IEC 61850 Industrial Communication Standards Under Test

F. Tilaro, B. Copy, M. Gonzalez Berges (CERN, Geneva, Switzerland)

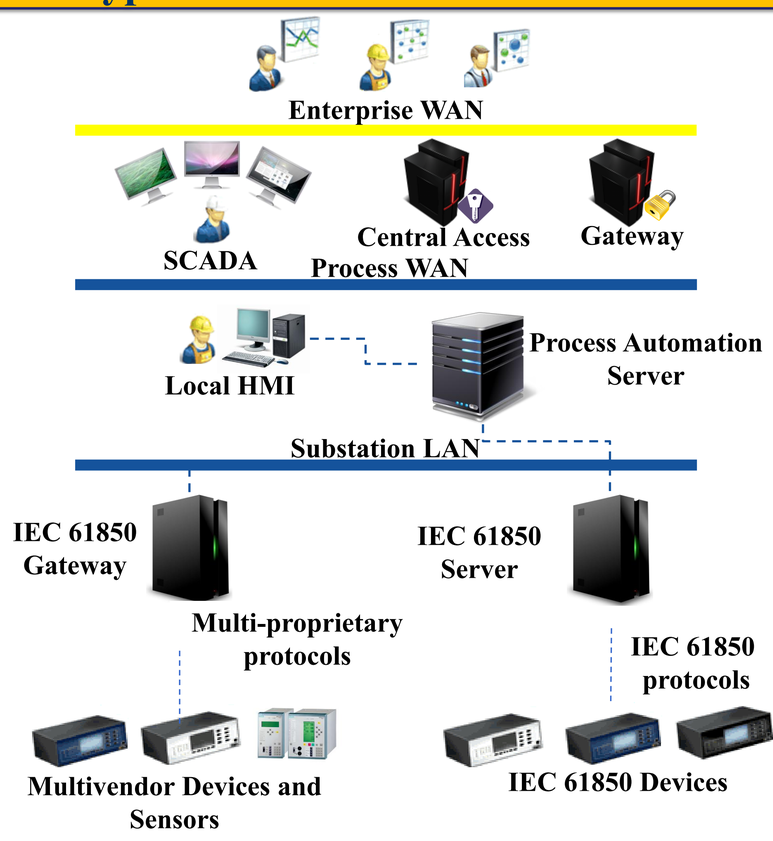
Abstract

IEC 61850, as part of the International Electro-technical Commission's Technical Committee 57, defines an international and standardized methodology to model electric power automation substations. It specifies a common way of communicating and integrating heterogeneous systems based on multivendor intelligent electronic devices (**IEDs**). They are connected to Ethernet network and according to IEC 61850 their abstract data models have been mapped to specific communication protocols: **MMS**, **GOOSE**, **SV** and possibly in the future Web Services. All of them can run **over Ethernet networks**, so they can be easily integrated with Enterprise Resource Planning networks; while this integration provides economical and functional benefits for the companies, on the other hand it exposes the industrial infrastructure to the external existing cyber-attacks. Within the OpenLab collaboration between CERN and Siemens, a test-bench has been developed specifically to evaluate the robustness of industrial equipment (**TRoIE**). This poster shows the general design and the implementation of the testing framework focusing on the IEC 61850 previously mentioned protocols implementations.

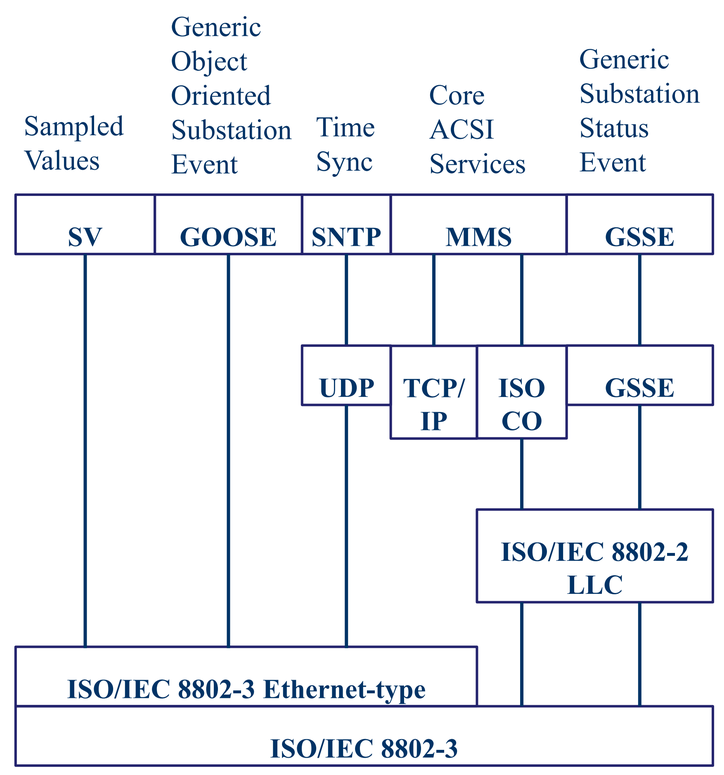
Smart Grids and Cyber Security

Smart grids are electrical power systems that are more efficient, more resilient, more advanced — hence "smarter" — than old , electromechanical power grids. Digitalized information and **communication technology** is used to drive the industrial process operations on the base of consumers' needs. As Smart Grid technology progresses, the information technology (IT) and **telecommunications** infrastructures have gained more and more importance at ensuring the **reliability** and **security** of the entire electric system. Therefore, the security of IT systems plays a fundamental role in the evolution of any **safe power smart-grid**. As pointed out by some historical events like the North America blackout in 2003, **cyber security** must address not only deliberate attacks, but also inadvertent compromises of the information infrastructure due to user errors, possible equipment failures, and even natural disasters. Any **vulnerability** might allow an attacker to penetrate any network boundary, gain access to the control software, and alter the industrial process data to destabilize the grid in unpredictable ways.

Typical Smart Grid Architecture



IEC-61850 Communication Model



IEC 61850 defines strict rules to map specific functions into devices independently from the manufacturers; this provides a common and clear interface for a complete interoperability with other vendors systems. Different types of communication load according to the specific service level:

- **MMS (Manufacturing Message Specification)**:
  - Application object model mapping
  - Non-time critical data messages
- **GOOSE (Generic Object Oriented Substation Event):**
  - Trip, interlocks and low level signals
  - Definition of Performance classes for critical communication: P1 for maximum delay of 10ms, P2/3 for 3ms signal delay
- **Sampled Values (SV):**
  - Multicast raw data messages like measurements
  - Performance Classes M1, M2, M3

The security evaluation has to take into account all of these performance requirements.

International Security Standards and Regulations

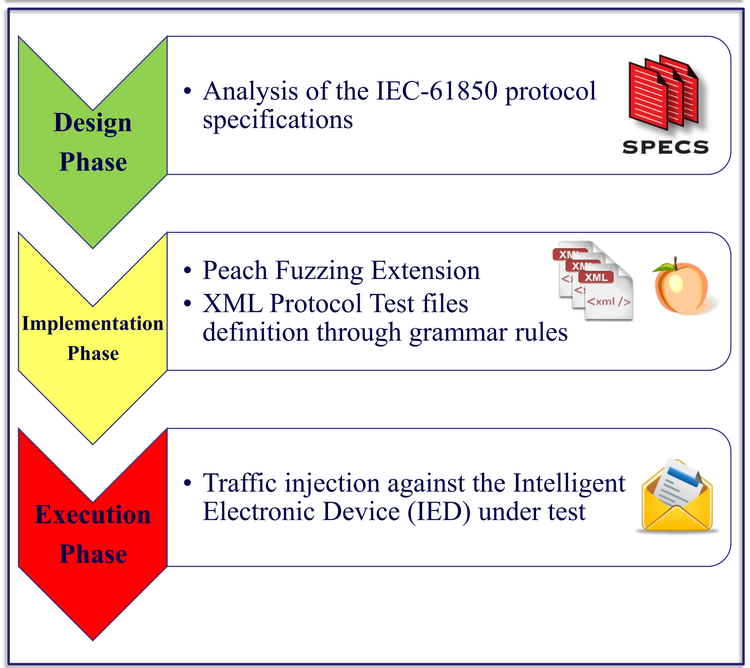
The **North America Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP)** provides a list of guidelines to identify and protect critical cyber asses to support the reliability of the Bulk Electric System.

The **National Institute of Standards and Technology (NIST) NISTIR 7628** presents an analytical framework to develop effective cyber security strategies specifically tailored for Smart-Grids.

The technical specification **IEC 62351** represents another effort to secure the IEC-61850 communication.

ISA Security Compliance Institute (ISCI) Communication Robustness Testing (CRT) program which has been produced on the basis of ISA-99 security standards specifications.

IEC-61850 Testing Process



Fuzzing and Grammar-based Security Testing

- **Objective**
  The enumeration of all possible faulty messages for each IEC 61850 protocol is exponential in the number of protocol fields; so it is necessary to devise a strategy to reduce the number of possible malformed messages to generate, but at the same time to increase the confidence that few vulnerabilities remain.
- **Strategy**
  The knowledge of communication experts has been translated into **XML files**, which define specific **grammars,** used as input of the **Peach fuzzing framework** to generate sequences of malformed messages.
- **Validation**
  If the protocol implementation cannot properly handle invalid packets, anomalous behaviours may occur and possible **security breaches** could be detected.

CONCLUSIONS

In conclusion the approach presented aims at discovering protocol implementation vulnerabilities by generating malicious non-standard traffic load on the basis of XML files. They contain the protocol specifications translation according to specific grammar rules. This testing methodology, making use of both fuzzing and grammar testing techniques, is so flexible that it could be used to generate any kind of communication traffic, therefore able to test any kind of communication protocol. The developed tools and extended testing framework can help any organization or control system manufacturer to assess and validate their own products; the result of these testing activities is an improvement of the security level, and then a better quality of the product itself. At last "Security-by-Obscurity" is not anymore a valid approach to secure any industrial system like power grids: it could work in the past when the industrial networks were totally isolated and disconnected by the external environments; today industrial systems are not immune against external threats, so they need to be provided with a more robust design, which takes care not only of the functional but also the security aspects.

Industrial Controls
Engineering Department

CERN EN Engineering Department