Annex A – Summary of Requirements

Project No. 2016/0CM03123, CP 9A0130

1. Project Objective

The purpose of this project is to provide an Advanced Satellite Network Monitoring and Control (ASNMC) capability to monitor and control the NATO satellite communication assets in an efficient and effective manner.

2. Required Capability

The NCI Agency provides SATCOM services to NATO through a variety of SATCOM terminals. These terminals include Radio Frequency (RF) systems (e.g. antennas, amplifiers, splitters/combiners, matrix switches, modems, spectrum monitoring systems), Information Technology (IT) infrastructure (e.g. routers, switches, servers), and supporting facilities (e.g. power, heating and cooling, buildings).

The ASNMC supports the monitoring, control and troubleshooting of the terminals and links between them, both for local terminal operators, as well as for remote operators at the central Service Operating Centres (SOCs) managing the complete SATCOM infrastructure and its services. Apart from interfacing with the elements (equipment) of the terminals, the ASNMC also interfaces with planning tools and spectrum monitoring systems.

In addition, the ASNMC provides:

- Dedicated SATCOM hub and spoke systems acting as Engineering Order Wire (EOW),
- LAN connectivity between the elements of the terminal and its local ASNMC instance,
- WAN connectivity (VPNs) between ASNMC instances at the terminals and the SOCs, using the NATO WAN and the EOW.

The ASNMC, as depicted in the below figure, has a distributed architecture with as main M&C systems (ASNMC in green, Purchaser systems in orange):

1. The Local Managers (LMs) at each terminal, which enable local management of the terminal elements. LMs report the status of their associated terminal to a Central Manager (CM, see below). Conversely, LMs can receive control information from the CM.

2. The LM Clients, that provide local operators' access to the LM.

3. The Central Managers (CMs), which provide a global SATCOM status overview including all terminals and links between them. The CMs can, through the LMs, manage terminals and provision links between the terminals. The CMs can also convert the output of Purchaser's Link Planning Tools (LPT) into modem settings and apply them.

4. The CM Clients, that provide browser based GUI access to the CMs for SATCOM operators at the Service Operations Centres (SOCs) and at static terminals.

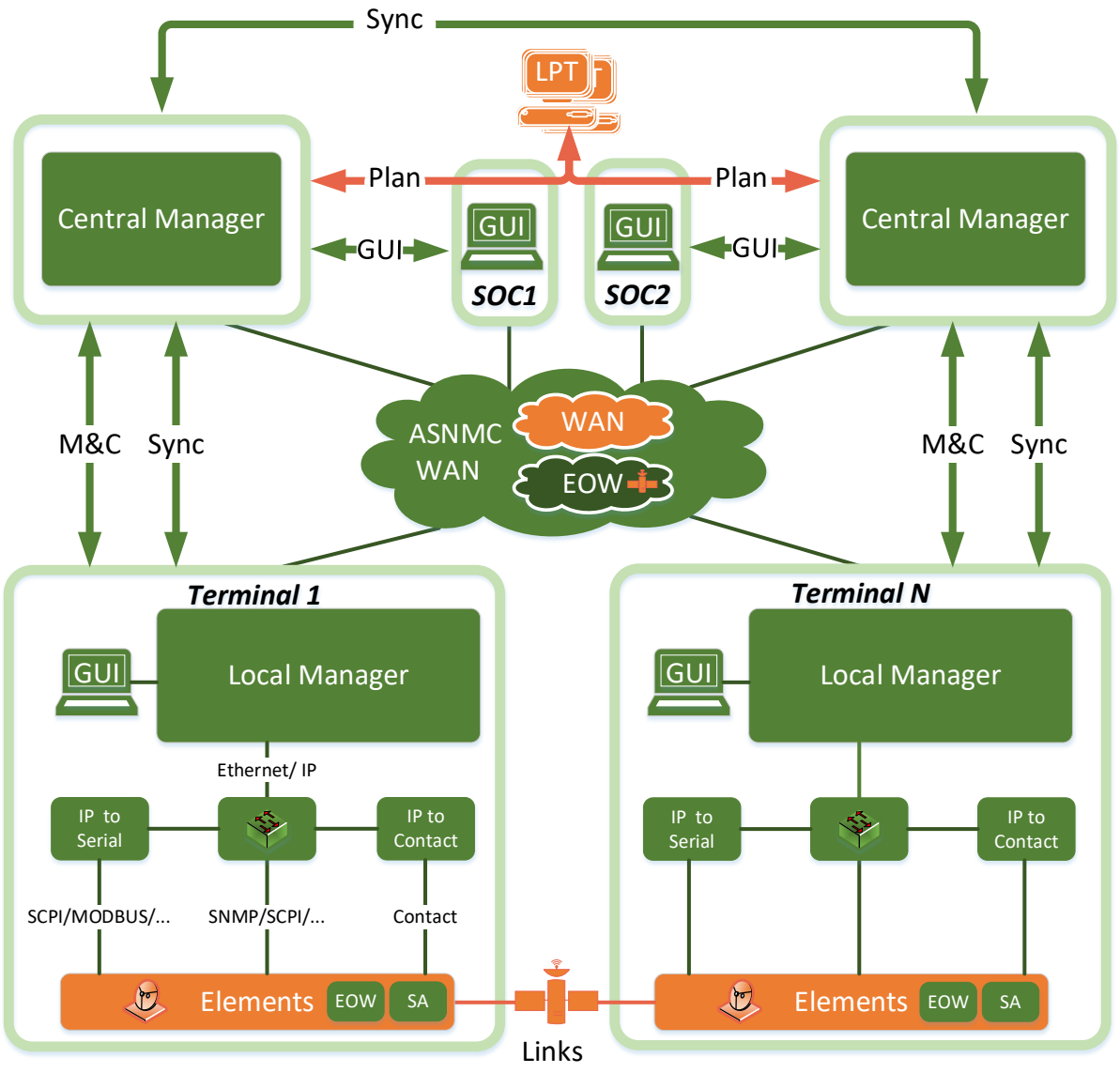

Figure: ASNMC architecture

The current ASNMC requires a technology refresh, which is the subject of this project. In summary, the needs for the ASNMC include:

1. The ASNMC provides LAN and WAN connectivity within and between terminals and the SOC.
2. The ASNMC provides an EOW system, including:
    a) Hubs at large and medium terminals

b) A deployable hub

c) Spokes at other terminals

d) Transmission Security (TRANSEC)

e) High bandwidth efficiency through adaptive coding and modulation, efficient waveforms, and dynamic multiple access technologies

3. For deployable terminals without rack space their ASNMC instances operate outside the terminal and are ruggedized to be transported, stored and operated with full exposure to the environment; for deployable terminals with rack space their ASNMC instances fit in 4U rack space with limited depth.
4. The ASNMC at deployable terminals provides a spectrum analyser function that integrates with the ASNMC M&C functions.
5. The ASNMC implements LM, CM and Client functions as described above in the background section.
6. The ASNMC M&C provides:
    a) Monitoring of the SATCOM terminals and links with:
        i. Event creation, i.e. detecting that elements, networks and SATCOM links operate outside (configurable) normal operation conditions, and determining the anomaly/alarm severity of such an event. For the SATCOM link the ASNMC uses link quality information reported by the modems at each end of the link.
        ii. Event correlation (filtering, aggregation, masking, and root cause analysis based on element and dynamic terminal topologies and dependencies), classification and prioritisation.
        iii. Logging of key performance parameters and events.
        iv. Operator interaction, including graphical presentation of status and performance, and alerting and tracking of relevant events.
    b) Control of the SATCOM terminals and links with:
        i. Configuration of terminal elements by operators at LM and CM.
        ii. A sequence of predefined control actions (“scripts”) on one or multiple elements, which can be triggered through scheduling, operation action, or by monitoring events.
7. Communication between the LMs, CMs and Clients is implemented such that:
    a) LMs can interoperate with the CMs over constrained SATCOM links.
    b) LMs can be operated locally without connectivity to CMs.
    c) CMs operate in a redundant configuration, in which the information between CMs is synchronised (over the NATO terrestrial WAN), so all CMs provide the same status to SOC operators.

8. The LM supports management of elements via:
    a) Industry standard protocols and interfaces:
        i. All SNMP v1, v2c and v3 functionalities.
        ii. SCPI and MODBUS over IP, RS485, and RS422 interfaces.
        iii. Dry contacts.
    b) Element specific and proprietary Monitoring & Control (M&C) protocols, through software (SW) modules implementing APIs/ drivers for these elements. For this purpose, LMs must be able to host such modules and support information exchange with the LM. Interface Control Documents will be provided by NCIA.
9. The ASNMC offers a GUI at LM and CM, which:
    a) Is accessible through a browser.
    b) Provides a uniform presentation of elements with similar functionality (e.g. modems, amplifiers, test instruments…) but different implementations (e.g. different manufacturers or versions).
    c) Can represent the following topologies of each terminal dynamically (i.e. with actual states/ connectivity of switches as obtained through M&C data or entered by the operator for passive switches and patch panels):
        i. RF (including IF).
        ii. Power.
        iii. Network connectivity
        iv. The ASNMC itself (switches, servers, routers, EOW etc.)
    d) Enables at LMs a presentation in which elements can be grouped into sub-systems, and combinations of subsystems (and be displayed as subsystem, rather than displaying numerous elements in one screen).
    e) Enables at CMs a presentation in which terminals and links can be grouped according to criteria such as geographical area, user group, and technology.
    f) Can present in graphs and tables, and can export, logged performance data with user configurable filters including time frame, terminals, type of data etc.
    g) Can provide statistics for SATCOM links (SLA monitoring).
10. The ASNMC can be customised by the operator independent of the ASNMC vendor, through graphical interfaces and without requiring programming skills, to address changes in:
    a) Terminal topology (connectivity between elements, and the type and number of elements in a terminal).
    b) The number of terminals.
    c) The types of elements (e.g. new modems) with industry standard interfaces.

d) The GUI.

11. The LMs and CMs provide open and industry standard interfaces for the exchange of management information with northbound management systems.
12. The ASNMC includes the tools for the administration of the ASNMC itself, including:
    a) Mechanisms for provisioning of new and spare LM and CM.
    b) Configuration management database, detailing which SW versions are applied to which LM and CM.
    c) Mechanisms to distribute SW updates.
    d) Backup and restore.
13. The ASNMC meets the security requirements for processing classified data including:
    a) The Operating System is approved (Red Hat Enterprise Linux, Microsoft Windows).
    b) Application(s) pass penetration testing.
    c) Applications follow a defined Secure Software Development Life Cycle process.
    d) OS and applications are hardened (OS guidance is provided by NCIA)
    e) Applications:
        i. Are supported with security patches.
        ii. Do not require an obsolete version of OS, libraries or dependencies to function.
    f) Security relevant events and account activity are logged.
    g) Users have the minimum set of permissions to accomplish their work tasks.
    h) The ASNMC implements NATO approved security solutions for anti-malware, Data Loss Prevention, vulnerability scanning, intrusion detection etc.
14. The ASNMC, in relation to the SATCOM M&C functionality, provides access control which for each individual user of the system defines:
    a) Its role(s) (e.g. IT (ASNMC) administrator, SATCOM administrator, SATCOM operator, SOC operator) with associated rights (e.g. manage ASNMC, view and/ or configure terminals, acknowledge alarms).
    b) Which resources the user can access, based on attributes (properties) of that resource (e.g. terminals or elements within a specific mission or of specific type).
15. The Hardware (HW) implementation is:
    a) Non-proprietary COTS for computing resources (e.g. server or workstation running the LM, CM and client applications). Serial protocol adapters and dry contact adapters as part of the solution may be proprietary, but must provide open and industry standard interfaces towards the LM computing resources.
    b) Scalable in performance through adding HW resources to CMs at data centres

and to LMs at static ground stations (which host hundreds of elements). At these locations, rack space and power are sufficiently available.

16. The Software (SW) implementation is:
    a) Modular, non-monolithic, following a Service Oriented Architecture or Micro services Architecture, in which:
        i. Main functions, including element specific APIs, are separate SW modules.
        ii. SW modules can be maintained independent of each other, minimizing the need for regression testing of the complete ASNMC if updates to SW modules are made.
        iii. Updates to the ASNMC SW can be applied gradually to the LMs and CMs (one by one rather than a big bang approach), and different versions of SW can co-exist.
        iv. Instabilities in one SW module do not create instabilities in other SW modules and the ASNMC.
        v. Modules are small in size, can hence lower the maintenance costs and can be updated over low bandwidth links.
    b) Resource efficient, such that for deployable terminals (which are the terminals with the lowest amount of elements) the LM function can be hosted on compact low power servers
17. Provides Trend Analysis and Anomaly Detection.
18. Provides templates or other mechanisms for the efficient provisioning of the LMs for similar terminals (i.e. topologies, type of elements, parameters to monitor etc).
19. Can make changes to the terminal topology definition through both LM level and CM, with synchronisation in both directions.
20. Supports the provisioning of links through the import of link parameters (in XML format) from the Purchasers Link Planning Tools, including:
    a) Translating the link parameters into modem specific settings and applying those to these modems, adjusting the monitoring parameters accordingly etc.
    b) Request fulfilment tracking.
21. Can store elements settings (configurations), and detect and log changes in the element settings
22. Can log control actions that the ASNMC applied to elements (i.e. changing the settings or status).
23. Provides and integrates a Configuration Management Database, which stores (and can ideally retrieve) element properties such as location, IP address, SW version, hardware revision etc.
24. Supports exclusive element control, or a lockout-tagout function, which avoids that multiple operators (or the ASNMC itself through scheduled actions) can simultaneously

take control of an element. Such exclusive control is a safety feature to avoid for example that a transmitter is activated or an antenna is rotated while an operator is working on this equipment.

3. Scope of Work

The NCI Agency aims to minimise new design and development as much as possible by utilising use of Commercial of The Shelf (COTS) product at maximum extent. The project work will mainly include system design, development of software drivers, test, verification & validation, integration of ASNMC system components, integration with external systems, trainings, site installations, security accreditation support, acceptance activities, and system support, etc.

4. Period of Performance

a. The Period of Performance is anticipated to start in Q1-2026 and end in Q2-2029. It is important to note that this timeline represents the anticipated duration of the Project, and adjustments may be made as per the requirements of the solicitation process and subsequent contractual agreement.

5. Warranty and O&M Support

b. Following acceptance of the final operational delivery, the contract will require warranty for any software delivered.

c. The contract is expected to include Operations & Maintenance (O&M) support following acceptance of the final operational delivery.]