

5G (ENCQOR) Technology Development Challenge  
**5G OSS for Mass Rail Transit System**

<b>Challenge Launch Date</b>	October 21 2019
<b>Challenge Deadline</b>	November 18 2019
<b>Challenge Statement</b>	<p>Public transportation serves a larger public interest, delivering numerous benefits to society, such as lowering carbon emissions, which improves and promotes healthier urban space. The efficiency of public transport also has a direct impact on the economies of cities. One of the cornerstones of success in Thales’s mission to provide 5G Smart Cities Solutions is in the area of Mass Transit systems. These solutions involve complex communication networks and multiple devices. Herein lies the challenge to find an efficient, effective and secure configuration management system.</p> <p>Thales Canada is interested in working with an Ontario based small and medium sized enterprise (SME) to develop a prototype of an operational system support (OSS) solution for the Thales SelTrac system optimized for transportation sector needs, particularly Urban Rail Transit systems.</p>
<b>Project Partner</b>	Thales Canada Inc.
<b>Timeline</b>	1 Year
<b>Available funding</b>	\$100,000
<b>Applicant Type</b>	Ontario small and medium sized enterprise
<b>Location</b>	Work can be completed remotely with scheduled online meetings and face-to-face workshops. Demonstration and testing will be scheduled and performed in different phases of project according to the plan that will be established between the applicant and Thales.

<b>Project Details</b>	<p>Thales is a firsthand witness of the challenges Mass Transit Operators are facing today:</p> <ul style="list-style-type: none"><li>- continuous demand in traffic growth, both in terms of passenger flow and the number of and frequency of mass transit vehicles;</li><li>- critical need to ensure passenger safety and security;</li><li>- demand for better and more intelligent remote management and monitoring that would result in further operational efficiency improvements through preventive maintenance solutions</li><li>- a strong demand for travel comfort improvement specifically providing passengers access to the internet</li><li>- a significant increase in the type and number of different services needed to be enabled within customer networks</li><li>- significant increase in the variety of networking devices, servers, platforms, sensors that will be deployed and utilized within customer solution</li><li>- never ending need for connectivity (IoT Internet of trains)</li></ul> <p>It is clear that one of the critical tools to accomplish all this will be the selection and optimization of a communication network. 5G will enable a number of new applications and inherently provide a platform on top of which we will be able to build all these future services. However, with all these new capabilities there are new challenges. A very important question that needs to be addressed is how do we securely and efficiently manage all these new resources.</p> <p>It is evident that basic element management system (EMS)/ network management system (NMS) system will not be sufficient for future operations. It is becoming clear that comprehensive an OSS specifically addressed and tuned for transportation sector needs is a possible way to address some of these issues.</p> <p>Thales goal is to provide highly available, secure, stable and well performing systems solutions to our customers. In order to achieve this goal, we will have to provide</p>

consistent management of the configuration of all network devices, such as routers and switches, application servers, firewalls, storage devices, 5G enode B's and 5G Core Network located in Thales wayside networks.

Standardization efforts in the railway industry has introduced the concept of fully Ethernet based train backbones that will be used to interconnect various types of subnets vital and non-vital (WiFi, video surveillance, passenger information services (PiS) that are located and installed on the train itself. So, the trains themselves are becoming complex networks with the mixture of network devices, computing devices and a variety of sensors devices (radar, lidar, inertia measurement unit (IMU), global positioning system (GPS), ultra wide-band radio (UWB) etc).

As a result, a consistent, automated and centralized device configuration management is key to meeting the following goals:

- Safe and secure operation of Thales SelTrac Communication Based Train Control (CBTC) systems
- Assurance that all system elements, network devices, servers, sensors are operating under configurations that are specified and accepted between Thales and their customers for particular deployments
- Traceability and easy audit of changes
- Infrastructure upgrades to support the new technologies
- Support the launch of new transportation lines or extension of existing lines with different set of services
- Greater operational agility for cost-effectively support for the introduction of new services, across multiple environments/devices.
- Full support of the legacy-to-next generation networks.

**Current Challenges Faced in Managing the Device Configuration within the Thales SelTrac Network**

Device Configuration Management is a process traditionally based on a combination of manual tasks and a specific set of tools. It is also highly dependent on the intimate knowledge that belongs to a set of super-users.

The change of teams, users or networks typically result in errors and inconsistencies, and basic tasks can become major problems when we add volume, technology evolution, complexity and continuous provisioning of new services into the equation.

A centralized, vendor-neutral Configuration Management system essentially automates tasks that were historically managed by hand or some ad-hoc legacy solution. The advantage of configuration management systems replacing these tools and super-users is ensuring repetitive, repeatable tasks can be done in a way that closes the door on human-error/mistakes, as these repetitive tasks are managed across a larger scale.

Device configurations can be backed up and restored, but what is more important is that standard best practices and knowledge for your network can be applied consistently through Device Configuration Management in an automated, centralized, consistent way. To address these issues, any Device Configuration Management system must provide the capability to assess the status of a wide range of devices, perform automation of repetitious backup and restore configuration tasks, allow configuration tracking, reporting, historical logs, etc. These device configuration management systems must, as a minimum, provide easy ways to manage this complexity and track configuration changes easily.

Furthermore, the control of user privileges allows customized access to specific functions for specific user groups, forcing changes to proceed through defined procedures while still providing ready access to required information. These functionalities result in reduced workload, high levels of accuracy, reduced errors, and the flexibility to respond swiftly and accurately to network events and changes.

**Given the background above the specific objectives of this project are as follows:**

The project should demonstrate and propose an architectural solution and basic prototype of the Thales SelTrac OSS solution optimized for the transportation sector needs especially Urban Rail Transit systems. More specifically the following details should be addressed:

Challenge 1:

- 1) Define a methodology and solution for the implementation of SW Connectors/Adapters needed for effective operation and interaction of SelTrac OSS taking in mind the need to address and deal with a variety of different devices in a multi- vendor environment:
  - Network devices, switches, routers, firewalls
  - Application servers running applications in a virtualized environment
  - Storage Servers and devices
  - Trains themselves and train on board network should be analyzed and modeled as individual logic units with many physical networking, computing and sensor devices.
- 2) Automated configuration management solution that shall enable periodically scheduled backup actions for specified devices, multiple schedules may be defined based on the requirements of different areas of the network
- 3) Automatic backup of a device configuration in response to a specific syslog message sent by a device
- 4) Backup of a device triggered by an application programming interface (API) request from an internal script or external system.
- 5) Optional automatic backup of a configuration prior to restoring a configuration to a device.
- 6) Discovery of all devices deployed in the network that are not known to the system and providing Active Inventory of the system enabling quick and easy audit procedure of particular customer deployment

Challenge #2:

- 1) Users must be able to easily and consistently perform multiple concurrent configuration tasks on large multi-vendor, multi-technology networks. Users require the capability to quickly fix and/or revert (rollback) to previous/known device configurations and network states.
- 2) Multiple user access based on assigned user group security profiles. Each user has access only to the information and capabilities that they require.
- 3) Consistent user presentation of configuration management functions independent of the device vendor or technology.
- 4) Automation to relieve users of tedious, repetitive work enabling them to focus and respond more quickly and accurately to network events and updates.
- 5) Management of large multi-technology, multi-vendor networks. Fast configuration changes/restorations enabling network stability and control.

Challenge #3:

- 1) Stored Configurations are out-of-date and inaccurate due to continual change in a dynamic environment: Accurate and agile configuration management is required to guarantee that stored configurations match actual running configurations, and that these are updated to reflect any changes performed in the network.
- 2) Automation to relieve users of tedious, repetitive work ensuring that required backups are performed regularly without depending on user actions.
- 3) Automated syslog triggered backup actions based on real-time events to ensure configurations are up-to-date.
- 4) Consistent mechanisms for users to manage configurations.
- 5) Common repository of current and past configuration information for quick configuration comparison, update and restoral.

Challenge #4:

- 1) Automated schedules, Syslog monitoring, allows configuration management timing and distribution of network access to be effectively managed.
- 2) Access to up-to-date network configurations to users thus avoids multiple device accesses and queries
- 3) Accurate configuration information is available to other management systems without requiring queries to the network devices.
- 4) These capabilities decouple uncontrolled network access from configuration management activities.

Challenge #5:

- 1) Maintenance of network reliability and security through SelTrac OSS Policy Manager where specific policy enforcement and auditing shall be enforced and managed.
- 2) Logging of all SelTrac OSS configuration and management actions.
- 3) Accurate, up-to-date access to device configurations in the network is easily available.
- 4) Management of user capabilities through assigned user group security profiles. Each user has access only to the information and capabilities that they require.
- 5) Device login and password information required to communicate with the devices is managed by SelTrac OSS and does not need to be provided to the users.

<b>Project Goals/ Outcomes</b>	<p>The desired project outcome is :</p> <ol style="list-style-type: none"> <li>1) A clearly defined architectural solution that addresses the stated challenges</li> <li>2) A definition of work required to fully implement the SelTrac OSS as per challenge statement.</li> <li>3) Demonstration of a prototype that interacts with a selected number of devices and servers that are commonly used in the Thales SelTrac deployments</li> </ol>
<b>Applicant Capabilities</b>	<p>2 SW Developers and Product Architect  Engineering team with a strong background in wireless/wired communications and network management software  Familiar with OSS for multi-national organizations and Enterprise Networks  Experienced in the design of OSS systems for multi-vendor based solutions  Experience in solutions capable of delivering secure, auditable transaction based management and service deployments</p>
<b>Additional Information</b>	<p>NA</p>