, therefore TDCIS and DPOP terminology will be consistently and commonly used.

NOTE (PRTTDCIS-1114)

~~[27]~~ For each CIS Module, the functional and technical requirements will be:

- firstly provided at a Module level; then,
- by the requirements specific to each of the identified subsystems as a part of the preliminary design conveyed in this specification.

SRS (PRTTDCIS-1115)

~~SRS-14~~ Within this document the Functional Requirements are provided at module level, whereas the Technical (non-functional) Requirements are provided down to subsystem-level. The latter are derived from existing architectures and systems, which are proven and in operation, and detail the DPOP nodes where interoperability is critical. This specification contains Implementation Constraints which the Contractor shall adhere to when preparing the Low Level Design (LLD) specification.

SRS (PRTTDCIS-4019)

~~SRS-15~~ As illustrated in the following diagrams, a Variant Element shall be understood as a specialization of a Source Element.

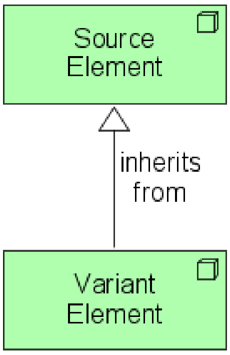


Figure 2 - Variant specialization

SRS (PRTTDCIS-4020)

~~SRS-16~~ Any set of specifications defined for a certain Element shall be automatically inherited by all its Variants. For instance, what is specified as to be implemented in xx shall be implemented in all Security Domains, what is specified as to be implemented in xU shall be implemented in all UNCLASSIFIED Domains, etc.

SRS (PRTTDCIS-4021)

~~SRS-17~~ Any set of specifications defined for a Variant Element shall supersede those from the Source it specializes from.

SRS (PRTTDCIS-4022)

~~SRS-18~~ What is specified as to be implemented in an Element, shall be implemented in all its Variants. For instance (non-exhaustive): what is specified to be implemented in xx shall be implemented in all Security Domains, what is specified as to be implemented in xU shall be implemented in all UNCLASSIFIED Domains, etc.

SRS (PRTTDCIS-4023)

~~SRS-19~~ A statement defined at a higher level shall automatically be applicable to all its composing elements unless specified otherwise at the element level. For instance: an Environmental Endurance target such as IPxx defined at (D)POP level is automatically applicable to all it composing elements; if the SATCOM Antenna Subsystem states a different IPzz (higher or lower) than the (D)POP level one, this IPzz will take precedence over the IPxx but only for the SATCOM Antenna Subsystem.

SRS (PRTTDCIS-2092)

~~SRS-20~~ An Element specific SRS statement shall always supersede global conventions.

NOTE (PRTTDCIS-4237)

~~[28]~~ Relationships between building blocks are complemented with text providing additional information. This textual information does not supersede the relationship definition as per Archimate standard.

NOTE (PRTTDCIS-1116)

~~[29]~~ Diagrams representing building blocks are coloured using standard Archimate 3.1 color scheme. The additional following conventions apply:

1) Coloured block with continuous border identifies Architectural Building Blocks which are in scope of the project and are project deliverables; and,
2) White block with dashed border identifies Architectural Building Blocks which relates to, influences or impacts the project but do not constitute project deliverables (e.g. Purchaser existing infrastructure or systems).

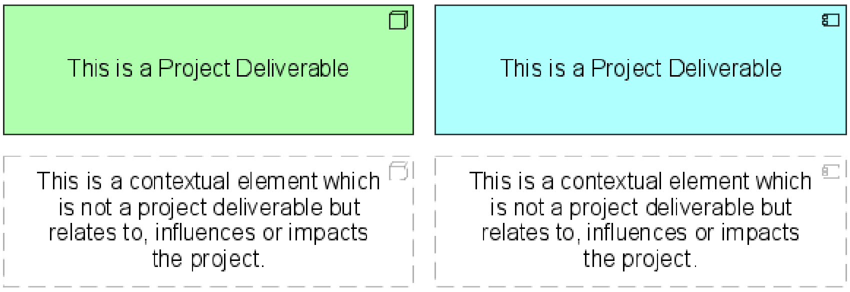

This is a Project Deliverable
This is a Project Deliverable
This is a contextual element which is not a project deliverable but relates to, influences or impacts the project.
This is a contextual element which is not a project deliverable but relates to, influences or impacts the project.

Figure 3 - Block styling convention

NOTE (PRTTDCIS-4024)

~~[30]~~ Purchaser Furnished Equipment (PFE) elements are identified with an additional PFE marking as illustrated on the following diagram.

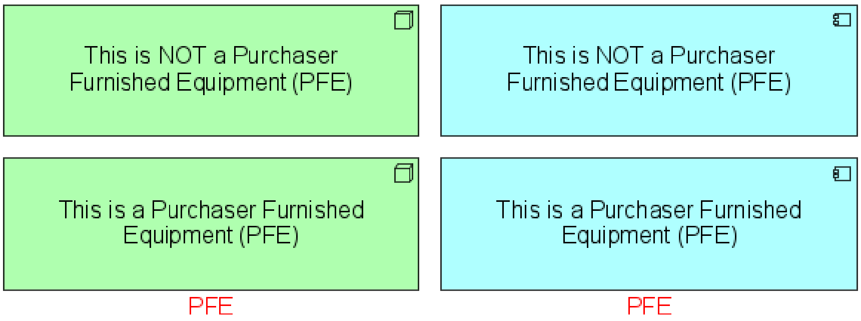

This is NOT a Purchaser Furnished Equipment (PFE)
This is NOT a Purchaser Furnished Equipment (PFE)
This is a Purchaser Furnished Equipment (PFE)
This is a Purchaser Furnished Equipment (PFE)
PFE
PFE

Figure 4 - PFE marking convention

SRS (PRTTDCIS-1117)

~~SRS-21~~ When calling for implementations conformant with the DCIS Cube Architecture (DCIS CA), it shall be understood as being in accordance with and conformant to the principles described in *DCIS Cube ADD Main, 2018*, and its *DCIS Cube ADD Annexes, 2018*, hereafter referred to as the DCIS CA Annexes. Where conformance to a specific DCIS CA Annex is required, in addition conformance to the DCIS CA as a whole is implicit.

SRS (PRTTDCIS-3090)

~~SRS-22~~ Implementation examples depicted in DCIS CA and its Annexes shall not be considered as an implementation constraint to deliver specific hardware and software; neither shall it exempt the Contractor from any acquisition regulation constraint.

NOTE (PRTTDCIS-1160)

~~[31]~~ This specification is based on the extant DCIS Target Architecture (TA) and it provides the foundation and the boundary conditions upon which this specification is built.

NOTE (PRTTDCIS-1161)

~~[32]~~ Boundary conditions are formulated as Technical Requirements and Implementation Constraints. In particular, Implementation constraints are introduced:

1) To minimize implementation risk, based on lessons learned; and,
2) To assure interoperability; and,
3) To minimize total cost of ownership across the entire pool of DCIS assets.

SRS (PRTTDCIS-1842)

~~SRS-23~~ Unless stated specifically, lines interconnecting elements in any figures (context, architecture, illustrative implementation…) are not intended to be representative of the actual number of interfaces/links between any pair of components. Those quantities shall be derived from the design, which shall in turn implement the minimum quantity of interfaces presented in the subsystem interface tables.

SRS (PRTTDCIS-3249)

~~SRS-24~~ The elements shall be modular in their construction to maximise commonality of components.

SRS (PRTTDCIS-3250)

~~SRS-25~~ As far as possible, the elements shall be implemented with Commercial Off-The-Shelf (COTS) solutions, field-proven in the Armed Forces of a NATO partner country or in a comparable industry, under similar geographical and climatic conditions.

SRS (PRTTDCIS-3251)

~~SRS-26~~ The DPOP shall be flexible and adaptable to meet the mission demands, but fundamentally, it shall be technologically robust and stable.

SRS (PRTTDCIS-3252)

~~SRS-27~~ The DPOP shall also have integrity and resilience and, where appropriate, have inbuilt redundancy.

SRS (PRTTDCIS-3253)

~~SRS-28~~ The design shall use modern software process and tooling that reduces the burden on the DPOP User and Administrators.

2.4 Units of Measurements

SRS (PRTTDCIS-4461)

~~SRS-29~~ The DPOP shall use metric system for all elements and documentation.

2.5 Computations

SRS (PRTTDCIS-1136)

~~SRS-30~~ The router throughput performances shall assume the following constant packet size distribution, representative of NATO DCIS traffic over the Wide Area Network (WAN):

1) IP packets sized <= 64 bytes is 25%; and,
2) IP packets sized 64<>127bytes is 20%; and,
3) IP packets sized 128<>255bytes is 9%; and,
4) IP packets sized 256<>511 bytes is 5%; and,
5) IP packets sized 512<>1023 bytes is 18%; and,
6) IP packets sized larger than1024 bytes is 23 %.

SRS (PRTTDCIS-1503)

~~SRS-31~~ With respect to User Port quantities, the rule-set for modelling the design shall be as follows:

- 1 User requires 2.25 switch ports, noting that 1 User consists of:
    - 1 data-port; and,
    - 1 VoIP port, and,
    - Access to a printer at 0.25 port; and,
- Maximum port utilization is 90% on any given access switch; for example: for 48 port switches, a reserve of 5 ports shall be considered as per design.

SRS (PRTTDCIS-4271)

~~SRS-32~~ With respect to Virtual Compute and Storage, the design rule-set for oversubscription shall be as follows:

- vCPU: maximum 3 to 1 oversubscription; and,
- vRAM: maximum 1.2 to 1 oversubscription; and,
- Storage: no oversubscription.

2.6 Interfaces and Cables

SRS (PRTTDCIS-2091)

~~SRS-33~~ Ethernet Network Termination Equipment shall be Small Form-Factor Pluggable (SFP)-based connectivity providing following variants:

- *Eth-Cu*: 100/1000 Copper RJ45 (Cat. 6 or better) Ethernet Interface;
- *Eth-FO-SR*: 1G/10G Multimode Fiber Optic (FO) Interface (Short Range);
- *Eth-FO-LR*: 1G/10G Single Mode Fiber Optic Interface (Long Range).

SRS (PRTTDCIS-4262)

~~SRS-34~~ Ethernet interfaces shall support Virtual Local Area Network (VLAN) tagging in accordance with IEEE802.1Q:2011.

SRS (PRTTDCIS-4265)

~~SRS-35~~ Copper Ethernet SFPs, where used, shall be able to operate at 100 Megabits per second (Mbps) and 1 Gigabits per second (Gbps).

SRS (PRTTDCIS-4266)

~~SRS-36~~ 10Mbps and 100Mbps Ethernet interfaces shall support both half-duplex and full-duplex, both configured through auto-negotiation and through manual configuration.

SRS (PRTTDCIS-4267)

~~SRS-37~~ All 1000BASE-T interfaces shall support 1Gbps auto-negotiation and shall support manual configuration of the speed to 1000Mbps, to 100Mbps and to 10Mbps.

SRS (PRTTDCIS-3822)

~~SRS-38~~ Ethernet Ports providing Power over Ethernet (PoE) shall not be of SFP type.

SRS (PRTTDCIS-2093)

~~SRS-39~~ All physical connections shall have clear indication of the security domain that they are assigned with respect to the following coloring convention:

- Black label for BLK;
- Green label for xU;
- Blue label for xR;
- Red label for xS.

SRS (PRTTDCIS-2385)

~~SRS-40~~ Labels shall be applied using a method that provides a legible, durable and non-fading result capable of withstanding exposure to the environmental conditions during operation, storage, transport and handling.

SRS (PRTTDCIS-2386)

~~SRS-41~~ Whenever possible, the labels shall be applied in such a manner that allows them to be visible after installation.

SRS (PRTTDCIS-2388)

~~SRS-42~~ The labels shall withstand the same environmental conditions as the equipment they are attached on (both for indoor and outdoor use).

SRS (PRTTDCIS-2387)

~~SRS-43~~ The labels shall be subject to the same environmental testing regime as the equipment they are attached on (both for indoor and outdoor use).

SRS (PRTTDCIS-4026)

~~SRS-44~~ Robust shielded cables, designed for tactical environment, shall be used to interconnect (D)POP elements.

SRS (PRTTDCIS-4027)

~~SRS-45~~ Insulating and sheathing compounds of all outdoor cables shall have minimum tensile strength of 12 N/mm2 in compliance with IEC 60811-501:2012.

SRS (PRTTDCIS-4028)

~~SRS-46~~ All outdoor power and data cables shall be: water, rodent, trampling and Ultra Violet (UV) resistant according to EN 50289-4-17:2015 or its IEC, ISO equivalent.

SRS (PRTTDCIS-4029)

~~SRS-47~~ All outdoor data cables, as the minimum, shall meet following requirements:

1) Tensile load during installation: 1800N; and,
2) Tensile load during operation: 600N; and,
3) Impact resistance: 200 impacts (according to EIA/TIA-455-25 Military req. or equivalent standard); and,
4) Crush resistance: 440 N/cm (according to EIA/TIA-455-41 Military req. or equivalent standard).

SRS (PRTTDCIS-4030)

~~SRS-48~~ The regulations of ISO/IEC 11801-1:2017 or equivalent shall be followed for the dimensioning of the bending radius of cables.

SRS (PRTTDCIS-4031)

~~SRS-49~~ In Case MIL-DTL-38999 series III based connectors are used for Copper Ethernet interfaces, they shall have an internal RJ45 connector and a MIL-DTL-38999 series III shell.

SRS (PRTTDCIS-4032)

~~SRS-50~~ All data cables used for Ethernet Copper connections shall be CAT6 Shielded Foil Twisted Pair (SFTP).

SRS (PRTTDCIS-4577)

~~SRS-51~~ The Contractor shall apply industry best practices for cable routing, fixing, etc. when integrating Elements in racks.

2.7 Environmental Endurance

2.7.1 General

NOTE (PRTTDCIS-2390)

~~[33]~~ This section contains the maximum severities that equipment provided under this contract can be exposed to. When the equipment is not able to satisfy those severity levels (especially for solar radiation, rain/snow/hail, wind and humidity), the contractor can make use of enclosures to partially isolate the materiel from the most demanding conditions. When these sheltering enclosures are used, the equipment becomes part of an assembly, and the contractor is responsible to guarantee compliance of the complete assembly (including electrical and electronic equipment, enclosures, fixing and mounting hardware, and all supporting subsystems like heating or cooling) with the totality of the required climatic, environmental, mechanical, biological and chemical parameters and severities.

NOTE (PRTTDCIS-1137)

~~[34]~~ *NC3A Technical Note TN-1078, 2008* (hereafter referenced as TN-1078) defines minimal requirements with respect to: High temperature, Low temperature, Change of temperature (temperature shock), Solar radiation, Humidity, Rainfall, Ice, Hail, Snow load, Wind, Dust/sand particle size and concentration, Min/max elevation, Max/min atmospheric pressure, Shock, Vibration, Acceleration, Bump, Drop and topple, Free-fall, Ingress Protection Rating, Salt mist, Acid atmosphere, Contamination by fluids, Mould growth and Electro-Magnetic Compatibility (EMC).

SRS (PRTTDCIS-1138)

~~SRS-52~~ TN-1078 shall be considered as the reference for all subjects it covers.

SRS (PRTTDCIS-1139)

~~SRS-53~~ Any deviation from TN-1078 in this SRS will be clearly articulated, in that instance the deviation shall prevail.

NOTE (PRTTDCIS-1140)

~~[35]~~ Clarifications can be sought from; *NATO Standardization Agreement 4370, "Environmental Testing", Edition 7* - hereafter referenced as STANAG 4370 - and its associated NATO Allied Environmental Conditions and Test Publications, latest edition - hereafter referenced as AECTPs.

SRS (PRTTDCIS-2391)

~~SRS-54~~ For defining design and test criteria, the contractor shall address all climatic and environmental conditions as stipulated in TN-1078.

SRS (PRTTDCIS-3108)

~~SRS-55~~ The climatic and environmental conditions are divided into following specifications, where all modes (operation, transport, storage and handling) shall be addressed:

- Climatic specification; and,
- Mechanical specification; and,
- Sealing specification; and,
- Biological and Chemical specification.

SRS (PRTTDCIS-3109)

~~SRS-56~~ Proof of compliance to all specifications (climatic, mechanical, sealing, biological and chemical) stipulated in TN-1078 shall be demonstrated by testing performed in accordance with STANAG 4370 edition 7 and its all associated AECTPs or equivalent national or commercial standards.

SRS (PRTTDCIS-2394)

~~SRS-57~~ The environmental tests shall include series of tests conducted in EU or NATO country certified climatic chambers including following tests:

- High temperature; and,
- Low temperature; and,
- Change of temperature (temperature shock); and,
- Solar radiation; and,
- Humidity; and,
- Wind load; and,
- Ingress protection; and,
- Salt mist; and,
- Acidic atmosphere; and,
- Altitude, pressure; and,
- Combined stress testing.

SRS (PRTTDCIS-3110)

~~SRS-58~~ The mechanical tests shall include series of tests conducted in EU or NATO country certified laboratory/testing plant including following tests:

- Shock; and,
- Vibration; and,
- Acceleration; and,
- Bump; and,
- Drop and topple; and,
- Free fall.

SRS (PRTTDCIS-1141)

~~SRS-59~~ Where the requirements for testing methods specified in TN-1078 and STANAG 4370 and all its associated AECTPs are in conflict, STANAG 4370 and all its associated AECTPs shall prevail.

SRS (PRTTDCIS-3111)

~~SRS-60~~ Where the requirements for testing parameters (for example high and low temperature, temperature shock, humidity, pressure etc.) specified in TN-1078 and STANAG 4370 and all its associated AECTPs are in conflict, TN-1078 shall prevail.

SRS (PRTTDCIS-3112)

~~SRS-61~~ The (D)POP shall be able to withstand the Climatic specification with following additional comments on Test Conditions when packaged as designed during transportation, storage and handling:

1) High temperature: test methods according AECTP-300 Edition D, version 1, method 302; and,
2) Low temperature: test methods according AECTP-300 Edition D, version 1, method 303; and,
3) Change of temperature (temperature shock): test methods according AECTP-300 Edition D, version 1, method 304; and,
4) Solar radiation: test methods according to AECTP-300 Edition D, version 1 method 305; and,
5) Humidity: test methods according to MIL-STD-810H METHOD 507.6 ; and,
6) Rainfall: test methods according to AECTP-300 Edition D, version 1 method 310; and,
7) Ice: test methods according to AECTP-300 Edition D, version 1 method 311; and,
8) Dust/sand particle size and particle concentration: test methods according to AECTP-300 Edition D, version 1 method 313; and,
9) Maximum elevation and atmospheric pressure: test methods according to
    1) AECTP-300 Edition D, version 1 method 301; or,
    2) MIL-STD-810G, 2008, Method 500.5; or,
    3) MIL-STD-810G w/Change 1, 2014, Method 500.6; or,
    4) MIL-STD-810H, 2019, Method 500.6.

SRS (PRTTDCIS-3113)

~~SRS-62~~ The (D)POP shall be able to withstand the Mechanical specifications with following additional comments on Test Conditions when packaged as designed during transportation, storage and handling:

1) According to STANAG 7213, Edition 1 and its associated ATP-3.3.4.1 Edition A, Version 1 (Tactics, Techniques and Procedures for NATO Air Movements) all cargo, whether or not on pallets or platforms, when carried in aircraft, shall be restrained to the following minimum ultimate factors:
    1) Forward 3.0g; and,
    2) Side 1.5g; and,
    3) Aft 1.5g; and,
    4) Vertical (up) 2.0g; and,
2) Shock: 10 G peak value (11 ms, half sine mechanical shock) according to
    1) AECTP-400, Edition D Version 1 , Method 403; or,
    2) IEC 60068-2-27:2008; or,
    3) MIL-STD-810G, 2008, Method 516.6, Procedure I; or,
    4) MIL-STD-810G w/Change 1, 2014, method 516.7, Procedure I; or,
    5) MIL-STD-810H, 2019, method 516.8, Procedure I; or,
    6) AECTP-400, Edition D Version 1, method 403; or,
    7) IEC 60068-2-27:2008; and,
3) Vibration as per TN-1078 with the following additional comment: test methods according to
    1) AECTP-400, Edition D, Version 1, Method 401; or
    2) IEC 60068-2-64:2008 +AMD1:2019 CSV; or,
    3) MIL-STD-810G, 2008, Method 514.6; or
    4) MIL-STD-810G w/Change 1, 2014, Method 514.7; or
    5) MIL-STD-810H, 2019, Method 514.8; and,
4) Acceleration as per TN-1078 with the following additional comment: with ≤ 10g for transport and ≤ 2g for storage and handling; and, test methods according to
    1) IEC 60068-2-7:1983+AMD1:1986 CSV; or,
    2) MIL-STD-810G, 2008, Method 513.6; or,
    3) MIL-STD-810G w/Change 1, 2014, method 513.7; or,
    4) MIL-STD-810H, 2019, method 513.8; and,
5) Bump as per TN-1078 with the following additional comment: with 10g, 6 ms, 1000 pulses for transport, storage and handling and test methods according to IEC 60068-2-27:2008; and,
6) Drop and topple as per TN-1078 with the following additional comment: test methods according to
    1) IEC 60068-2-31:2008; or,
    2) ISO 8768; or,
    3) MIL-STD-810G, 2008, Method 516.6, Procedure IV; or,
    4) MIL-STD-810G w/Change 1, 2014, method 516.7, Procedure IV; or,
    5) MIL-STD-810H, 2019, method 516.8, Procedure IV; and,
7) Free fall as per TN-1078 with the following additional comment: test methods according to IEC 60068-2-31:2008.

SRS (PRTTDCIS-4033)

~~SRS-63~~ A component defined as Semi-Rugged shall

- Withstand a drop to concrete surface from the height of 75 cm, without any additional protective accessory (i.e. case, rubber boot, etc.) beyond those belonging to the component itself, while being operated. The component shall be dropped on all sides to verify its ability to withstand shock from any direction. Particularly, the display, and other sensitive components shall be tested to verify if they withstand the shock and operate properly; and,
- Have an ingress protection rating of IP 53 as a minimum; and,
- Withstand High Temperature of +49 degree Celsius while being operated; and,
- Withstand Low Temperature of -20 degree Celsius while being operated; and,
- Withstand road test condition while being docked in the vehicle and being operated.

SRS (PRTTDCIS-2484)

~~SRS-64~~ The DPOP shall be subject to the acceptance road test.

SRS (PRTTDCIS-2485)

~~SRS-65~~ If not otherwise specified, all tests shall be performed according to commonly used practices for material test methods or standards (e .g. DIN, ISO and/or MIL-STDs).

SRS (PRTTDCIS-2486)

~~SRS-66~~ The acceptance road test shall be a rugged road test over the distance of 100km including 10km off-road.

SRS (PRTTDCIS-2487)

~~SRS-67~~ The equipment under the acceptance road test shall be capable of withstanding the shocks and vibrations induced by ground transport equipment over the mobility courses described for Type V mobility in SAE-AS8090.

SRS (PRTTDCIS-2488)

~~SRS-68~~ The (D)POP under road test shall be towed by or mounted on a vehicle on all-roads: motorway at 80 km/h, unpaved road (e.g. a gravel road) at 50 km/h and country road at 25 km/h, without sustaining any damage. This shall be demonstrated by a test in which the (D)POP attached to a vehicle will be driven over test tracks. For the verification of these requirements, the following procedures shall be applied in addition to the roadworthiness test:

- Road test over a level hard surface (asphalt or concrete) with a specially prepared course; and,
- The course shall have twelve 10 x 20 cm boards placed 7.5 m apart on the 20 cm face and with the 10 cm face fully above the ground. The edges shall have a 2.5 x 2.5 cm bevel. The sixth and twelfth boards shall be placed 45° to the direction of travel; all the other ones will be placed perpendicular to the direction of travel. The boards shall be long enough to span the vehicle/trailer and shall be anchored securely; and,
- The DPOP shall be subjected to ten (10) laps of the course (one lap is defined as traversing the course in one direction) at each of the following speeds: 8 km/h, 15 km/h, 25 km/h and 30 km/h:
    - After the road test, all (D)POP elements will be inspected using methods defined in the SOW; and,
    - After the test there shall be no evidence of permanent deformation, delamination, buckling or any damage to any of the (D)POP elements.

SRS (PRTTDCIS-3114)

~~SRS-69~~ The (D)POP shall be able to withstand the Sealing specifications with following additional comments on Test Conditions when packaged as designed during transportation, storage and handling:

1) for immersion test methods according to AECTP-300 Edition D, version 1 method 307; and,
2) other requirements according to IEC 60529:1989+AMD1:1999+AMD2:2013 CSV.

SRS (PRTTDCIS-3115)

~~SRS-70~~ The (D)POP shall be able to withstand the Biological and Chemical specification with following additional comments on Test Conditions when packaged as designed during transportation, storage and handling:

1) Salt mist: test methods according to AECTP-300 Edition D, version 1 method 309 or IEC 60068-2-52:2017 RLV; and,
2) Acid atmosphere: test methods according to AECTP-300 Edition D, version 1 method 319 or MIL-STD-810H method 518.2; and,
3) Contamination by fluids: test methods according to AECTP-300 Edition D, version 1 method 314 or MIL-STD-810H method 504.3; and,
4) Mould growth: test methods according to AECTP-300 Edition D, version 1 method 308.

SRS (PRTTDCIS-3245)

~~SRS-71~~ When (D)POP elements are packaged as designed during transportation, storage and handling, all outdoor exposed materials (painted surfaces, sealing, etc.) shall be resistant to Biological and Chemical (BC) contaminants and decontamination agents according to STANAG 4521 edition 2 - NATO AEP-7, edition 5: Chemical, Biological, Radiological and Nuclear (CBRN) contamination survivability factors in the design, testing and acceptance of military equipment.

SRS (PRTTDCIS-2110)

~~SRS-72~~ All Housing Elements, when exposed to climatic and environmental conditions as defined in TN-1078 (climatic, mechanical, sealing, biological and chemical) shall assure that equipment housed in them meets respective manufacturer climatic and environmental specifications for:

- Operation; and,
- Transport; and,
- Storage and handling.

SRS (PRTTDCIS-2481)

~~SRS-73~~ The design of Housing Elements and components to be housed in them shall assure that no active heating and cooling is required for transport, storage, and handling.

SRS (PRTTDCIS-2455)

~~SRS-74~~ Shelter shall be capable of being submerged for a minimum of 2cm from the bottom of the entry door while all drain caps are fully submerged, for 30 minutes without the use of additional external sealing, caulking, taping, and so forth. No water ingress shall be detected.

SRS (PRTTDCIS-2564)

~~SRS-75~~ Equipment shall meet IP Rating, stipulated in TN-1078, without the use of additional external sealing, caulking, taping, and so forth.

SRS (PRTTDCIS-3117)

~~SRS-76~~ The IP ratings, stipulated in TN-1078, shall be in compliance with IEC 60529:1989, AMD1:1999 and AMD2:2013.

SRS (PRTTDCIS-2420)

~~SRS-77~~ All outdoor assemblies and sub-assemblies (Housing Elements, CIS Components (e.g. Antenna, Mast, ODU ...)...) under full operational configuration, shall be capable of withstanding ice accumulation without suffering degradation of system performance (gain, pattern type, sensitivity) and without suffering permanent mechanical damage.

SRS (PRTTDCIS-3116)

~~SRS-78~~ All outdoor assemblies and sub-assemblies (Housing Elements, CIS Components (e.g. Antenna, Mast, ODU ...)...) under full operational configuration, shall not permit water accumulation in pockets, creases, fissures or depressions that could cause structural damage upon freezing.

NOTE (PRTTDCIS-4034)

~~[36]~~ TN-1078 does not contain a Climatic and Environmental Conditions State (i.e. OPE-xx) fitting all PRT TDCIS Operational Use Cases. To that end, OPE-1c is defined in the next section.

2.7.2 Climatic and Environmental Specification for Deployable CIS Assets to be used in tactical exposure conditions (OPE-1c)

SRS (PRTTDCIS-4035)

~~SRS-79~~ OPE-1c State, as defined in this section, shall be considered the same as any other OPE-xx from TN-1078.

SRS (PRTTDCIS-4036)

~~SRS-80~~ OPE-1c compliant Elements shall withstand High Temperature as follow:

- +60 degree Celsius for operation; and,
- +78 degree Celsius for transport, storage and handling.

SRS (PRTTDCIS-4037)

~~SRS-81~~ OPE-1c compliant Elements shall withstand Low Temperature as follow:

- 0 degree Celsius for operation; and,
- -20 degree Celsius for transport, storage and handling.

SRS (PRTTDCIS-4038)

~~SRS-82~~ OPE-1c compliant Elements shall withstand Change of Temperature (temperature shock) as follow:

- For heat radiating devices, 13.4 degree Celsius/min during equipment switch-on. For non-heat radiating devices, or during steady operation, 0.12 degree Celsius/min; and,
- 0.12 degree Celsius/min for natural conditions during transport. 3.5 degree Celsius/min if equipment may be subject to air drops. When moved from open environment into an acclimatised area, the equipment in the applicable storage /transport packaging shall withstand the maximum expected temperature variation of 63 degree Celsius; and,
- 0.12 degree Celsius/min for natural conditions during storage and handling. When moved from open environment into an acclimatised area, the equipment in the applicable storage/transport packaging shall withstand the maximum expected temperature variation of 63 degree Celsius.

SRS (PRTTDCIS-4039)

~~SRS-83~~ OPE-1c compliant Elements shall withstand Solar Radiation up to 1120 W/m2 for operation, transport, storage and handling.

SRS (PRTTDCIS-4040)

~~SRS-84~~ OPE-1c compliant Elements shall withstand Humidity from 5% to 95% for operation, storage, transport and handling with the applicable change of temperature.

SRS (PRTTDCIS-4041)

~~SRS-85~~ OPE-1c compliant Elements shall withstand Rainfall up to 2.38 mm/min for storage, transport and handling, with short duration peaks of up to 41.5 mm/min.

SRS (PRTTDCIS-4042)

~~SRS-86~~ OPE-1c compliant Elements shall withstand Ice up to 37 mm for transport, storage and handling.

SRS (PRTTDCIS-4043)

~~SRS-87~~ OPE-1c compliant Elements shall withstand Hailstones up to 25 mm diameter, 0.9 g/m3 density and 58 m/s terminal velocity for transport, storage and handling.

SRS (PRTTDCIS-4044)

~~SRS-88~~ OPE-1c compliant Elements shall withstand Snow Load up to 50 kg/m2 for transport, storage and handling.

SRS (PRTTDCIS-4045)

~~SRS-89~~ OPE-1c compliant Elements shall withstand Dust and Sand particle size and concentration as follow:

- Up to 2.0 g/m3 of 150 micrometer particles for operation, transport, storage and handling. Sedimentation rate as high as 2.0 g/m2/day; and,
- Average particle hardness of 7 in the Mohs scale, occasionally reaching 9 on that scale.

SRS (PRTTDCIS-4046)

~~SRS-90~~ OPE-1c compliant Elements shall withstand Maximum elevation as follow:

- 4,570 m for operation, storage and handling; and,
- 12,000 m for transport.

SRS (PRTTDCIS-4047)

~~SRS-91~~ OPE-1c compliant Elements shall withstand Maximum and minimum atmospheric pressure from 1,087 mbar to 154 mbar for operation, transport, storage and handling.

SRS (PRTTDCIS-4048)

~~SRS-92~~ OPE-1c compliant Elements shall withstand Shock at a minimum peak value of 10G and pulse duration of 11 ms for operation, transport, storage and handling.

SRS (PRTTDCIS-4049)

~~SRS-93~~ OPE-1c compliant Elements shall withstand Vibration as defined for OPE-1a.

SRS (PRTTDCIS-4050)

~~SRS-94~~ OPE-1c compliant Elements shall withstand Acceleration as defined for OPE-1a.

SRS (PRTTDCIS-4051)

~~SRS-95~~ OPE-1c compliant Elements shall withstand Bump at 10g, 6 ms, 1000 pulses for operation, transport, storage and handling.

SRS (PRTTDCIS-4052)

~~SRS-96~~ OPE-1c compliant Elements shall withstand Drop and topple at a 30 degree angle face and corner during operation, transport, storage and handling.

SRS (PRTTDCIS-4053)

~~SRS-97~~ OPE-1c compliant Elements shall withstand Free Fall for operation, transport, storage and handling as follow:

- 1000 mm for items <2 kg; and,
- 500 mm for items from 2 kg to <5 kg; and,
- 250 mm for items from 5 kg to <10 kg; and,
- 100 mm for items from 10 kg to <50 kg.

SRS (PRTTDCIS-4054)

~~SRS-98~~ OPE-1c compliant Elements shall comply with IP rating as follow:

- IP67 for operation, transport, storage and handling for outdoor cables and connectors; and,
- IP65 for operation, transport, storage and handling for outdoor enclosures; and,
- IP54 for outdoor antennas and associated electronics/ mechanisms, when in operation, and IP55 when in transport, storage and handling; and,
- IP42 for outdoor portable terminals when in operation, and IP55 when in transport, storage and handling; and,
- IP41 for outdoor use handheld terminals when in operation, and IP55 when in transport, storage and handling.

SRS (PRTTDCIS-4055)

~~SRS-99~~ OPE-1c compliant Elements shall withstand Salt mist environments at severity level 4, as described in TN-1078, Section K.3.1.5, for all operation, transport, storage and handling.

SRS (PRTTDCIS-4056)

~~SRS-100~~ OPE-1c compliant Elements shall withstand, in the pertaining operating configuration (i.e., when properly mounted in the intended assembly), occasional exposure to the acid rainfall conditions existing in heavily industrialized areas or in the proximity of fuel burning machinery or vehicles exhaust systems.

SRS (PRTTDCIS-4057)

~~SRS-101~~ OPE-1c compliant Elements shall withstand occasional contamination by exposure to the contaminant fluids listed in MIL-STD-810H, Table 504.3-I.

2.8 CIS Security

SRS (PRTTDCIS-1155)

~~SRS-102~~ All the CIS equipment involving firmware and software, and integrated into or directly supporting the (D)POP, shall be hardened in accordance with the Purchaser's standard security hardening settings, to be provided after Contract Award (CAW).

SRS (PRTTDCIS-1156)

~~SRS-103~~ Each CIS Module shall be implemented with distinct physically independent elements per security domain.

SRS (PRTTDCIS-1227)

~~SRS-104~~ The (D)POP shall employ technology solutions that conforms to the NATO Technical and Implementation Directive on CIS Security AC/322-D/0048-REV3 (hereafter referenced as D48Rev3).

SRS (PRTTDCIS-4320)

~~SRS-105~~ User Password credentials shall comply with NATO approved password hashing algorithms as per AC/322-D(2012)0022, 2020 policy.

SRS (PRTTDCIS-4073)

~~SRS-106~~ Any element including passwords shall allow modification of these passwords.

NOTE (PRTTDCIS-4319)

~~[37]~~ The NATO Information Assurance Product Catalogue (NIAPC - https://www.ia.nato.int/niapc/) provides NATO nations, and NATO civil and military bodies with a catalogue of Information Assurance (IA) Products, Protection Profiles and Packages that are in use or available for procurement to meet operational requirements.

2.9 EMC and EMSEC

NOTE (PRTTDCIS-1142)

~~[38]~~ Electromagnetic Compatibility (EMC) is a measure of a device's ability to operate as intended in its shared operating environment while, at the same time, not affecting the ability of other equipment within the same environment to operate as intended.

NOTE (PRTTDCIS-4058)

~~[39]~~ Electromagnetic Interference (EMI), is a disturbance generated by an electrical device, an electronic device or natural sources that can adversely affect (by electromagnetic induction, electrostatic coupling, or conduction) the performance of other electrical or electronic device located within the same environment.

NOTE (PRTTDCIS-2389)

~~[40]~~ Emission Security (EMSEC) is an analysis of a system’s vulnerability to unauthorized access and subsequent exploitation as a result of issues with electromagnetic emanations from hardware.

NOTE (PRTTDCIS-1143)

~~[41]~~ TEMPEST concerns preventing attacks using compromising radio frequency emanations.

SRS (PRTTDCIS-1144)

~~SRS-107~~ All CIS Nodes, Modules and their electric and electronic components shall comply with the EMC requirements as contained in the *MIL-STD-461G*, latest edition (hereafter referred to as MIL-STD-461G).

SRS (PRTTDCIS-3336)

~~SRS-108~~ All CIS Nodes, Modules and their electric and electronic components shall comply with the Directive 2014/30/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to electromagnetic compatibility.

SRS (PRTTDCIS-1145)

~~SRS-109~~ All CIS Nodes, Modules and their electric and electronic components (inc. EUD) shall be compliant with *SDIP-29/2*, (hereafter referred to as SDIP-29/2).

SRS (PRTTDCIS-1146)

~~SRS-110~~ SDIP-29/2 compliance shall take into consideration the RED/BLACK separation on power lines, equipment and associated data lines (i.e. filters on power lines, minimum distance between RED and BLACK lines, and between RED and BLACK equipment, when operated).

SRS (PRTTDCIS-4059)

~~SRS-111~~ All CIS Nodes, Modules and their electric and electronic components shall be compliant with *CIS Security Technical and Implementation Directive on Emission Security, AC/322-D(2019)0021(INV)*, latest edition.

NOTE (PRTTDCIS-2396)

~~[42]~~ Unless stated otherwise, Fiber cables will be preferred on xS to avoid the need for separation.

SRS (PRTTDCIS-2469)

~~SRS-112~~ TEMPEST testing and certification shall only be performed by approved providers listed on the NIAPC.

SRS (PRTTDCIS-1150)

~~SRS-113~~ When not implemented at Component level, all CIS Nodes and Modules shall implement power filter within their housing element (e.g. transit case or shelter) as per SDIP 29/2.

SRS (PRTTDCIS-2470)

~~SRS-114~~ Power filters shall be sourced from approved vendors listed in the NIAPC.

SRS (PRTTDCIS-1151)

~~SRS-115~~ It shall be possible to restore TEMPEST sealing, in theatre, following the replacement of one or more components.

SRS (PRTTDCIS-2471)

~~SRS-116~~ If Copper cables are used on xS, then shielding shall be carried out.

2.10 International Mobile Telecom

NOTE (PRTTDCIS-4060)

~~[43]~~ Different International Mobile Telecommunication (IMT) terms and names, referring to technology elements, families and generations, are utilized throughout this document. The following are the terminology conventions followed throughout this Document.

NOTE (PRTTDCIS-4061)

~~[44]~~ The 3rd Generation Partnership Project (3GPP) is a worldwide recognized specifications body, whose specifications meet the International Telecommunication Union (ITU) targets for IMT systems. 3GPP specifications ensure multinational and multi-manufacturer interoperability. When accepted by ITU, 3GPP specifications are adopted as ITU standards.

SRS (PRTTDCIS-4062)

~~SRS-117~~ Public Mobile Network Operators (MNO) or Private Provider shall be understood as the entity responsible for the procurement, operation and maintenance of IMT networks and enabling services and applications to users.

SRS (PRTTDCIS-4063)

~~SRS-118~~ IMT User Equipment (IMT-UE) shall be understood as the mobile device, which can take the form of several instantiations (smart personal devices, terminals, dongles, embedded devices, etc.) and provides access to the public MNO or private provider services and applications.

SRS (PRTTDCIS-4064)

~~SRS-119~~ Radio Access Network (RAN) shall be understood as the fixed infrastructure, owned and operated by a public MNO or private provider, with the role to wirelessly connect IMT-UE and the public MNO / private provider fixed network.

SRS (PRTTDCIS-4065)

~~SRS-120~~ Radio Access Technology (RAT) shall be understood as the underlying technology, typically operating at the physical and data link layers, which enables the wireless connection between IMT-UEs and the RAN.

SRS (PRTTDCIS-4066)

~~SRS-121~~ IMT Core Network (IMT-CN) shall be understood as the fixed infrastructure, owned and operated by a public MNO or private provider, with the role to provide network functions (control, management, billing ,etc.) and data transport services, connecting the IMT-UE to a data network (usually the Public Internet).

SRS (PRTTDCIS-4067)

~~SRS-122~~ UMTS shall be understood as 3GPP's Universal Mobile Telecommunications System (UMTS) family of technologies with:

- UMTS Terrestrial Radio Access Network (UTRAN) being the radio interface technology of the UMTS system; and,
- UMTS Core Network being the infrastructure providing the network functions and data transport services of the UMTS system.

SRS (PRTTDCIS-4068)

~~SRS-123~~ LTE shall be understood as the 3GPP's Long-Term Evolution (LTE) family of technologies with:

- Evolved Universal Terrestrial Radio Access (E-UTRA) being the radio interface technology of the LTE system; and,
- Evolved Packet Core (EPC) being the infrastructure providing the network functions and data transport services of the LTE system.

SRS (PRTTDCIS-4069)

~~SRS-124~~ A 5G system shall be understood as 3GPP's technologies superseding LTE technologies with:

- 5G New Radio (5G NR) being the radio interface technology of the 5G system; and,
- 5G Core (5GC) being the infrastructure providing the network functions and data transport services of the 5G system.

SRS (PRTTDCIS-4070)

~~SRS-125~~ 3G shall be understood as the 3rd generation technologies meeting the IMT2000 standards from ITU, from UMTS-family of 3GPP releases (3GPP Release 99 to 7) up to early LTE-family of releases (3GPP Release 8 and 9) .

SRS (PRTTDCIS-4071)

~~SRS-126~~ 4G shall be understood as the 4th generation technologies meeting the IMT-Advanced standards from ITU, from LTE-family of 3GPP Release 10 onwards.

SRS (PRTTDCIS-4072)

~~SRS-127~~ 5G (as a generation) shall be understood as the 5th generation technologies meeting the IMT-2020 standards from ITU, by LTE-family of 3GPP releases and by 5G family of 3GPP releases from Release 15 onwards.

2.11 Timing

SRS (PRTTDCIS-1157)

~~SRS-128~~ Elements requiring timing shall primarily rely on the Network Time Protocol (NTP) feed from the static infrastructure when available.

SRS (PRTTDCIS-4074)

~~SRS-129~~ The Contractor shall design the (D)POP in such a way that its Elements will continue to operate without performance degradation even if NTP feed becomes unavailable.

2.12 Electricity

2.12.1 General

SRS (PRTTDCIS-2310)

~~SRS-130~~ Electrical design and installation shall be compliant with following publications:

- Directive 2014/35/EU of The European Parliament and of The Council of 26 February 2014 – 'low voltage directive' ; and,
- EN 50110-1:2013 Operation of electrical installations. General requirements ; and,
- IEC 60364 series - Low-voltage electrical installations ; and,
- IEC 60309 series - Plugs, socket-outlets and couplers for industrial purposes ; and,
- IEC 61508:2010 - Functional safety of electrical/electronic/programmable electronic safety-related systems – Parts 1 to 7.

SRS (PRTTDCIS-3106)

~~SRS-131~~ Trailer electrical design and installation shall comply with STANAG 2601 edition 4 and associated Allied Engineering Publication (AEP) – 2601 Edition A, version 1.

SRS (PRTTDCIS-3829)

~~SRS-132~~ 230VAC shall be understood as per IEC 60038 standard.

SRS (PRTTDCIS-3818)

~~SRS-133~~ All 230VAC power plugs shall be of CEE 7/7 type, compatible with both type E (French) and type F (Schuko) power sockets.

SRS (PRTTDCIS-2149)

~~SRS-134~~ Electrical distribution shall be in accordance to Portuguese National Regulations.

2.12.2 Electrical Grounding

SRS (PRTTDCIS-4082)

~~SRS-135~~ The power distribution and conditioning shall implement a grounding and potential equalization system, which shall provide effective protection for personnel.

SRS (PRTTDCIS-4083)

~~SRS-136~~ All metallic frames, transformers and electrical apparatus shall be connected to the frame ground.

SRS (PRTTDCIS-4084)

~~SRS-137~~ All metallic panels and covers shall be fastened or connected to the associated frame, in a manner that ensures that they are securely grounded.

SRS (PRTTDCIS-4085)

~~SRS-138~~ Safety grounding and potential equalization shall be implemented in accordance with safety regulations, including IEC 60364-5-54:2011 and AMD1:2021 CSV.

2.12.3 Uninterruptible Power Supply

SRS (PRTTDCIS-1792)

~~SRS-139~~ Uninterruptible Power Supply (UPS) shall provide protection against data loss and CIS components damage due to power failures, voltage dips, voltage spikes, under voltage, overvoltage, switching spikes, interference voltages, frequency changes and harmonic distortion.

SRS (PRTTDCIS-4075)

~~SRS-140~~ UPS shall be compliant with:

1) IEC 62040-1:2017/COR1:2019 Corrigendum 1 - Uninterruptible power systems (UPS) - Part 1: Safety requirements; and,
2) IEC 62040-2:2016 Uninterruptible power systems (UPS) - Part 2: Electromagnetic compatibility (EMC) requirements; and,
3) IEC 62040-3:2011 Uninterruptible power systems (UPS) - Part 3: Method of specifying the performance and test requirements; and,
4) IEC 62040-4:2013 Uninterruptible power systems (UPS) - Part 4: Environmental aspects - Requirements and reporting.

SRS (PRTTDCIS-4076)

~~SRS-141~~ UPS shall meet following requirements:

1) On line, double conversion type; and,
2) Power factor: 0.9; and,
3) Total Harmonic Distortion (THD): < 5% in accordance with IEC TS 61000-3-4; and,
4) System efficiency: > 90% at full load; and,
5) Soft start; and,
6) Zero transfer time; and,
7) Surge suppressor; and,
8) Static bypass for overload; and,
9) Manual bypass for maintenance; and,
10) Battery monitoring; and,
11) Protection against deep discharge of batteries; and,
12) Hot swappable (replacement of the batteries shall be possible without powering down the UPS), rechargeable and user replaceable batteries; and,
13) The sound pressure level shall not exceed 65 dB(A) at 1 meter distance in accordance with ISO 3746:2010.

SRS (PRTTDCIS-4077)

~~SRS-142~~ UPS batteries shall be provided with Material Safety Data Sheet (MSDS) as required by International Civil Aviation Organization (ICAO), and International Air Transportation Association (IATA) for air transportation of dangerous goods.

SRS (PRTTDCIS-4078)

~~SRS-143~~ The battery MSDS shall confirm the batteries testing and certification according to United Nations publication: *Manual of Tests and Criteria for Transportation of Dangerous Goods, part III, subsection 38.3, transport class 9*.

SRS (PRTTDCIS-4079)

~~SRS-144~~ UPS batteries shall be capable of operating safely in a low ventilation environment.

SRS (PRTTDCIS-4080)

~~SRS-145~~ Minimum operating life-time of UPS batteries shall be FIVE (05) years.

SRS (PRTTDCIS-4081)

~~SRS-146~~ UPS shall take single phase Mains/Generator TN-S Supply in accordance with the International Electrotechnical Commission, (IEC) 60038 standard, to power and operate Elements.

NOTE (PRTTDCIS-4509)

~~[45]~~ In architecture diagrams, UPS are shown as included in housing elements. However, UPS implementations are Design Driven. e.g. it may be implemented as a single system supporting multiple elements in the same housing solution, as an embedded or extension of a single element or any combination of those, as long as the UPS implementation does not impact any Functional and Technical Requirements, Implementation Constraints and Performance Targets.

2.13 Lightning Protection

SRS (PRTTDCIS-2198)

~~SRS-147~~ The contractor shall design the most suitable solution for the (D)POP to ensure lightning protection of (D)POP Elements and human life.

SRS (PRTTDCIS-2202)

~~SRS-148~~ The Elements shall not be damaged and shall continue to operate without degradation when subjected to the lightning waveforms conforming to STANAG 4370 edition 7, AECTP 250 - leaflet 254 atmospheric electricity and lightning.

SRS (PRTTDCIS-2203)

~~SRS-149~~ Appropriate Surge Protection Devices (SPD) and other lightning protection measures shall be compliant with following publications:

- IEC 61643-11:2011 ; and,
- IEC 62305:2022 SER ; and,
- IEC 61643-21:2000+AMD1:2008+AMD2:2012 CSV ; and,
- IEC 61643-22:2015.

SRS (PRTTDCIS-2204)

~~SRS-150~~ Where applicable, the earth electrode (e.g. wire and penetration rods) system shall be able to handle the lightning current for dispersal into the ground.

SRS (PRTTDCIS-2199)

~~SRS-151~~ The Lighting Protection System and Grounding System shall be in in compliance with IEC 62305:2022 SER and IEC 60364 series.

SRS (PRTTDCIS-3212)

~~SRS-152~~ SPD shall be provided of at least T1+T2 class for Alternating Current (AC) supply systems and T3 for sensitive communication systems.

SRS (PRTTDCIS-4632)

~~SRS-153~~ SPD shall be provided of at least T2 class for Direct Current (DC) supply systems.

SRS (PRTTDCIS-4086)

~~SRS-154~~ The (D)POP Lightning Protection and EMI/EMC measures shall be compatible with each other.

SRS (PRTTDCIS-4087)

~~SRS-155~~ The grounding cable for Lightning Protection, where applicable, shall be minimum 10 meters long.

2.14 Environmental Control

SRS (PRTTDCIS-3101)

~~SRS-156~~ Environmental Control Units (ECU) design and implementation shall be compliant with following publications:

- Regulation (EC) No 1005/2009 of the European Parliament and of the Council of 16 September 2009 (on substances that deplete the ozone layer); and,
- Pressure Equipment Directive 2014/68/EU, CE marked and provided with EC Declaration of Conformity; and,
- Regulation (EU) No 517/2014 of the European Parliament and of the Council of 16 April 2014 on fluorinated greenhouse gases and repealing Regulation (EC) No 842/2006; and,
- EN – 378 series: Refrigerating systems and heat pumps. Safety and environmental requirements.

SRS (PRTTDCIS-3102)

~~SRS-157~~ The ECU shall be of so called “on/off”-design avoiding use of inverter.

SRS (PRTTDCIS-3103)

~~SRS-158~~ The ECU refrigerant shall be NON-flammable according to EN 378-3:2016+A1:2020.

SRS (PRTTDCIS-3104)

~~SRS-159~~ Hydrofluoroolefines (HFO) refrigerants shall not be used.

2.15 Road Regulation

SRS (PRTTDCIS-2264)

~~SRS-160~~ Trailers shall comply with all applicable regulations of Portugal.

SRS (PRTTDCIS-2483)

~~SRS-161~~ Trailer shall be designed and manufactured to comply with applicable European Union (EU) safety regulations, standards and requirements.

SRS (PRTTDCIS-3118)

~~SRS-162~~ Trailer shall be compliant with the following publications:

- Regulation (EC) No 661/2009 of the European Parliament and of the Council of 13 July 2009 concerning type-approval requirements for the general safety of motor vehicles, their trailers and systems, components and separate technical units intended therefor; and,
- Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC.

SRS (PRTTDCIS-2490)

~~SRS-163~~ With its delivery each trailer shall be provided with expert reports by competent test organizations to prove the compliance with public road traffic and public road traffic licensing regulations, safety regulations and accident preventing regulations in accordance with EU Directives mentioned below.

SRS (PRTTDCIS-2491)

~~SRS-164~~ Trailers shall be supplied with the necessary documents required for its registration in Portugal.

SRS (PRTTDCIS-2493)

~~SRS-165~~ Trailers shall be provided with:

- EU Type-approval Certificate, EU Certificate of Conformity in accordance with Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC; and,
- Roadworthiness Certificate in accordance with Directive 2014/45/EU of the European Parliament and of the Council of 3 April 2014 on periodic roadworthiness tests for motor vehicles and their trailers and repealing Directive 2009/40/EC; and,
- ADR Certificate in accordance with Agreement Concerning the International Carriage of Dangerous Goods by Road (ADR) applicable as from 1 January 2021.

2.16 Transportation

SRS (PRTTDCIS-2265)

~~SRS-166~~ When in the Storage/Transportation mode, the trailer and the shelter weight with all the equipment it carries shall be distributed as evenly as possible over the trailer frame in accordance with STANAG 2236 Multimodal Transport Issues - AMovP-5.

SRS (PRTTDCIS-2494)

~~SRS-167~~ Trailers and shelters shall be designed and manufactured to be towed and transported by road (paved and unpaved), rough terrain, railway, sea (on and under deck of merchant or navy vessels), and air (e.g. C130H, KC 390).

SRS (PRTTDCIS-2498)

~~SRS-168~~ All equipment and components shall be sufficiently robust to remain undamaged when correctly secured and transported across country on trailers and vehicles, on board of vessels or aircraft.

SRS (PRTTDCIS-2492)

~~SRS-169~~ An authorized technical surveillance authority shall approve the mechanical and electrical safety of Trailers. This includes the allowance for transport of the fully equipped trailer (with Power Generators, Antenna...) on public roads, aircrafts, trains and ships.

SRS (PRTTDCIS-2495)

~~SRS-170~~ Trailer equipped with its payload (Power Generators, Antenna ...) shall be capable to Roll On/Roll-Off (RO-RO) during loading/off-loading a C-130 and KC 390 for air transportation.

SRS (PRTTDCIS-2497)

~~SRS-171~~ In order to meet RO-RO requirements, the trailer equipped with its payload (Power Generators, Antenna ...), shall be able to negotiate the maximum required ramp angle and shall comply with the applicable weight, dimensions and stowage criteria.

SRS (PRTTDCIS-2496)

~~SRS-172~~ The preparations of the trailer before loading on the aircraft shall be limited to activities that can be executed in not more than 60 minutes by a trained crew of two (2) without any specialized equipment. This stipulated time limit includes preparation activities for RO-RO of complete configuration of the trailer equipped with its payload (Power Generators, Antenna, etc.).

2.17 Supportability

2.17.1 General

NOTE (PRTTDCIS-3308)

~~[46]~~ The system will represent the simplest design consistent with functional requirements and expected operational conditions and will be capable of being operated and maintained in its operational environment by personnel with a minimum of training.

NOTE (PRTTDCIS-3309)

~~[47]~~ For Reliability, Maintainability, Testability and Availability definitions and methods please refer to:

- MIL-HDBK-338B : Electronic Reliability Design; and,
- IEC 61078:2006 : Analysis techniques for dependability - Reliability block diagram and Boolean methods; and,
- MIL-STD-756B : Reliability Modelling and Prediction; and,
- SR-332 : Reliability Prediction Procedure for Electronic Equipment; and,
- MIL-HDBK-781 : Reliability test methods, plan and environments for engineering development, qualification and production; and,
- MIL-HDBK-470A : Design and developing of maintainable systems; and,
- IEC 60812:2018 : Failure modes and effects analysis (FMEA and FMECA); and,
- MIL–STD–1629A : Failure Mode Effect and Criticality Analysis.

NOTE (PRTTDCIS-3310)

~~[48]~~ For Maintenance Level definitions please refer to the *Maintenance and Support Concepts* Annex of the SOW.

NOTE (PRTTDCIS-3311)

~~[49]~~ For Human Engineering design criteria for supportability please refer to MIL-STD-1472G.

2.17.2 Reliability

SRS (PRTTDCIS-3312)

~~SRS-173~~ The system shall be designed such that a failure or removal of a component or item in the entities equipment does not cause a physical and, or functional failure of another component or item.

SRS (PRTTDCIS-3313)

~~SRS-174~~ The TDCIS Mean Time Between Failures (MTBF) shall be greater than 800 hours in Ground Fixed environment (ref. MIL-HDBK-338B) using certified failure rates data at component level.

SRS (PRTTDCIS-3314)

~~SRS-175~~ The TDCIS Mean Time Between Critical Failures (MTBCF) shall be greater than 1200 hours in Ground Fixed environment (ref. MIL-HDBK-338B) using certified failure rates data at component level.

2.17.3 Maintainability

SRS (PRTTDCIS-3315)

~~SRS-176~~ Mean Time To Repair (MTTR) per relevant Maintenance Levels both Hardware (HLs) and Software including Firmware (SLs) shall be:

1) MTTR for HL/SL1 and HL/SL2 < 30 min; and,
2) MTTR for HL/SL3 < 120 min.

SRS (PRTTDCIS-3316)

~~SRS-177~~ Mean Time To Restore Service (MTTRS) per relevant Maintenance Levels both Hardware (HLs) and Software including Firmware (SLs) shall be:

1) MTTRS for HL/SL1 and HL/SL2 < 20 min
2) MTTRS for HL/SL3 < 60 min

2.17.4 Testability

SRS (PRTTDCIS-3317)

~~SRS-178~~ Fault Detection (FD) rate shall be greater than 95% through Built-In Test (BIT) capable of on-line detection of failure modes.

SRS (PRTTDCIS-3318)

~~SRS-179~~ Fault Isolation (FI) rate without ambiguity shall be greater than 90% through Built-In Test (BIT) capable to isolate the detected internal function/component in failure.

SRS (PRTTDCIS-3319)

~~SRS-180~~ The Built-in-Test (BIT) shall give a fault indication down to at least the level of Line Replaceable Unit (LRU).

SRS (PRTTDCIS-3320)

~~SRS-181~~ BIT fault detection and isolation resultant information shall be recorded in electronic logs.

2.17.5 Product Support

SRS (PRTTDCIS-3321)

~~SRS-182~~ Maintenance Levels apportionment for hardware and software including firmware for corrective and unscheduled maintenance tasks weighted with the relevant failure rate shall be:

1) (Critical + Non-Critical) Failures for HL1-2/SL1-2 > 80%; and,
2) Critical Failures for HL1-2/SL1-2 > 94%; and,
3) (Critical + Non-Critical) Failures for HL3/SL3 < 15%; and,
4) Critical Failures for HL3/SL3 < 6%; and,
5) (Critical + Non-Critical) failures HL4/SL4 < 5%; and,
6) Critical Failures for HL4/SL4 = 0%.

SRS (PRTTDCIS-3322)

~~SRS-183~~ The annual average hours workload for preventive and scheduled maintenance (up to HL3/SL3) shall not exceed (x10) 10 times the relevant annual average hours workload for corrective and unscheduled maintenance (up to HL3/SL3). To be considered for critical and non-critical failures.

SRS (PRTTDCIS-3323)

~~SRS-184~~ Maintenance tasks shall not involve more than TWO (02) persons for Organizational Maintenance (Level 2) HL/SL2 or lower.

SRS (PRTTDCIS-3324)

~~SRS-185~~ The SW updates and setting shall be Software Organizational Maintenance (Level 2) SL2 or lower.

SRS (PRTTDCIS-3325)

~~SRS-186~~ Removable items shall weigh:

1) less than 16.8 kilograms (37 pounds) for more than 99% of LRUs with direct accessibility; and,
2) less than 11.3 kilograms (25 pounds) for more than 99% of LRUs accessible through removal of part or component that is functioning.

SRS (PRTTDCIS-3326)

~~SRS-187~~ Items over 16.8 kilograms (37 pounds) shall be designed for two-person handling.

SRS (PRTTDCIS-3327)

~~SRS-188~~ The combination of BIT and troubleshooting in Technical Publications shall allow for the fault isolation of 100% of detected failures.

SRS (PRTTDCIS-3512)

~~SRS-189~~ The maximum allowable down time when the equipment is deployed shall not exceed 8 hours to fix a fault (i.e. Unscheduled/Corrective Maintenance due to one critical failure or sequence of non-critical failures that lead to a loss of critical function).

SRS (PRTTDCIS-3513)

~~SRS-190~~ The maintenance plan shall consider ad hoc pre deployment and post deployment maintenance actions to allow no down time (i.e. zero hours) due to scheduled maintenance and preventive maintenance during deployment.

2.17.6 Parts Obsolescence

SRS (PRTTDCIS-3328)

~~SRS-191~~ The system shall be designed for a service life of at least 15 years with mid-life upgrade to allow enhancements and obsolescence removal activities with relevant design change with a planned and controlled level of risk and cost.

SRS (PRTTDCIS-3329)

~~SRS-192~~ The system design shall permit to change a specific functional block while maintaining the overall architecture unchanged.

2.18 Availability

NOTE (PRTTDCIS-1507)

~~[50]~~ Services are organised as follow:

1) Communications Services, consisting of:
    1) Transmission Services;
    2) Transport Services;
    3) Protected Core Access (PCA) Services;
    4) Coloured Cloud Access (CCA) Services, at xU, xR and xS levels, including interworking with Mission Network Participants (MNP) (on xU and xS);
    5) Multimedia Access (MMA) Services, at xU, xR and xS level, including interworking with MNP (on xU and xS).
2) Infrastructure Services, in turn enabling:
    1) Business Support Services, including Local Cross-Domain Services;
    2) Community Of Interest (COI) Services;
    3) Service Management and Control (SMC) Services;
    4) CIS Security Services.

NOTE (PRTTDCIS-2923)

~~[51]~~ DPOP Availability Targets are formulated for Communications Services and Infrastructure Services provided by the various CIS elements of the DPOP.

NOTE (PRTTDCIS-2924)

~~[52]~~ Intrinsic availability calculation methods are taken into consideration for the assigned system availability targets.

NOTE (PRTTDCIS-2925)

~~[53]~~ Availability Targets assume the following:

1) No outages related to misconfiguration or misuse of the systems concerned; and
2) Mean logistics delay time is zero; and
3) Availability targets of the enabling services, as formulated here.

NOTE (PRTTDCIS-2926)

~~[54]~~ Availability Targets for Service Management and Control and CIS Security are not separately specified. Instead, they are subsumed into Communications services, as they are enabling/transversal to them.

NOTE (PRTTDCIS-2927)

~~[55]~~ From the assumptions above, service continuity and recovery from outages are solely contingent upon the intrinsic availability of the hardware and firmware supporting those systems, including any non-CIS elements related to the integration and operation of the integrated hardware.

SRS (PRTTDCIS-2928)

~~SRS-193~~ The design shall be driven by the intrinsic availability targets for the hardware and firmware, in order to achieve the stated minimum DPOP availability levels.

2.19 Paint and Corrosion

SRS (PRTTDCIS-1367)

~~SRS-194~~ All external visible surfaces of outdoor assemblies and subassemblies of Housing Elements, Nodes, Modules and Components (e.g. Shelters, Trailers, Cases, Antenna, Mast, ODU ...) shall be painted in RAL 840R 6014, non-gloss or equivalent.

SRS (PRTTDCIS-1368)

~~SRS-195~~ The exterior paint finish shall be guaranteed for a minimum of ten (10) years without signs of deterioration.

SRS (PRTTDCIS-3845)

~~SRS-196~~ The exterior paint finish shall ensure an anti-corrosion protection of a minimum C5I (Very High) as per ISO 12944-5:2019.

SRS (PRTTDCIS-3182)

~~SRS-197~~ There shall be no shiny, reflective, bright color or light visible on the equipment, this applies during transit, transport and operation. When surfaces cannot be treated by painting, an alternative solution shall be provided (i.e. protection by a specific cover).

SRS (PRTTDCIS-3183)

~~SRS-198~~ Paint of all external surfaces for all outdoor assemblies and sub-assemblies (Housing Elements, CIS Components (e.g. Antenna, Mast, ODU, etc.) shall meet requirements of STANAG 4360, Edition 3 and its associated AEPs:

- AEP-64, Edition A, Version 1: Performance requirements for paint systems resistant to chemical agents and decontaminants, for the protection of land military equipment; and,
- AEP-65, Edition A, Version 1: Performance requirements and test method for paint systems resistant to chemical warfare agents.

SRS (PRTTDCIS-4088)

~~SRS-199~~ Elements shall be made of non-corroding metallic materials.

SRS (PRTTDCIS-4089)

~~SRS-200~~ Dissimilar metals shall not be used in intimate contact unless suitably protected against electrolytic corrosion.

3 High Level Specification

3.1 General

NOTE (PRTTDCIS-1213)

~~[56]~~ The TDCIS is a modular system that can support operations up to Brigade level. It can also support smaller deployments with a subset of the full system, to both Battalion or Company level operations.

NOTE (PRTTDCIS-1216)

~~[57]~~ The TDCIS will not support any deployment larger than a full Brigade.

NOTE (PRTTDCIS-1214)

~~[58]~~ The operations to be supported are either within the National or Multi-national environment, in response to an agreed level of support with NATO or other allied countries.

NOTE (PRTTDCIS-1217)

~~[59]~~ The TDCIS is layered in following meshes:

- Brigade level (highest tactical command) to National Defence Network (NDN) over SATCOM with an HF fallback capability;
- Internal Brigade and Brigade towards Battalion over the tactical backbone mesh network;
- Internal Battalion over the tactical backbone mesh network;
- Battalion to Company and Company to Company over direct radio based connection;
- Company to Platoons over tactical radios.

NOTE (PRTTDCIS-1218)

~~[60]~~ Each echelon will have typical Functional Application Services (FAS) relative to their Information Exchange Requirements (IER).

NOTE (PRTTDCIS-1445)

~~[61]~~ The TDCIS will be configured with an initial mission data set prior to the deployment. This will be done in the garrison Mission Preparation Center (MPC).

NOTE (PRTTDCIS-1188)

~~[62]~~ The TDCIS is composed of different Nodes installed in shelters. The shelters are mounted on all-terrain vehicles so that they can be located in the operational scenario as per the mission requirements. Vehicles are not in scope of this project.

NOTE (PRTTDCIS-1189)

~~[63]~~ The TDCIS operates as a stand-alone system, as a NDN extension or any combination of both.

NOTE (PRTTDCIS-1200)

~~[64]~~ The TDCIS can work either as a whole system, or in smaller subsets; e.g. a subset that supports a Battalion deployment, in this latter case the required nodes for the Battalion being a subset of the full TDCIS.

NOTE (PRTTDCIS-3248)

~~[65]~~ The TDCIS, or some of its sub-elements, will be configured with a Mission Data Set, specific to the mission and prior to the deployment. This will be performed by PRT staff in the Mission Preparation Centre (MPC). MPC is not a deliverable of this project.

NOTE (PRTTDCIS-1201)

~~[66]~~ As illustrated on the following figure, six different node variants build up the full system capability. These nodes are:

- **Access Node** (AN):Provides Brigade echelon users with a set of communications and information systems required to support the command and control action of the respective Commander;
- **Battalion Communication Centre** (BCC): Provides Battalion echelon users with the set of communications and information systems required to support the command and control action of the respective Commander;
- **Company Communication Centre** (CCC): Provides Company echelon users with the set of communications and information systems required to support the command and control action of the respective Commander;
- **Transit Node** (TN): Provides a backbone network node. Assures the automatic routing of information through a set of redundant connections and different types of physical media in order to create the tactical network backbone;
- **Radio Access Point** (RAP): Provides full integration of tactical mobile user in TDCIS communications infrastructure;
- **Rear Link** (RL): Provides reach-back capability to the static infrastructure.

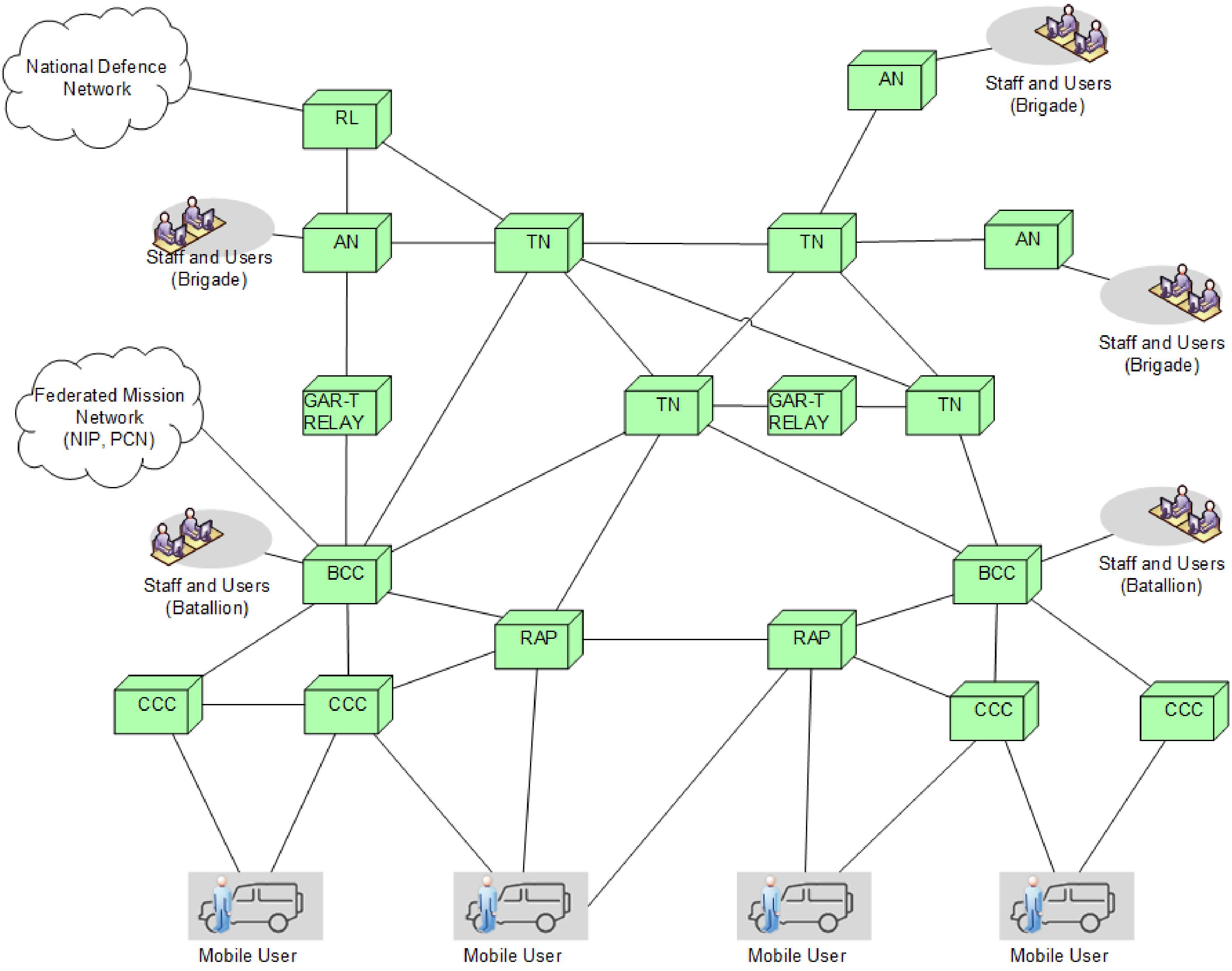

National Defence Network
RL
AN
Staff and Users (Brigade)
TN
TN
AN
Staff and Users (Brigade)
AN
Staff and Users (Brigade)
Federated Mission Network (NIP, PCN)
GAR-T RELAY
TN
GAR-T RELAY
TN
Staff and Users (Batallion)
BCC
BCC
Staff and Users (Batallion)
RAP
RAP
CCC
CCC
CCC
CCC
Mobile User
Mobile User
Mobile User
Mobile User

Figure 5 - TDCIS Nodes in context

NOTE (PRTTDCIS-1190)

~~[67]~~ The backbone of the TDCIS is composed of TN that create an independent wireless and/or wired network infrastructure that interconnects AN, BCC, RAP, CCC and RL nodes.

NOTE (PRTTDCIS-1191)

~~[68]~~ In the lower level backbone of the network, the BCC connects to the CCC and to the RAP over direct wireless and/or wired links.

NOTE (PRTTDCIS-1192)

~~[69]~~ Side-standing CCC can connect with each other through wired or wireless links.

NOTE (PRTTDCIS-1443)

~~[70]~~ The wireless node to node connection is ensured by

- The High Capacity Line Of Sight (HCLOS) radio system between AN, BCC, TN, RAP and RL; and,
- The Mini-Line of Sight (Mini-LOS) radio system between BCC and CCC; and,
- The Broadband IP Radio system for AN, BCC, CCC and RAP nodes.

NOTE (PRTTDCIS-1193)

~~[71]~~ Mobile Users (vehicles other than the TDCIS vehicles) and dis-mounted soldiers are connected to the TDCIS through the RAP or through the CCC, using the Combat Net Radio (CNR) or The Broadband IP Radio System.

NOTE (PRTTDCIS-1194)

~~[72]~~ The reach back to the NDN of Portugal from TDCIS is achieved through the RL node, which can be wire-connected to either an AN, TN, BCC, RAP or CCC. This will allow PRT to deploy standalone Battalions and Companies. The RL connects to the NDN through SATCOM or HF Transmission Systems.

NOTE (PRTTDCIS-4633)

~~[73]~~ The connectivity concept described in this section is not meant to be limitative. Ultimately, any TDCIS Node can connect to any other TDCIS Node as long as they share compatible Transmission Systems.

NOTE (PRTTDCIS-1204)

~~[74]~~ AN, BCC and CCC are nodes supporting users directly connected to them. TN, RAP and RL are nodes which create the required TDCIS network connectivity.

NOTE (PRTTDCIS-1202)

~~[75]~~ Besides the nodes, the TDCIS also includes a pool of GAR-T HCLOS Relay variant trailers that can either:

- be assigned to any node to enable or augment its HCLOS capacity; or
- be used to extend the reach of a HCLOS links.

NOTE (PRTTDCIS-4467)

~~[76]~~ Besides the nodes, the TDCIS also includes a NS Kit which extends the TDCIS and its Nodes with access to NS services hosted in the Theatre but also from the Federation with Mission Partners.

NOTE (PRTTDCIS-4386)

~~[77]~~ The TDCIS includes Pooled Elements to be used by the Customer to augment, upgrade or enable TDCIS Nodes with more functionalities.

NOTE (PRTTDCIS-2932)

~~[78]~~ The breakdown of the TDCIS is illustrated in the following figure.

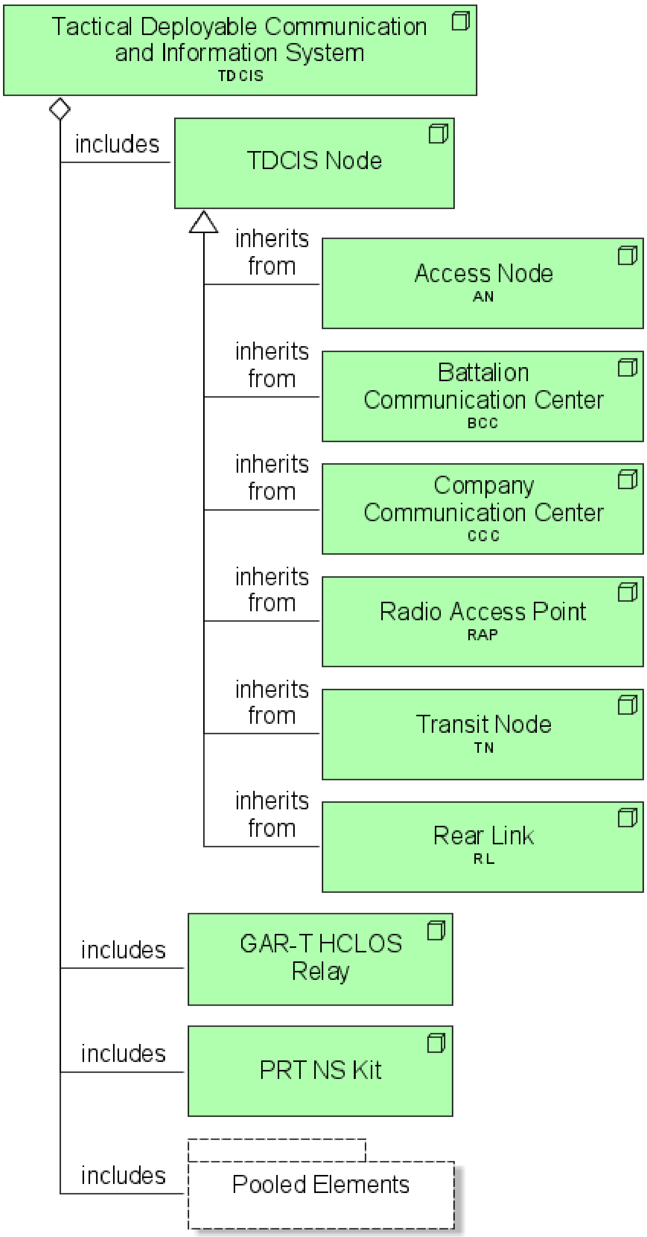


Figure 6 - TDCIS breakdown

3.2 TDCIS Nodes

3.2.1 General

SRS (PRTTDCIS-1239)

~~SRS-201~~ Each TDCIS node architecture shall adhere to the architecture depicted on following figure:

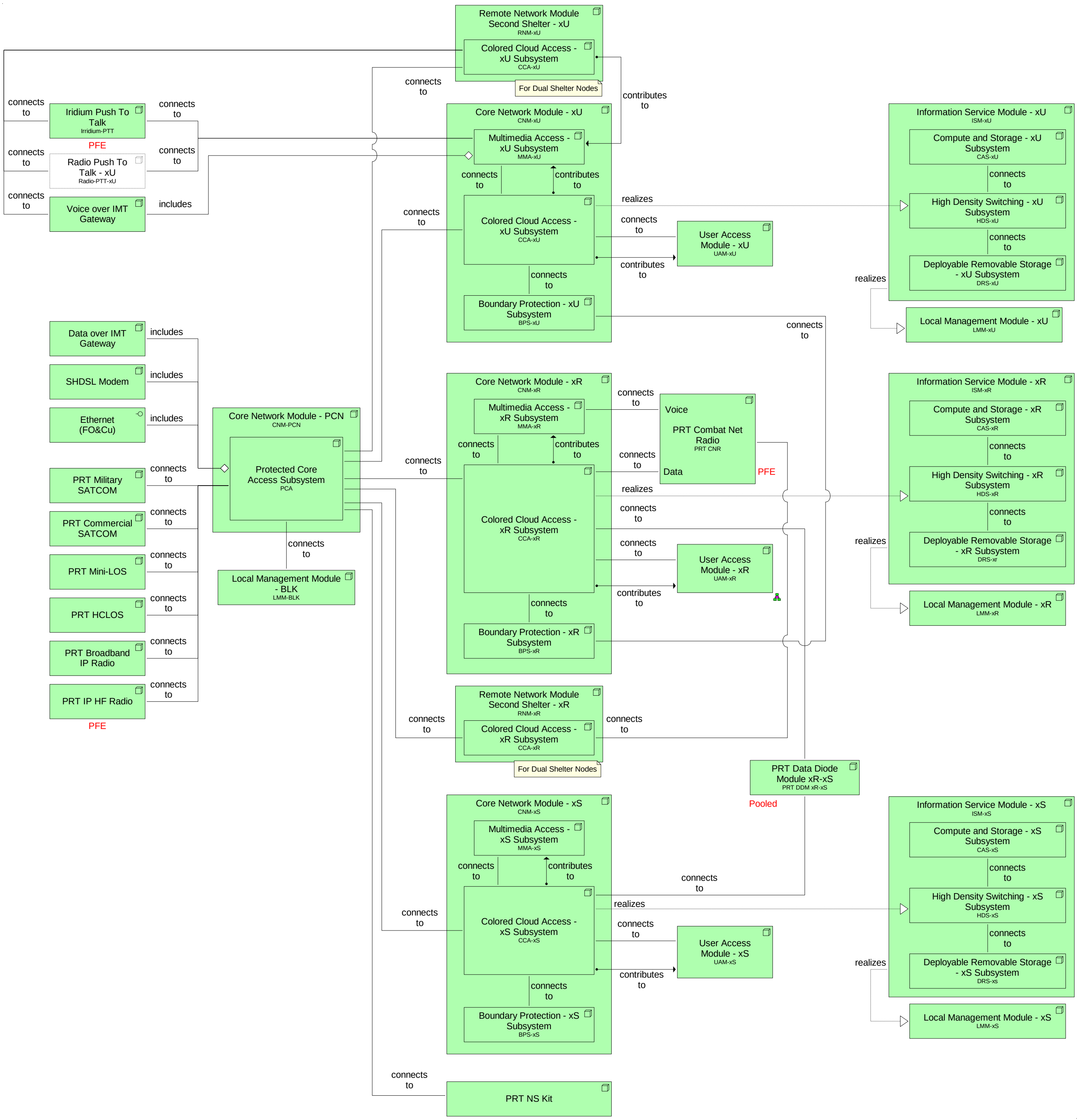

Remote Network Module Second Shelter - xU
RNM-xU
Colored Cloud Access - xU Subsystem
CCA-xU
For Dual Shelter Nodes
connects to
contributes to
Iridium Push To Talk
Iridium-PTT
PFE
Radio Push To Talk - xU
Radio-PTT-xU
Voice over IMT Gateway
includes
Core Network Module - xU
CNM-xU
Multimedia Access - xU Subsystem
MMA-xU
Colored Cloud Access - xU Subsystem
CCA-xU
Boundary Protection - xU Subsystem
BPS-xU
User Access Module - xU
UAM-xU
realizes
Information Service Module - xU
ISM-xU
Compute and Storage - xU Subsystem
CAS-xU
High Density Switching - xU Subsystem
HDS-xU
Deployable Removable Storage - xU Subsystem
DRS-xU
Local Management Module - xU
LMM-xU
Data over IMT Gateway
SHDSL Modem
Ethernet (FO&Cu)
PRT Military SATCOM
PRT Commercial SATCOM
PRT Mini-LOS
PRT HCLOS
PRT Broadband IP Radio
PRT IP HF Radio
PFE
Core Network Module - PCN
CNM-PCN
Protected Core Access Subsystem
PCA
Local Management Module - BLK
LMM-BLK
Core Network Module - xR
CNM-xR
Multimedia Access - xR Subsystem
MMA-xR
Colored Cloud Access - xR Subsystem
CCA-xR
Boundary Protection - xR Subsystem
BPS-xR
Voice
PRT Combat Net Radio
PRT CNR
Data
PFE
User Access Module - xR
UAM-xR
Information Service Module - xR
ISM-xR
Compute and Storage - xR Subsystem
CAS-xR
High Density Switching - xR Subsystem
HDS-xR
Deployable Removable Storage - xR Subsystem
DRS-xr
Local Management Module - xR
LMM-xR
Remote Network Module Second Shelter - xR
RNM-xR
Colored Cloud Access - xR Subsystem
CCA-xR
For Dual Shelter Nodes
PRT Data Diode Module xR-xS
PRT DDM xR-xS
Pooled
Core Network Module - xS
CNM-xS
Multimedia Access - xS Subsystem
MMA-xS
Colored Cloud Access - xS Subsystem
CCA-xS
Boundary Protection - xS Subsystem
BPS-xS
User Access Module - xS
UAM-xS
Information Service Module - xS
ISM-xS
Compute and Storage - xS Subsystem
CAS-xS
High Density Switching - xS Subsystem
HDS-xS
Deployable Removable Storage - xS Subsystem
DRS-xS
Local Management Module - xS
LMM-xS
PRT NS Kit

Figure 7 - Generic Node Architecture

SRS (PRTTDCIS-1195)

~~SRS-202~~ The TDCIS shall supports three (3) security domains, each with variants as follow:

- UNCLASSIFIED (xU) with National UNCLASSIFIED (Nat-U) as the single variant; and,
- RESTRICTED (xR) with the National RESTRICTED (Nat-R) as the single variant; and,
- SECRET (xS) with MISSION SECRET (MS) and National SECRET (Nat-S) as variants.

SRS (PRTTDCIS-3021)

~~SRS-203~~ Each security domain shall be prepared and configured specific for the mission prior to the deployment.

SRS (PRTTDCIS-3022)

~~SRS-204~~ When a security domain is configured in a Nat-X variant, it shall act as a PRT NDN extension and integrate with it.

SRS (PRTTDCIS-2548)

~~SRS-205~~ TDCIS subsets planned for different missions shall be isolated from each other. Therefore, the subsets shall not share any configuration parameters nor exchange any data with each other, not even between domains of same classification level.

SRS (PRTTDCIS-1206)

~~SRS-206~~ At the end of each mission, data will be archived and the TDCIS will be returned to the non-configured-state, ready for a new deployment configuration. This de-configuration shall be performed in accordance with national and/or NATO regulations.

SRS (PRTTDCIS-1209)

~~SRS-207~~ The TDCIS shall have Protected Core Network (PCN) capabilities as per *STANAG 5637*, namely PCN-1 and PCN-2 Interfaces as well as E-Node and P-Function functionalities.

SRS (PRTTDCIS-1450)

~~SRS-208~~ The breakdown of the AN is illustrated in the following figure. It identifies the required Modules, Transmission Systems and housing elements it is composed of. Each AN shall be built upon the building blocks as identified in this AN Breakdown.

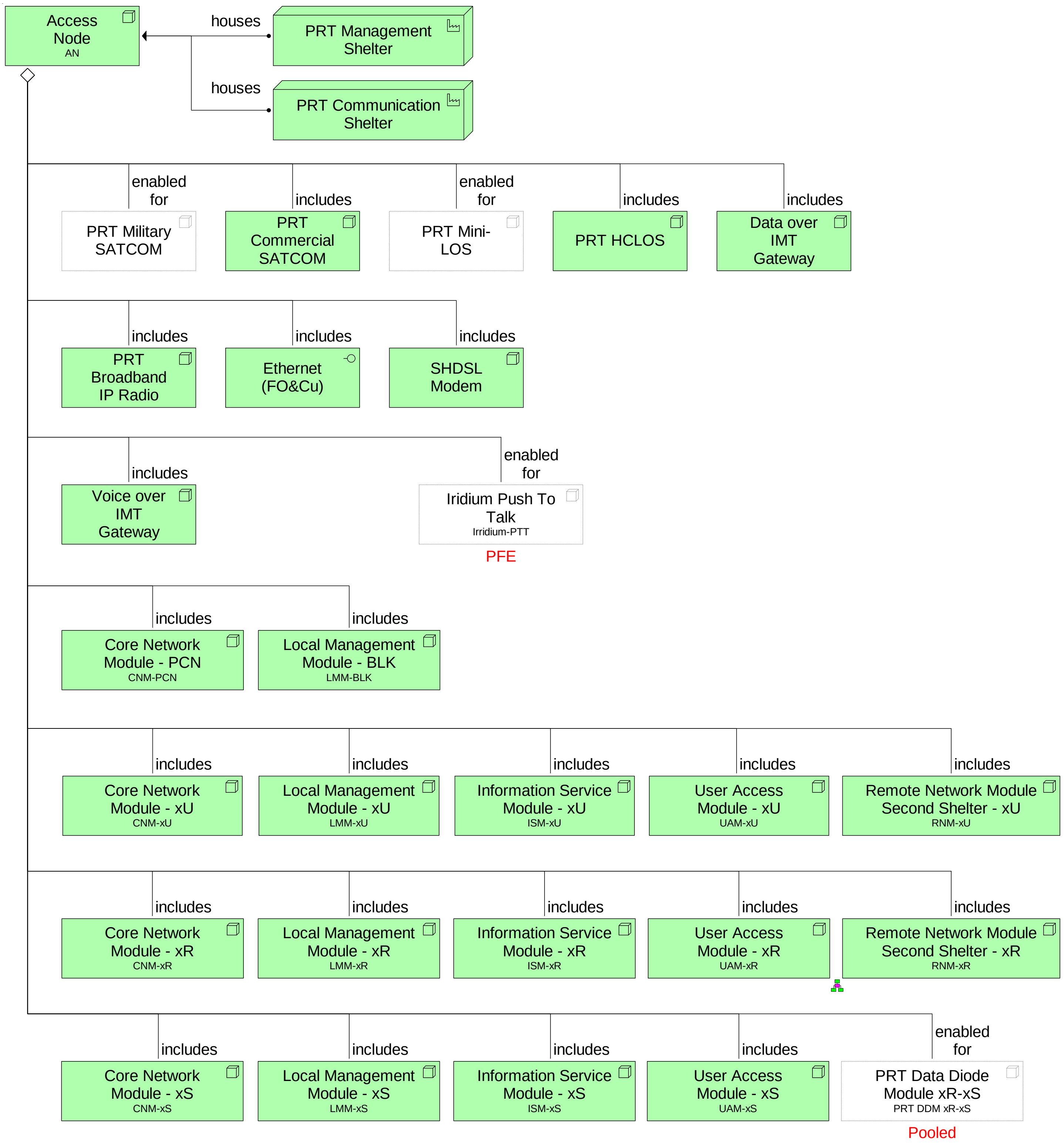


Figure 8 - Access Node breakdown

SRS (PRTTDCIS-1451)

~~SRS-209~~ The breakdown of the BCC is illustrated in the following figure. It identifies the required Modules, Transmission Systems and housing elements it is composed of. Each BCC shall be built upon the building blocks as identified in this figure.

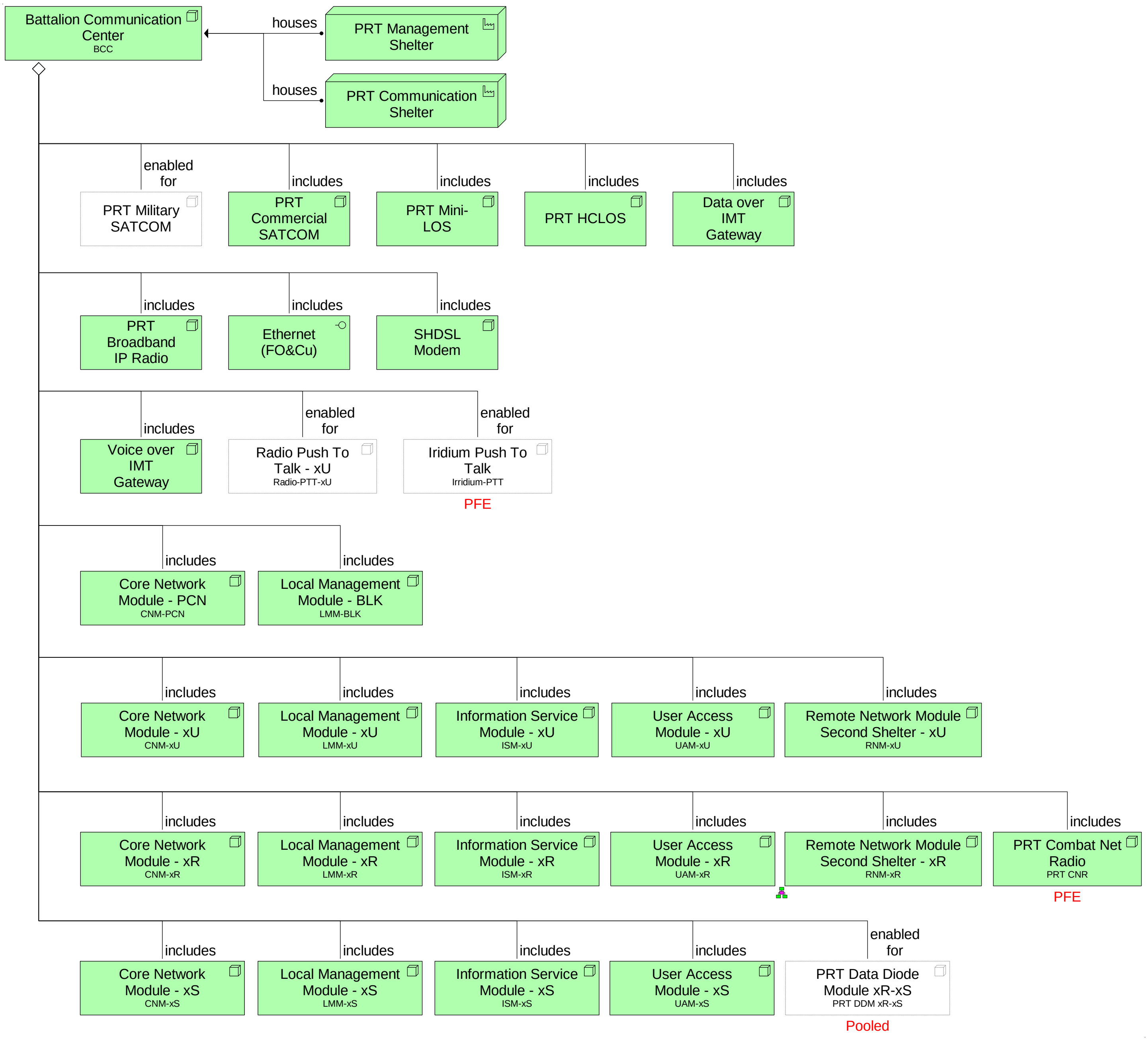


Figure 9 - Battalion Communication Center breakdown

SRS (PRTTDCIS-1452)

~~SRS-210~~ The breakdown of the CCC is illustrated in the following figure. It identifies the required Modules, Transmission Systems and housing elements it is composed of. Each CCC shall be built upon the building blocks as identified in this figure.

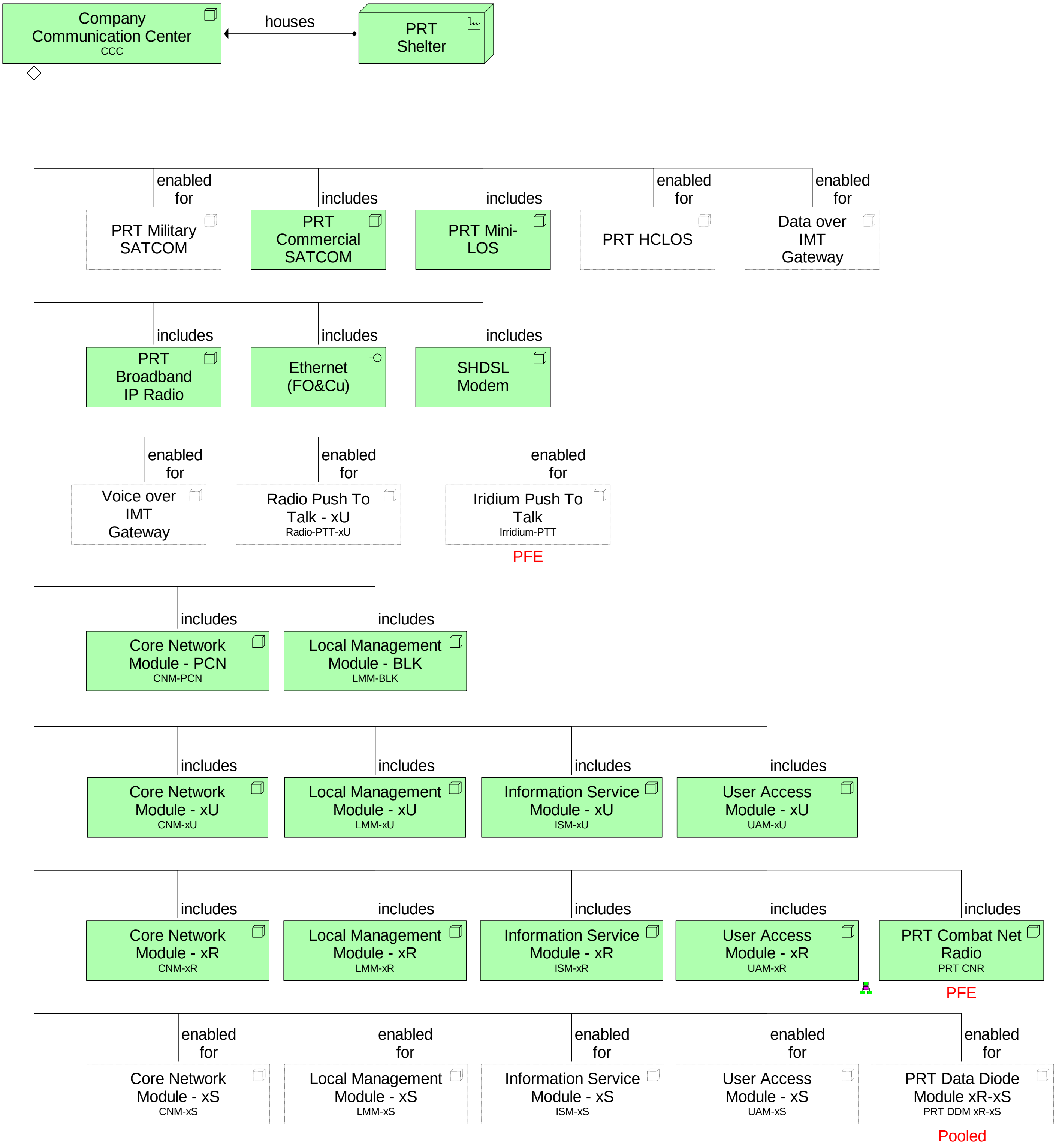


Figure 10 - Company Communication Center breakdown

SRS (PRTTDCIS-1453)

~~SRS-211~~ The breakdown of the TN is illustrated in the following figure. It identifies the required Modules, Transmission Systems and housing elements it is composed of. Each TN shall be built upon the building blocks as identified in this reference.

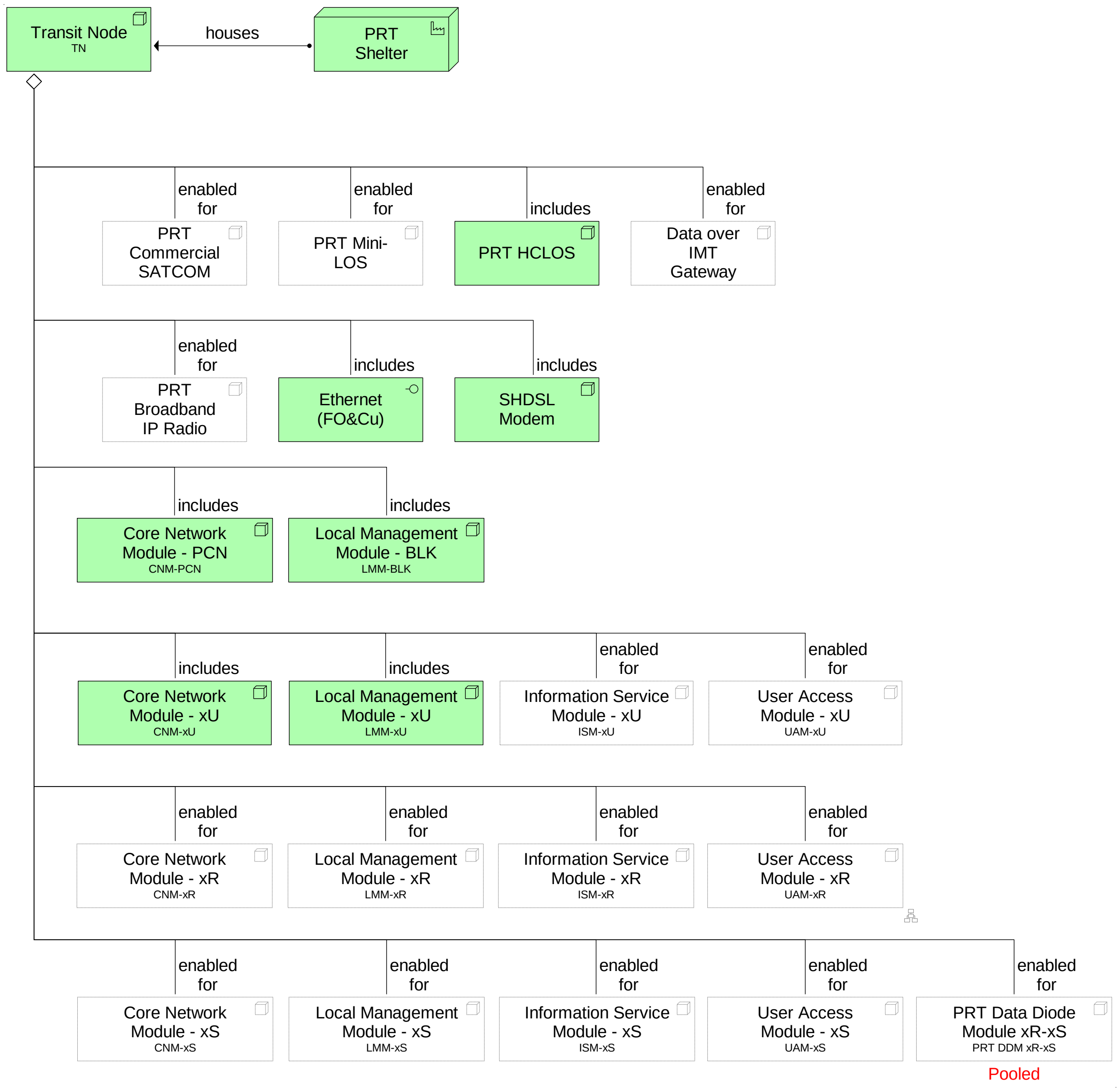


Figure 11 - Transit Node breakdown

SRS (PRTTDCIS-1454)

~~SRS-212~~ The breakdown of the RAP is illustrated in the following figure. It identifies the required Modules, Transmission Systems and housing elements it is composed of. Each RAP shall be built upon the building blocks as identified in this reference.

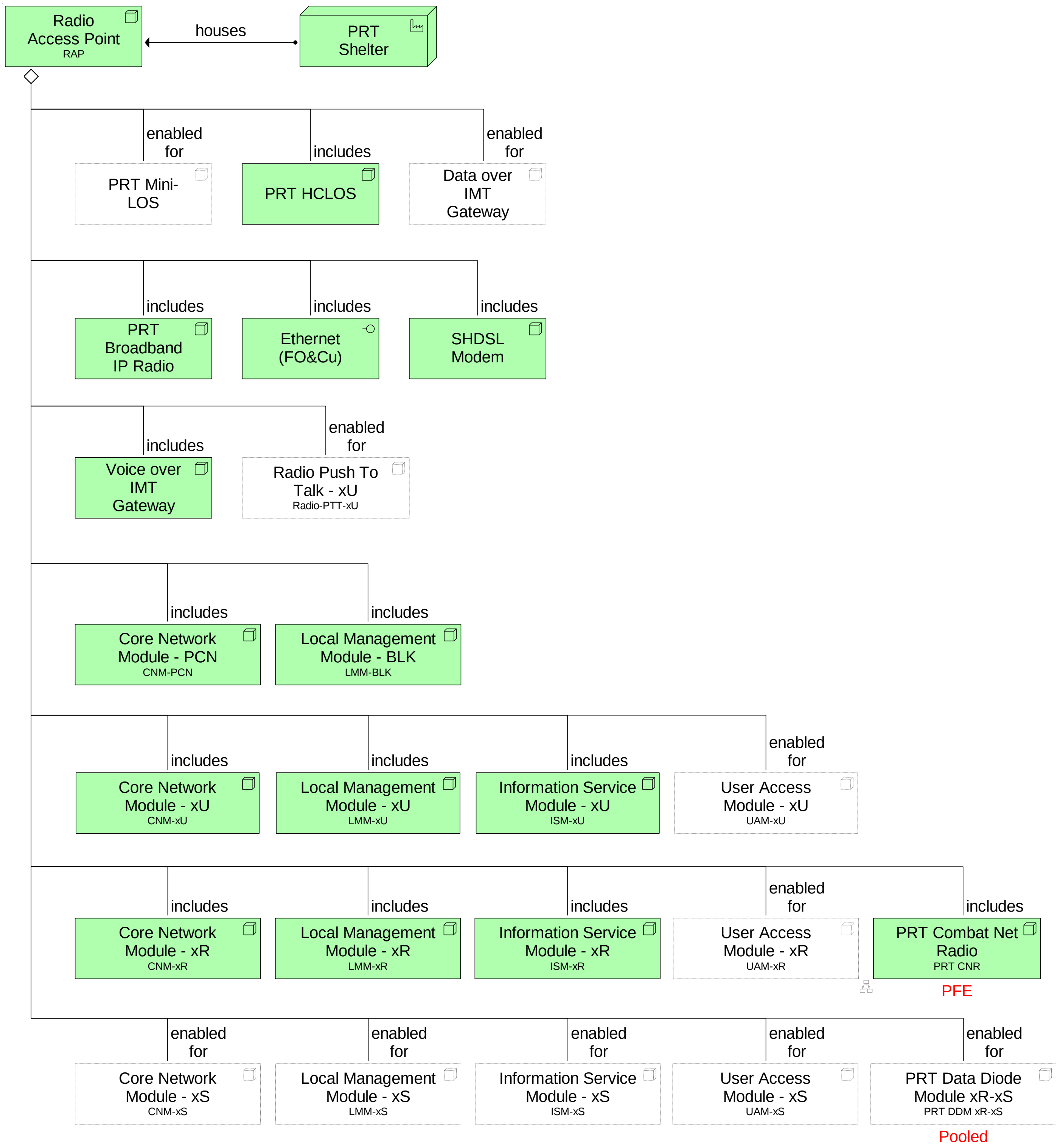


Figure 12 - Radio Access Point breakdown

SRS (PRTTDCIS-1455)

~~SRS-213~~ The breakdown of the RL is illustrated in the following figure. It identifies the required Modules, Transmission Systems and housing elements it is composed of. Each RL shall be built upon the building blocks as identified in this reference.

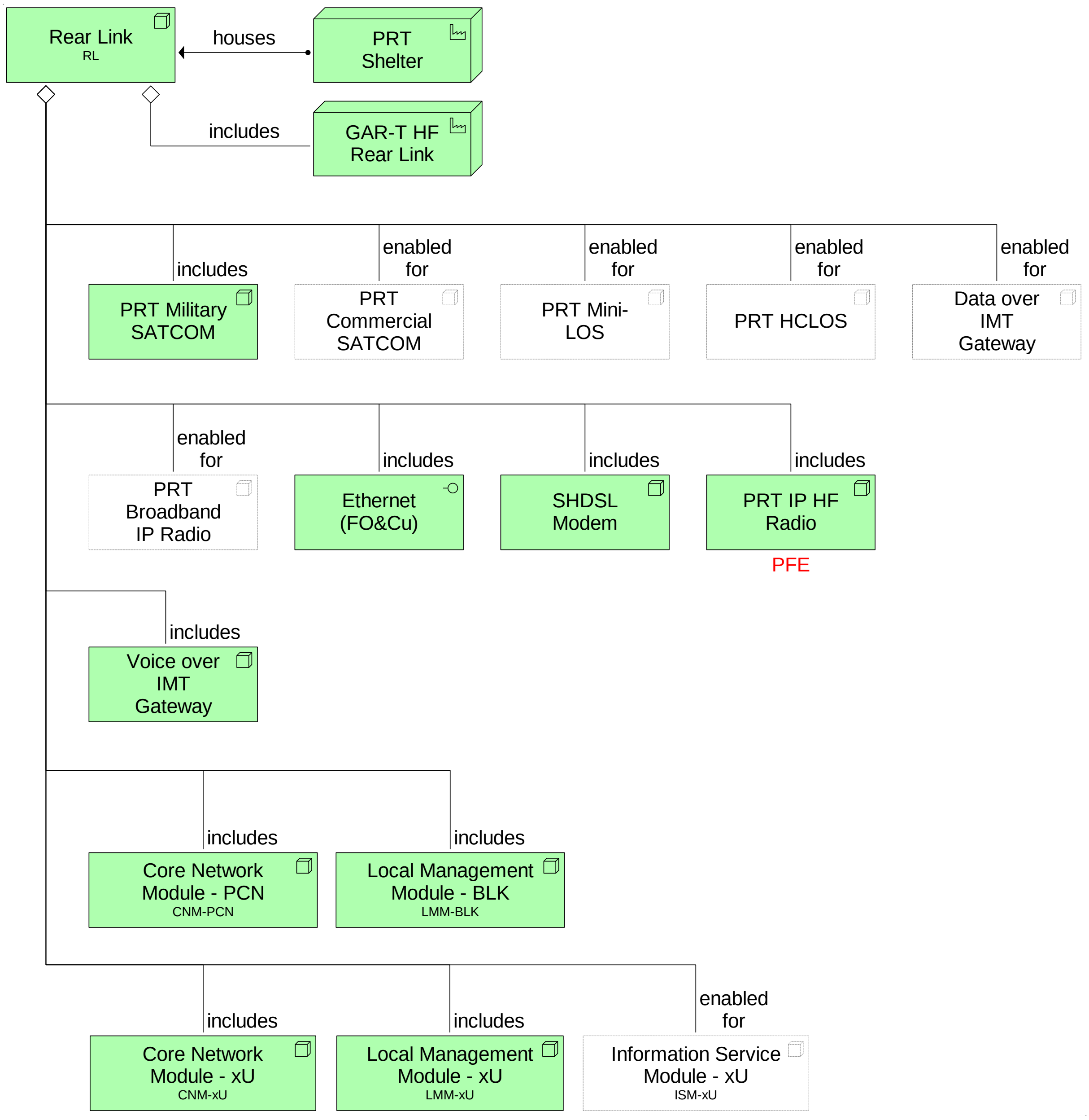


Figure 13 - Rear Link breakdown

3.2.2 Services

NOTE (PRTTDCIS-2921)

~~[79]~~ TDCIS Nodes host:

1) Communications Services; and
2) CIS Security Services; and
3) Infrastructure Service and
4) Business Support Services; and
5) COI Services; and
6) Service Management and Control Service.

SRS (PRTTDCIS-2461)

~~SRS-214~~ TDCIS Nodes shall provide following services on xU to their directly connected End Users and System Administrators as per following table:

<u>*Legend:*</u>

- *Local*: Service is locally hosted in the Node
- *Remote*: Service is remotely consumed from another deployed TDCIS Node (AN, BCC or CCC)
- *NDN*: Service is remotely consumed from the PRT NDN.

Service	Service Category	AN	BCC	CCC	RAP	TN	RL
Functional Area Services	Community of Interest	Local	Local	Local	Local	-	-
Email	Business Support	NDN	NDN	NDN	NDN	NDN	NDN
Collaborative Information Portal	Business Support	NDN	NDN	NDN	NDN	NDN	NDN
Video Teleconference	Business Support	NDN	NDN	NDN	NDN	NDN	NDN
Voice Collaboration (IP)	Business Support	Local	Local	Local	Local	Local	Local
Voice Collaboration (Analogue)	Business Support	Local	Local	Local	Local	Local	Local
Printing and Scanning	Business Support	Local	Local	Local	-	-	-
Interconnection to Nations	N/A	-	Local	-	-	-	-
Antivirus	CIS Security	Local	Local	Local	Local	Local	Local
Network Access Control	CIS Security	Local	Local	Local	Local	Local	Local
Encryption	CIS Security	Local	Local	Local	Local	Local	Local
Log Aggregation	CIS Security	-	-	-	-	-	-
Online Vulnerability Assessment	CIS Security	-	-	-	-	-	-

Table 1 - Services per Node on xU

SRS (PRTTDCIS-4234)

~~SRS-215~~ TDCIS Nodes shall provide following services on xR to their directly connected End Users and System Administrators as per following table:

Legend:

- *Local*: Service is locally hosted in the Node
- *Remote*: Service is remotely consumed from another deployed TDCIS Node (AN, BCC or CCC)
- *NDN*: Service is remotely consumed from the PRT NDN.

Service	Service Category	AN	BCC	CCC	RAP	TN	RL
Functional Area Services	Community of Interest	Local	Local	Local	Local	-	-
Email	Business Support	Local	Local	Local	Remote	-	-
Collaborative Information Portal	Business Support	Local	Local	Local	Remote	-	-
Video Teleconference	Business Support	Local	Local	Remote	Remote	-	-
Voice Collaboration (IP)	Business Support	Local	Local	Local	Local	-	-
Printing and Scanning	Business Support	Local	Local	Local	-	-	-
Interconnection to Nations	N/A	-	-	-	-	-	-
Antivirus	CIS Security	Local	Local	Local	Local	-	-
Network Access Control	CIS Security	Local	Local	Local	Local	-	-
Encryption	CIS Security	Local	Local	Local	Local	-	-
Log Aggregation	CIS Security	-	-	-	-	-	-
Online Vulnerability Assessment	CIS Security	-	-	-	-	-	-

Table 2 - Services per Node on xR

SRS (PRTTDCIS-4235)

~~SRS-216~~ TDCIS Nodes shall provide following services on xS to their directly connected End Users and System Administrators as per following table:

Legend:

- *Local*: Service is locally hosted in the Node
- *Remote*: Service is remotely consumed from another deployed TDCIS Node (AN, BCC or CCC)
- *NDN*: Service is remotely consumed from the PRT NDN.

Service	Service Category	AN	BCC	CCC	RAP	TN	RL
Functional Area Services	Community of Interest	Local	Local	-	-	-	-
Email	Business Support	Local	Local	-	-	-	-
Collaborative Information Portal	Business Support	Local	Local	-	-	-	-
Video Teleconference	Business Support	Local	Local	-	-	-	-
Voice Collaboration (IP)	Business Support	Local	Local	-	-	-	-
Printing and Scanning	Business Support	Local	Local	-	-	-	-
Interconnection to Nations	N/A	-	Local	-	-	-	-
Antivirus	CIS Security	Local	Local	-	-	-	-
Network Access Control	CIS Security	Local	Local	-	-	-	-
Encryption	CIS Security	Local	Local	-	-	-	-
Log Aggregation	CIS Security	-	-	-	-	-	-
Online Vulnerability Assessment	CIS Security	-	-	-	-	-	-

Table 3 - Services per Node on xS

SRS (PRTTDCIS-4368)

~~SRS-217~~ TDCIS Nodes shall provide following Cross Domain Services to their directly connected End Users and System Administrators as per following table:

Legend:

- *Implemented*: Service is implemented in the Node
- *Pooled:* Service is ready to be deployed using pooled appliances.

Service	Service Category	AN	BCC	CCC	RAP	TN	RL
Cross Domain xU-xR	CIS Security	Implemented	Implemented	Implemented	Implemented	-	-
Cross Domain xR-xS	CIS Security	Pooled	Pooled	-	-	-	-

Table 4 - Cross Domain Services per Node

NOTE (PRTTDCIS-1526)

~~[80]~~ TDCIS Nodes will have multiple Voice service integration options by means of following gateways:

- On the xU security domain:
  - **Voice over IMT** for integration with the telephony of an IMT network; and,
  - **Iridium PTT** for integration to the Iridium Satellite Phone Service; and,
  - **Radio PTT - xU** for integration with a PTT based radio transmitter; and,
- On the xR security domain:
  - **Radio PTT - xR** for integration of the PTT based Voice functionality of the CNR.

SRS (PRTTDCIS-1435)

~~SRS-218~~ TDCIS nodes shall be equipped or enabled with Voice Gateways quantities, as per the table below:

	AN	BCC	CCC	RAP	TN	RL
Voice over IMT	1	1	Enabled	1	-	1
Iridium PTT	Enabled	Enabled	Enabled	-	-	-
Radio PTT - xU	-	Enabled	Enabled	Enabled	-	-
Radio PTT - xR	-	Enabled	Enabled	1	-	-

Table 5 - xU Voice Gateways quantities

SRS (PRTTDCIS-1528)

~~SRS-219~~ The Voice over IMT gateway functionality shall be integrated in the MMA-xU of each node equipped with this Voice Gateway.

NOTE (PRTTDCIS-2244)

~~[81]~~ The Satphone terminal is an Iridium 9575 PTT Extreme terminal, which is PFE.

NOTE (PRTTDCIS-2678)

~~[82]~~ Any Radio PTT integration on xU and xR will be IP based and the Radio over IP gateway will be provided together with the radio to connect to.

NOTE (PRTTDCIS-1207)

~~[83]~~ A dismounted soldier uses situational awareness software (called DSS) that is connected to the vehicle's situational awareness software (called BMS) and to the TDCIS xR security domain over an integrated CNR. The TDCIS situational awareness software running in the xR security domain will merge information coming from the Mobile Users and xU data (i.e. meteo) fed from the xU security domain over the xU-xR cross domain solution. The BMS/DSS in the xR security domain will feed over the xR-xS DDM the NATO situational awareness software (LC2IS) with all the situational awareness data. Information from the LC2IS that needs to be fed into the BMS/DSS has to be transferred over an air-gap.

3.2.3 Users

SRS (PRTTDCIS-1431)

~~SRS-220~~ TDCIS Nodes shall support End Users, as per the table below:

Security Domain	AN	BCC	CCC	RAP	TN	RL
xU	34	16	4	-	-	-
xR	34	16	4	-	-	-
xS	22	10	-	-	-	-

Table 6 - End Users per security domain and node type

SRS (PRTTDCIS-2555)

~~SRS-221~~ TDCIS Nodes shall support System Administrators, as per the table below:

Security Domain	AN	BCC	CCC	RAP	TN	RL
BLK	2	2	2	2	2	2
xU	2	2	2	2	2	2
xR	2	2	2	2	-	-
xS	2	2	-	-	-	-

Table 7 - System Administrators per security domain and node type

NOTE (PRTTDCIS-1817)

~~[84]~~ End-User Devices (e.g. Phones, Workstations, Printer/Scanners, VTC appliances), are PFE at the exception of System Administrator devices.

SRS (PRTTDCIS-1440)

~~SRS-222~~ The TDCIS nodes shall be equipped with xU Wireless VoIP Telephone for System Administrator as listed in following table:

	AN	BCC	CCC	RAP	TN	RL
Wireless VoIP Telephone	3	3	1	1	1	4

Table 8 - System administrator Devices quantities per node

SRS (PRTTDCIS-2683)

~~SRS-223~~ Each TDCIS Node shall be equipped with two (2) System Administrator Workstations per security domain present in the Node.

SRS (PRTTDCIS-3119)

~~SRS-224~~ Each TDCIS Node shall be equipped with two (2) System Administrator Workstations dedicated to the management of the BLK.

SRS (PRTTDCIS-4469)

~~SRS-225~~ The composition of System Administrator Workstations shall comply with the breakdown illustrated in the following figure.

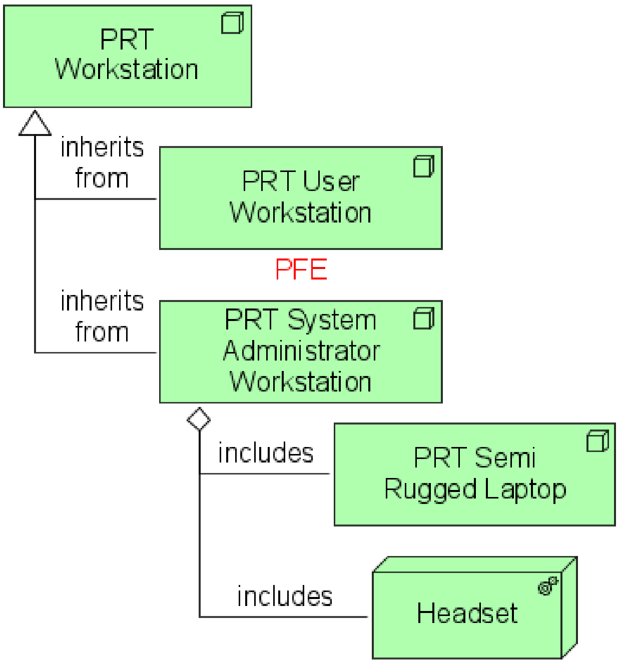


Figure 14 - System Administrator Workstation Breakdown

SRS (PRTTDCIS-2684)

~~SRS-226~~ Each TDCIS shelter shall be equipped with TWO (02) System Administrator wired VoIP Phones per security domain present in the Node.

SRS (PRTTDCIS-1810)

~~SRS-227~~ The TDCIS nodes shall be equipped with a number of UAM as listed in following table:

	AN	BCC	CCC	RAP	TN	RL
Medium UAM-xU	2	1	1	-	-	-
Small UAM-xU	4	4	2	2	2	2
Medium UAM-xR	2	1	1	-	-	-
Small UAM-xR	4	4	2	2	-	-
Medium UAM-xS	2	2	-	-	-	-
Small UAM-xS	2	2	-	-	-	-

Table 9 - UAM quantities per node

SRS (PRTTDCIS-2462)

~~SRS-228~~ Beside any other tools as specified in other sections and emerging from the design, all Workstations shall be installed with latest available version of following software:

- Adobe Acrobat Reader; and,
- Microsoft Windows; and,
- Microsoft Office.

3.2.4 Transmissions

NOTE (PRTTDCIS-1525)

~~[85]~~ TDCIS Nodes will be equipped with different Transmission Systems:

- On the BLK, connected to the PCA Subsystem:
  - **Mini LOS** as Point-to-Point Line of Sight transmission between BCC and CCC; and,
  - **HCLOS** as Point-to-Point Line of Sight transmission to build the Tactical backbone (TN, AN, BCC, RAP); and,
  - **Broadband IP Radio**, as radio network for AN, BCC, CCC and RAP; and,
  - **Commercial SATCOM** as fallback mean of communication; and,
  - **Military SATCOM** as rear-link transmission to PRT static infrastructure; and,
  - **Ethernet (FO and Cu)** as primary mean of interconnection between node; and,
  - **SHDSL** as an alternative mean of connection between node; and,
  - **Data over IMT** as a fallback mean of communication by connecting to an International Mobile Telecommunication (IMT) network (GSM/UMTS/LTE (4G)); and,
  - **IP HF Radio** as a fallback mean of communication for the rear-link transmission to PRT static infrastructure and for intra-theatre transmissions; and,
- On the xR security domain, connected to the CCA-xR Subsystem:
  - **Combat Net Radio** as a Mobile Tactical Forces (Vehicles and Soldiers) integration mean of communication.

NOTE (PRTTDCIS-4634)

~~[86]~~ Node to Node connectivity concept is illustrated on following diagram:

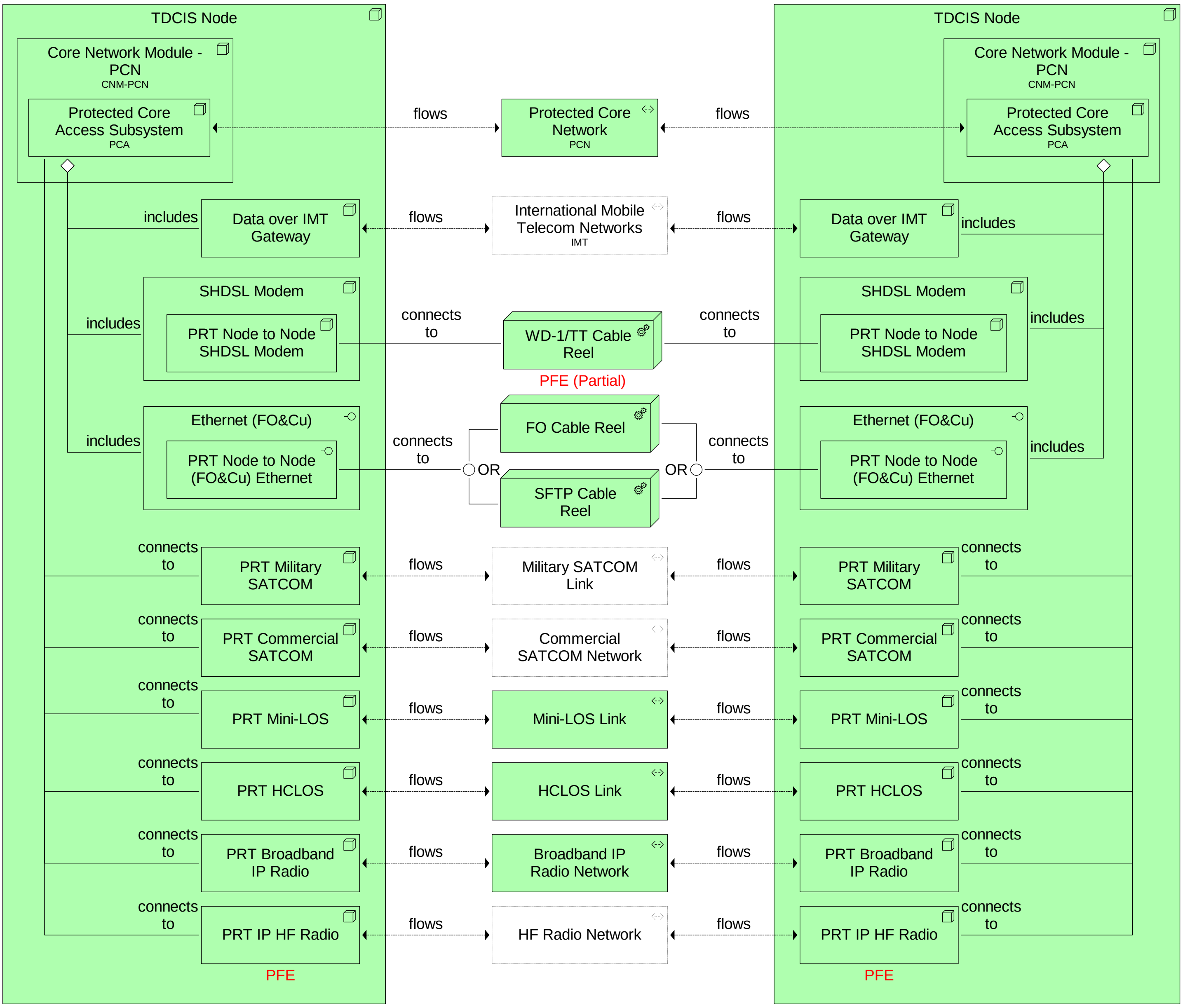


Figure 15 - Node to Node connectivity concept

SRS (PRTTDCIS-1527)

~~SRS-229~~ The Data over IMT functionality shall be integrated in the PCA of each node equipped with this Transmission System.

NOTE (PRTTDCIS-3074)

~~[87]~~ The HCLOS datalink will establish a High bandwidth and long distance wireless backbone network infrastructure connecting Access nodes, BCC nodes and RAP nodes through TN nodes.

SRS (PRTTDCIS-1434)

~~SRS-230~~ TDCIS nodes shall be equipped or enabled with Transmission Systems quantities, as per the table below:

	AN	BCC	CCC	RAP	TN	RL	GAR-T HCLOS
Mini LOS	Enabled	3	1	Enabled	Enabled	Enabled	Enabled
HCLOS	3	1	Enabled	2	4	Enabled	2
Broadband IP Radio	1	1	1	1	Enabled	Enabled	-
Commercial SATCOM	1	1	1	Enabled	Enabled	Enabled	-
Military SATCOM	Enabled	Enabled	Enabled	-	-	1	-
Ethernet (FO and Cu)	8	8	4	4	4	4	-
SHDSL	4	4	2	2	2	2	-
Data over IMT	1	1	Enabled	Enabled	Enabled	Enabled	-
IP HF	-	-	-	-	-	1	-

Table 10 - Transmission Systems quantities per Node

SRS (PRTTDCIS-2563)

~~SRS-231~~ All Nodes identified as Enabled shall be ready (mechanical, wiring...) to accommodate the associated Transmission System.

3.2.5 Housing

SRS (PRTTDCIS-1499)

~~SRS-232~~ The physical configuration of a TDCIS node shall comprise of:

- a single shelter; or,
- a single shelter and a trailer; or,
- a combination of two shelters.

SRS (PRTTDCIS-1365)

~~SRS-233~~ The TDCIS Nodes shall each be composed as in following table:

Node	Composition
Access Node	1 Management Shelter 1 Communication Shelter
Battalion Communications Centre	1 Management Shelter 1 Communication Shelter
Company Communications Centre	1 Shelter
Radio Access Point	1 Shelter
Transit Nodes	1 Shelter
Rear Links	1 Shelter 1 GAR-T Trailer - Rear Link HF Variant
GAR-T HCLOS Relay	1 GAR-T Trailer - HCLOS Relay Variant

Table 11 - TDCIS Nodes Shelter and Trailer composition

SRS (PRTTDCIS-1500)

~~SRS-234~~ In the case of dual shelter Nodes, the first shelter (Management Shelter) shall contain the Colour Clouds Elements and the second shelter (Communication Shelter) shall contain the Transmission Elements.

SRS (PRTTDCIS-4635)

~~SRS-235~~ The distribution of Node Elements between the Management and the Communication Shelter and the connectivity between those shelters shall adhere to the concept illustrated on the following diagram:

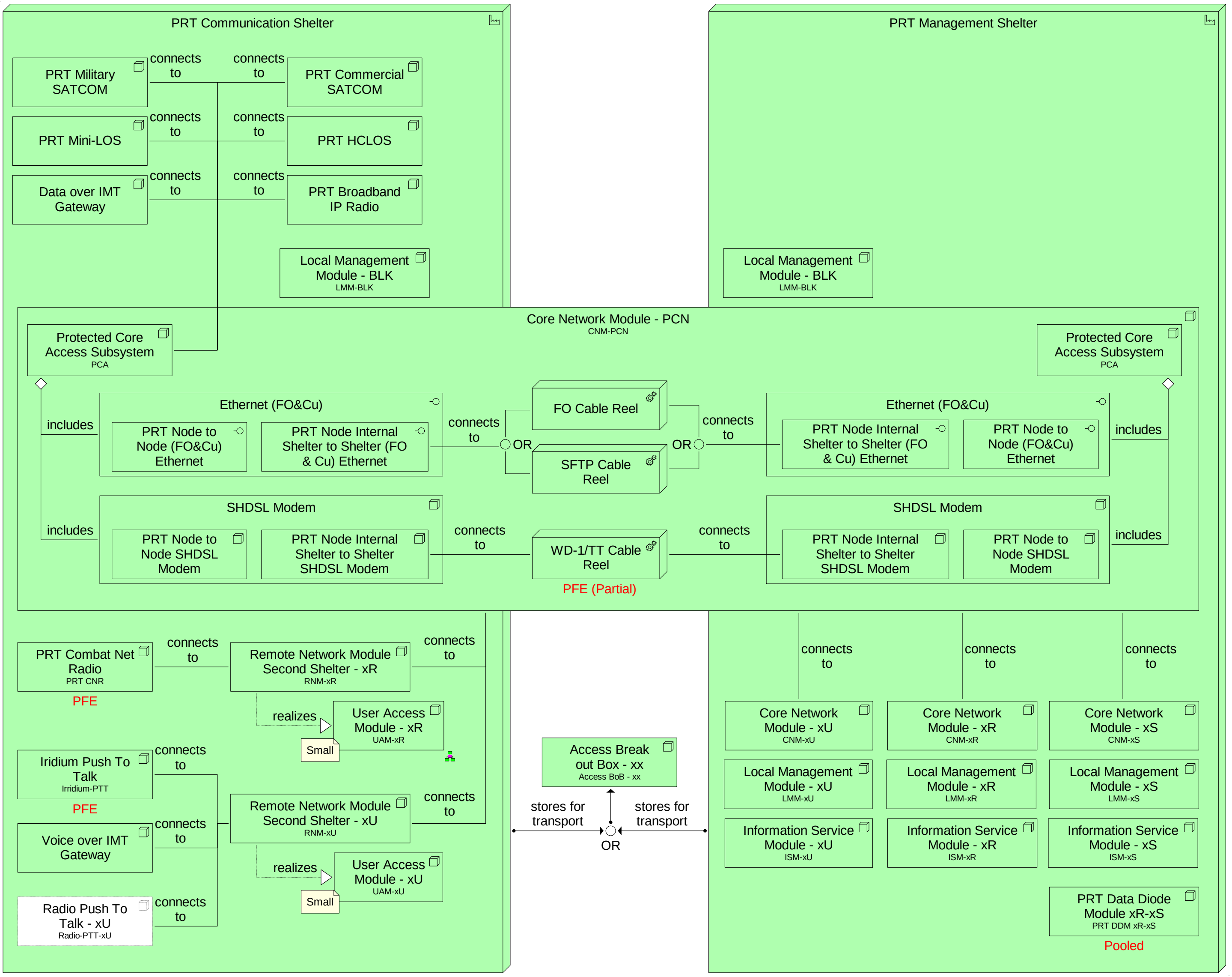


Figure 16 – Elements distribution and Shelter connectivity concept in dual shelter Nodes

NOTE (PRTTDCIS-2261)

~~[88]~~ The Tactical Towable Support Group trailer (GAR-T), provides support to the TDCIS Nodes Shelters.

NOTE (PRTTDCIS-2262)

~~[89]~~ The GAR-T forms the basis for the TDCIS two trailer variants, namely the “GAR-T HCLOS Relay” and “GAR-T Rear Link”

SRS (PRTTDCIS-1505)

~~SRS-236~~ Transit cases shall be used to host and support CIS assets built in it.

SRS (PRTTDCIS-1506)

~~SRS-237~~ Transport cases shall be used to store and transport non-PFE EUD and ancillaries.

SRS (PRTTDCIS-3091)

~~SRS-238~~ Transit and Transport Cases shall be fixed inside the Node Shelter for transport.

SRS (PRTTDCIS-2158)

~~SRS-239~~ Beyond the Cable reels specifically mentioned in element breakdowns, TDCIS Nodes shall include additional cable reels as per following table.

	AN	BCC	CCC	RAP	TN	RL
FO cable reel	4	4	2	2	2	2
SFTP cable reel	2	2	1	1	1	1
WD-1/TT cable reel	2	2	1	1	1	1
Backpack harness	2	2	1	1	1	1

Table 12 - Additional Cable Reels per node

SRS (PRTTDCIS-4636)

~~SRS-240~~ Cable reels and Backpack harnesses quantities shall be evenly distributed between shelters for dual shelters Nodes.

3.2.6 Purchaser Furnished Equipment

SRS (PRTTDCIS-1522)

~~SRS-241~~ The table below contains Crypto Purchaser Furnished Equipment (PFE) assets quantities that shall be considered for integration in the TDCIS nodes

Asset	AN	BCC	CCC	RAP	TN	RL
TCE 621B Crypto	1	1	-	-	-	-

Table 13 - Crypto PFE Quantities for TDCIS Nodes

SRS (PRTTDCIS-2679)

~~SRS-242~~ The table below contains CNR PFE assets quantities that shall be considered for integration in the nodes

Asset	AN	BCC	CCC	RAP	TN	RL
CNR Double Vehicle Module	-	2	1	3	-	-
CNR Single Vehicle Module	-	-	1	-	-	-
CNR Transceiver TR-525AH	-	2	1	2	-	-
CNR Transceiver TR-525AU	-	1	1	3	-	-
CNR Transceiver TR-525AU HQII	-	1	1	1	-	-
CNR 150W HF Power Amplifier	-	1	1	1	-	-
CNR 150W Antenna Tuning Unit	-	1	1	1	-	-
CNR 50W V/UHF Power Amplifier	-	1	1	1	-	-
CNR RoIP Gateway	-	-	-	1	-	-

Table 14 - CNR PFE Quantities

SRS (PRTTDCIS-2680)

~~SRS-243~~ The table below contains PFE CIS assets quantities that shall be considered for integration in the nodes

Asset	AN	BCC	CCC	RAP	TN	RL
IP HF Radio Rack - Single	-	-	-	-	-	1
IP HF Transceiver TR-525AH	-	-	-	-	-	1
IP HF 500W Power Amplifier and Antenna Tuning Unit	-	-	-	-	-	1
IP HF Log-Periodic HF Antenna	-	-	-	-	-	1
IP HF Whip Antenna	-	-	-	-	-	1

Table 15 - IP HF Radio PFE Quantities

NOTE (PRTTDCIS-4637)

~~[90]~~ The HF Whip Antenna will not be mounted nor used at the same time as the Military SATCOM Terminal in the RL Node.

NOTE (PRTTDCIS-1524)

~~[91]~~ TN has no CIS PFE to be integrated.

SRS (PRTTDCIS-1437)

~~SRS-244~~ The table below contains the characteristics of the different PFE CIS assets that shall be taken into consideration for integration in the different nodes and modules.

Asset	Estimated Rack Space (RU)	Weight (kg)	Power Supply	Electrical Power (Watt)	Estimated Heat dissipation (Watt)
TCE 621B Crypto	1	4.1	230VAC	25	-
CNR Double Vehicle Module	5	21.4	24VDC	672	550
CNR Single Vehicle Module	3	18.1	24VDC	360	286
CNR 150W HF Power amplifier	5	14.5	24VDC	960	810
CNR 50W V/UHF Power Amplifier	5	12.5	24VDC	450	360
CNR RoIP Gateway	3	10	24VDC	20	-
HF Radio Rack - Single	3	14	28VDC (Powered from Amplifier assembly)	120	100
HF 500W Power Amplifier and Antenna Tuning Unit	17	200	230VAC	2520	2000

Table 16 - PFE Characteristics

NOTE (PRTTDCIS-2682)

~~[92]~~ All other PFE assets listed in previous tables are taking place inside the modules for which characteristics are provided. Therefore, these are not considered as additional physical, environmental and electrical integration constraints.

NOTE (PRTTDCIS-3220)

~~[93]~~ PFE detailed specifications will be shared with the Contractor after Contract Award.

NOTE (PRTTDCIS-3222)

~~[94]~~ CNR 150W HF Antenna Tuning Unit is

- not rack mounted but outdoor installed (close to the ERFP) in a location as close as possible from the Antenna, therefore it does not require any rack mounting units; and,
- in-line powered from the CNR 150W HF Power Amplifier over the RF connection, therefore its Estimated Heat Dissipation and Power Consumption are included in the characteristics of the CNR 150W HF Power Amplifier.

NOTE (PRTTDCIS-3221)

~~[95]~~ CNR 150W HF Power amplifier and CNR 50W V/UHF Power Amplifier have the same form fit factor and are rack mounted on a plate which can accommodate up to two (2) of these amplifiers next to each other. Therefore, a single 5U rack space has to be considered for every 2 of these power amplifier units.

NOTE (PRTTDCIS-4737)

The PFE HF Log Periodic antenna will be an ALARIS RA10-118-01 mounted on a YAESU G-2800DXC Rotator.

NOTE (PRTTDCIS-4468)

~~[96]~~ Following licenses are PFE to this project:

- Microsoft Windows; and,
- Microsoft SharePoint (not Microsoft SQL); and,
- Microsoft Exchange; and,
- Antivirus Software.

NOTE (PRTTDCIS-4638)

~~[97]~~ WD-1/TT cable to be rolled on WD-1/TT cable reels is PFE.

3.3 GAR-T HCLOS Relay

SRS (PRTTDCIS-1363)

~~SRS-245~~ The GAR-T HCLOS Relay design shall adhere to the design concept presented in following figure:

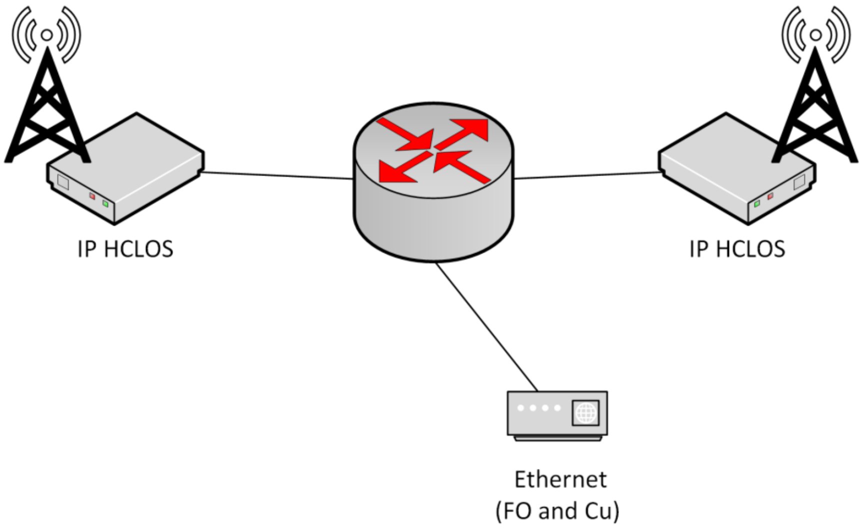


Figure 17 - GAR-T HCLOS Relay design concept.

SRS (PRTTDCIS-2302)

~~SRS-246~~ The GAR-T HCLOS Relay shall be built by TWO (02) HCLOS radios systems, mounted on a GAR-T autonomous trailer.

SRS (PRTTDCIS-2303)

~~SRS-247~~ The GAR-T HCLOS Relay shall route the IP traffic from one (receiving) HCLOS radio to the other (relaying) HCLOS radio when used as a relay.

SRS (PRTTDCIS-2304)

~~SRS-248~~ The GAR-T HCLOS Relay shall route the IP traffic from nodes to nodes over a maximum of two HCLOS links when used in Enabling or Augmenting Node HCLOS capacity configuration.

SRS (PRTTDCIS-2305)

~~SRS-249~~ The HCLOS routing function shall provide basic connectivity to the TDCIS Nodes through:

- TWO (02) 1 Gbps *Eth-FO* interfaces, and
- TWO (02) 1 Gbps *Eth-Cu* interfaces.

SRS (PRTTDCIS-2301)

~~SRS-250~~ The GAR-T HCLOS Relay telescopic mast shall support two HCLOS Radio Systems.

SRS (PRTTDCIS-2297)

~~SRS-251~~ In addition to those specified in the GAR-T Common Base, the HCLOS relay shall support compartments to accommodate the following;

- Two HCLOS Radio systems (antennas, radios, rotors, fixing/installing equipment); and,
- Associated installation cable reels (power, data) for two HCLOS radio systems.

SRS (PRTTDCIS-3039)

~~SRS-252~~ The GAR-T HCLOS Relay, when used as a relay, shall support working in isolation of any TDCIS Node.

3.4 NS Kit

SRS (PRTTDCIS-2549)

~~SRS-253~~ TDCIS shall include a NATO SECRET (NS) Kit.

SRS (PRTTDCIS-2550)

~~SRS-254~~ The NS Kit shall include:

- **Core Node lite** providing NS Services, end-user access and federating with other MNP in the NS security domain; and,
- **Remote Node lite** providing network extension and end-user access to NS Services.

SRS (PRTTDCIS-2931)

~~SRS-255~~ The NS Kit is a group of nodes and, unless specified otherwise, shall be considered as a TDCIS Node for all its Functional and Technical Requirements, Performances, Implementation Constraints and Service and Module implementation concepts.

SRS (PRTTDCIS-2551)

~~SRS-256~~ NS Kit being reserved only to NATO led missions, the NS Kit (and all of its composing elements) shall be considered a pooled resource and therefore shall not be assigned to any TDCIS node in particular.

SRS (PRTTDCIS-2552)

~~SRS-257~~ The NS Kit Nodes quantities shall adhere to following table:

	Quantities
NS Kit - Core Node lite	3
NS Kit - Remote Node lite	7

Table 17 - NS Kit Nodes quantities

SRS (PRTTDCIS-2697)

~~SRS-258~~ The NS Kit Nodes per node maximum collocated connected end users quantities shall adhere to following table:

	End User Quantities
NS Kit - Core Node lite	8
NS Kit - Remote Node lite	10

Table 18 - NS Kit Nodes End User quantities

SRS (PRTTDCIS-2920)

~~SRS-259~~ The NS Kit Core Nodes shall support TWO (02) System Administrators.

SRS (PRTTDCIS-2919)

~~SRS-260~~ Each NS Kit Core Nodes shall include System Administrator devices as per following table:

	Quantities
System Administrator Workstations	2
System Administrator VoIP phones	2

Table 19 - NS Kit System Administrator quantities per Core Node

SRS (PRTTDCIS-2553)

~~SRS-261~~ The breakdown and housing concept of the NS Kit Nodes are illustrated in the following figure. It identifies the required Modules it is composed of. Each NS Kit Node shall be built upon the building blocks and integrated in housing elements as identified in this reference.

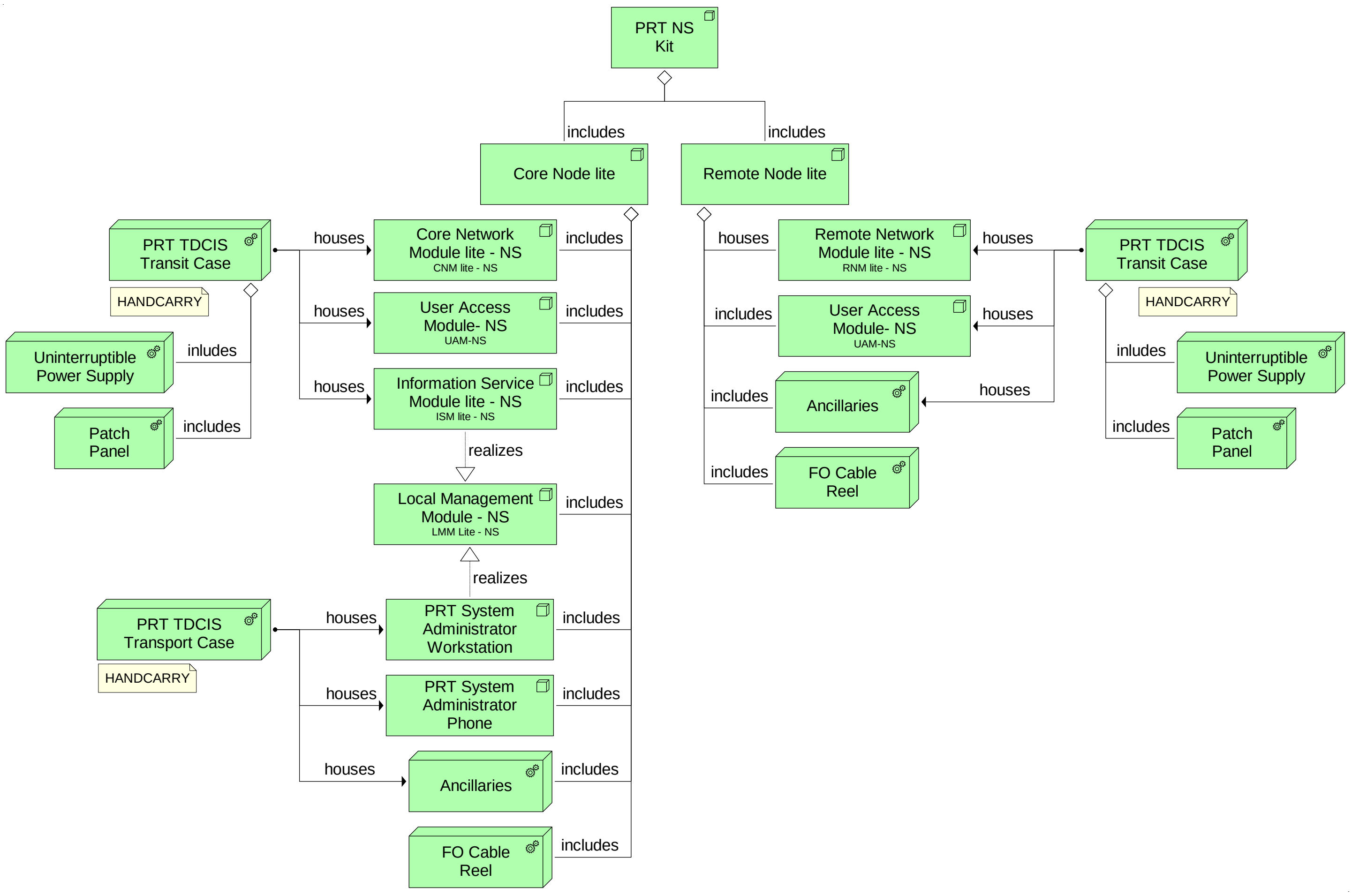


Figure 18- NS Kit breakdown

SRS (PRTTDCIS-2745)

~~SRS-262~~ The NS Kit Core Node lite shall contain ONE (01) CNM lite, ONE (01) medium UAM-NS and ONE (01) ISM lite.

SRS (PRTTDCIS-2746)

~~SRS-263~~ The NS Kit Remote Node lite shall contain ONE (01) RNM lite and ONE (01) medium UAM-NS.

SRS (PRTTDCIS-4371)

~~SRS-264~~ Each NS Kit Node shall be housed in cases profiles as per following table

	Quantities	Case Profile	Remark
Core Node lite	1	HANDCARRY	Single transit case housing all Core Node lite Modules
Core Node lite - Ancillaries	N	HANDCARRY	For Sys Admin appliances, cabling, etc. N is Design Driven
Remote Node lite	1	HANDCARRY	Single transit case housing all Remote Node lite Modules, including ancillaries (cables, etc.)

Table 20 - NS Kit housing cases integration profiles

NOTE (PRTTDCIS-2687)

~~[98]~~ The NS Kit Nodes in context is illustrated on the following picture.

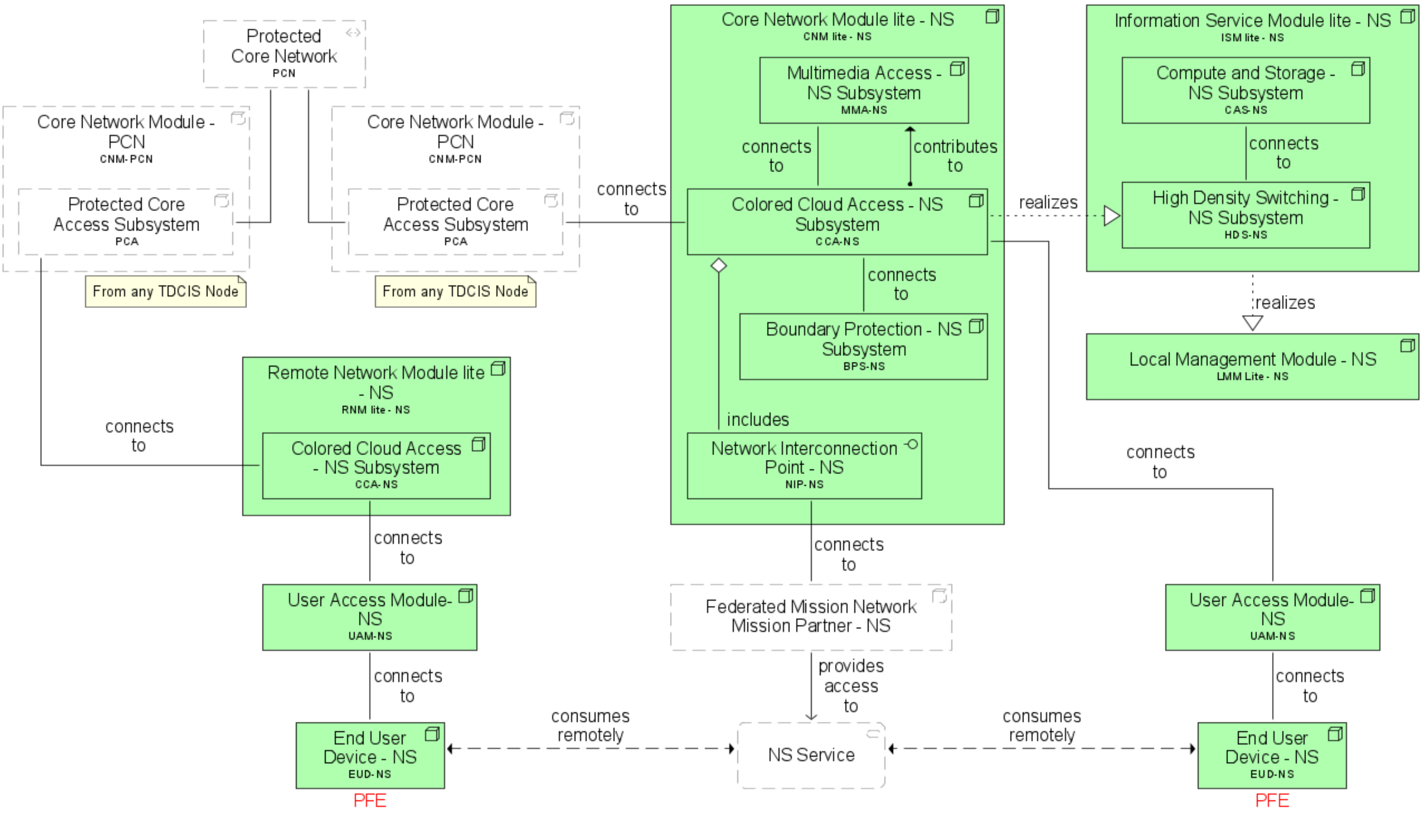

Protected Core Network
PCN
Core Network Module - PCN
CNM-PCN
Protected Core Access Subsystem
PCA
From any TDCIS Node
Core Network Module - PCN
CNM-PCN
Protected Core Access Subsystem
PCA
From any TDCIS Node
connects to
Core Network Module lite - NS
CNM lite - NS
Multimedia Access - NS Subsystem
MMA-NS
connects to
contributes to
Colored Cloud Access - NS Subsystem
CCA-NS
connects to
Boundary Protection - NS Subsystem
BPS-NS
includes
Network Interconnection Point - NS
NIP-NS
realizes
Information Service Module lite - NS
ISM lite - NS
Compute and Storage - NS Subsystem
CAS-NS
connects to
High Density Switching - NS Subsystem
HDS-NS
realizes
Local Management Module - NS
LMM Lite - NS
connects to
Remote Network Module lite - NS
RNM lite - NS
Colored Cloud Access - NS Subsystem
CCA-NS
connects to
User Access Module- NS
UAM-NS
connects to
End User Device - NS
EUD-NS
PFE
consumes remotely
connects to
Federated Mission Network Mission Partner - NS
provides access to
NS Service
consumes remotely
connects to
User Access Module- NS
UAM-NS
connects to
End User Device - NS
EUD-NS
PFE

Figure 19 - NS Kit in context

SRS (PRTTDCIS-2747)

~~SRS-265~~ NS Kit CNM lite and RNM lite shall interconnect their respective CCA through the PCA of any TDCIS Node and benefit from the PCN as a transport network.

SRS (PRTTDCIS-2695)

~~SRS-266~~ The table below contains Crypto PFE assets quantities that shall be considered for integration in the NS Kit.

Asset	NS Kit
TCE 621M Crypto	10

Table 21 - Crypto PFE Quantities for NS Kit

SRS (PRTTDCIS-2688)

~~SRS-267~~ Where and when possible, the contractor shall aim for an identical design and hardware for NS Kit modules as for the TDCIS Node modules.

SRS (PRTTDCIS-2691)

~~SRS-268~~ If necessary, the contractor shall prioritize small footprint and reduced size and weight of the NS Kit over hardware commonality with TDCIS Node modules.

SRS (PRTTDCIS-3003)

~~SRS-269~~ Each TDCIS Node Shelter shall have a storage and transport position for ONE (01) NS Kit Core Node and ONE (01) NS Kit Remote Node.

SRS (PRTTDCIS-3004)

~~SRS-270~~ NS Kit elements shall primarily rely on the Node Shelter power supply for a distance of minimum 25m though the Shelter Termination Panel.

SRS (PRTTDCIS-4639)

~~SRS-271~~ NS Kit elements shall support being powered from other 220VAC power sources (e.g. Mains, Power Generators, etc.)

SRS (PRTTDCIS-3006)

~~SRS-272~~ Each NS Kit Core Node shall be delivered with ONE (01) FO cable reel of 250m.

SRS (PRTTDCIS-3007)

~~SRS-273~~ Each NS Kit Remote Node shall be delivered with ONE (01) FO cable reel of 250m.

SRS (PRTTDCIS-4238)

~~SRS-274~~ The NS Kit shall provide following services on NS to their directly connected End Users and System Administrators as per following table:

Legend:

- *Local*: Service is locally hosted in the Core Node lite
- *Remote*: Service is remotely consumed from the federation

Service	Service Category	NS Kit
Functional Area Services	Community of Interest	Remote
Email	Business Support	Local
Collaborative Information Portal	Business Support	Remote
Voice Collaboration (IP)	Business Support	Local
Interconnection to Nations	N/A	Local
Antivirus	CIS Security	Local
Network Access Control	CIS Security	Remote
Encryption	CIS Security	Local
Log Aggregation	CIS Security	Remote
Online Vulnerability Assessment	CIS Security	Remote

Table 22 - End-users Services on NS

3.5 Pooled Elements

NOTE (PRTTDCIS-4387)

~~[99]~~ The TDCIS Pooled Elements are not to be used for the NS Kit.

NOTE (PRTTDCIS-4384)

~~[100]~~ The TDCIS Pooled Elements in context are illustrated on following figure:

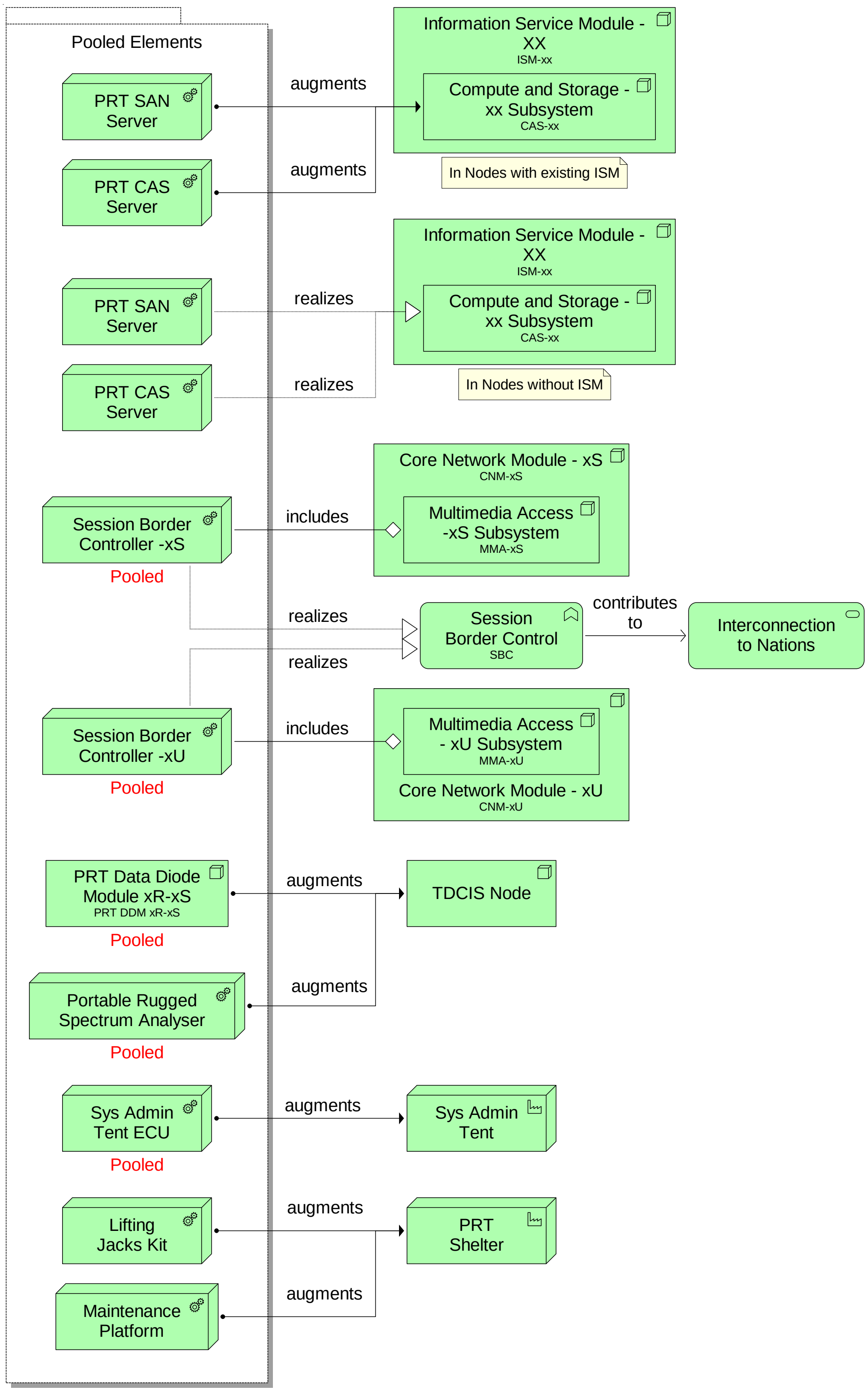


Figure 20 - Pooled Elements in context.

SRS (PRTTDCIS-4385)

~~SRS-275~~ The TDCIS Pooled Elements shall be delivered in quantities as per following table:

Elements	Quantities
PRT CAS Server	20
PRT SAN Server	2
Session Border Controller (SBC) - xU	6
Session Border Controller (SBC) - xS	6
DDM xR-xS	9
Rugged Portable Spectrum Analyser	6
Sys Admin Tent ECU	15
Lifting Jacks Kits	6
Maintenance Platforms	2

Table 23 - Pooled Elements quantities

SRS (PRTTDCIS-4388)

~~SRS-276~~ The Pooled CAS and SAN Servers shall support:

- Increasing an existing CAS variant with more Compute and Storage capacity in any Security Domain; and,
- Upgrading an existing CAS variant to another CAS variants such as converting a SAN based CAS into a Software Defined CAS and any other possible combinations in any Security Domain; and,
- Enabling a TDCIS Node with no pre-existing ISM with an ISM containing any possible CAS variant in any Security Domain.

NOTE (PRTTDCIS-4392)

~~[101]~~ Any potential licenses required for Increasing, Upgrading or Enabling a Node with Pooled CAS and SAN Servers are not deliverables of this project.

SRS (PRTTDCIS-4575)

~~SRS-277~~ The Pooled Session Border Controllers (SBC) for xU and xS shall support integration in any BCC to enable the federation of Voice and Video Teleconference parts of the Interconnection to Nations service.

SRS (PRTTDCIS-4389)

~~SRS-278~~ The Pooled DDM xR-xS shall support integration in any AN and in any BCC to enable the Cross Domain Service between xU and xS in that Node.