TERMS OF REFERENCE FOR THE R&D PROJECT

1. Title of the Project: Development and Validation of test method for Hardware Security Assessment of Electronic products / Field Equipment used in the Power System SCADA

Sectional Committee: LITD 10 "Power System Control and Associated Communications Sectional Committee"

2. Background

The proposal aims to address the critical need for the development of a test method, focused on Hardware Security requirements of the electronic products / Field Equipment used in Power System SCADA (Supervisory Control And Data Aquisition). It is imperative to conduct an in-depth study that evaluates the security performance of field equipment like Remote Terminal Unit (RTU) / Intelligent Electronic Equipment (IED) used in the Power System SCADA and Substation Automation Systems. Though there are Standards for communication and security conformance testing for these products, however hardware security like embedded Trojan in the form of malicious hardware logic built within the products or the firmware of the products are not available. This subject is still in the nascent stage and globally many works are happening towards this but as on date none of them are out with uniform evaluation / assessment procedures applicable for the range of products including products used in the power sector. The standardization and performance evaluation of these products are vital to ensure safety and cyber resiliency of power system operation. These deliverables will collectively contribute to the formulation of an Indian Standard for field products used in the power system SCADA for hardware security assessments / evaluation and provide valuable insights for the industries, utilities and regulatory bodies. The report would eventually be used to formulate an Indigenous Standard for developing test procedures for assessment of hardware security of the field products used in power system SCADA.

3. Scope

a) Study and analyze the existing literature which include but not restricted to the following:
   - National/ International Standards on the subject and related subject
   - Standard operating procedures (SOPs)/guidelines of laboratories
   - Journals and research papers
   - Any study conducted by other organizations
   - Any other relevant published information on the subject

b) Conduct a comprehensive study of existing standards related to subject and how those can be extended with modifications for the hardware security assessments of products by conducting laboratory experiments on a selected product.

c) Collect the database of testing infrastructure like test beds equipped with such test facilities or any other technically accepted method and users in the country.

d) Undertake 2 visits to laboratories equipped with such test facilities and collect information including but not restricted to the following:
   - Principle of the test method
   - Procedure for specimen preparation
   - Test Conditions
   - List of test equipment's used during the test
   - Test result representation
   - Laboratory Standard Operating Procedure (SOP) for the test method
   - Focused group discussion on testing related issues, challenges being faced and suggestion
   - Conformance testing methods being followed and details thereof

e) Undertake 4 visits to Load Despatch Centers/ Power Utilities to report on the procedures/ best practices being followed by them to assess the Hardware Security of Electronic products / Field Equipment used in the Power System SCADA

f) Visits to 2 manufacturing units to understand the product details and also to test tool / test equipment supplier facilities.

g) Selection of a representative sample of field products used in power system SCADA for testing. The sample size will include a minimum of 5 products, covering various types such as RTUs, IEDs, Bay controllers etc.

h) Expert group consultation

It's important to note that the scope is limited to only end products used in the field applications like RTUs & IEDS in the power system SCADA. The network components / equipment like router, firewalls etc. and basic component like Integrated Circuit (IC) / chip level are not considered in this proposal.

4. Expected Deliverables

The expected deliverables for this project are as follows:

a) Definition and Classification: A clear and comprehensive definition of hardware security assessment is to be provided as well as the probable security concerns are to be listed. Products are be identified and first phase of report submission will be limited to only those products.

b) Standards Review: A thorough review of existing standards related to hardware security for diverse products, in power sector including Information & Communication Technology (ICT), need to be conducted as detailed at 3 (a) & 3 (b). This review would identify gaps and areas where new standards are needed or existing ones require modifications.

c) Testing Methodology: A standardized testing methodology to be developed to assess the Hardware security vulnerabilities of the products. This methodology will include detailed procedures and criteria for assessing the cyber security posture of the products.

d) User Guidelines: Recommendations for cyber safe usage of field products used in the Power system SCADA.

5. Research Methodology:

a) Literature Review: A comprehensive literature review is to be done to understand the existing standards and studies related to hardware security in general and particular for power sector applications as defined at 3 (a) and 3 (b).
b) Data Collection: Gathering data on field products available in the market, including types, brands, and specifications. This will serve as a basis for product selection.
c) Focus Group Discussions: Conducting focus group discussions with potential users and experts in the field to identify key performance parameters from the point of cyber security.
d) Identifying test tools / test equipment availability: As this subject is in nascent area, very limited information is available on the test tools / equipment. Exercises need to be done to explore potential test tool / test equipment supplier for the hardware security assessment of products.
e) Manufacturer Visits: Visits to manufacturing units to understand the product details and also to test tool / test equipment supplier facilities.
f) Sample Selection: Selection of a representative sample of field products used in power system SCADA for testing. The sample size will include a minimum of 5 products, covering various types such as RTUs, IEDs, Bay controllers etc.
g) Laboratory Testing: Visit laboratories and collect data/ information as specified at 3 (d).
h) Feedback and Expert Consultation: Seek feedback and consultation from experts in IT & OT cyber security engineering to ensure the accuracy and relevance of the testing procedures.

6. Timeline and Method of Progress Review:

a) Project Initiation, Data Collection and Testing (First 3 Months): The project officially begins with a detailed review of the existing International/National Standards and other similar literature available on the topic. This phase also focuses on collection of data from manufacturers/laboratories/users and formulating test methodologies to address the Hardware Security Assessment of Electronic products / Field Equipment used in the Power System SCADA. The first draft of the project report is to be submitted during this stage.

b) Analysis and Assessments (Last 3 Months): A mid-term review is conducted to assess progress and adjust methodologies as necessary after taking feedback from concerned stakeholders and expert consultation. In these months, testing of the collected samples is to be carried out in the laboratories and the test methods and requirements prescribed are to be analyzed and assessed. The final project report is to be submitted.

This condensed timeline covers the essential phases for the hardware security assessments of field equipment used in power system SCADA within 6 months timeframe, ensuring efficiency in

project execution. Progress reviews will be conducted as needed to track developments and make timely adjustments.

7. Support BIS will provide:

BIS will provide access to latest available editions of Indian standards and/ or international standards relevant to the project, on request.

8. Nodal Technical Committee of BIS

Power System Control and Associated Communications Sectional Committee, LITD 10
Member Secretary – Ms. Alismita Khag, Scientist 'C', Electronics and Information Technology Department, Bureau of Indian Standards
(Email: litd@bis.gov.in)