IEC 61850 Industrial Communication Standards Under Test

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

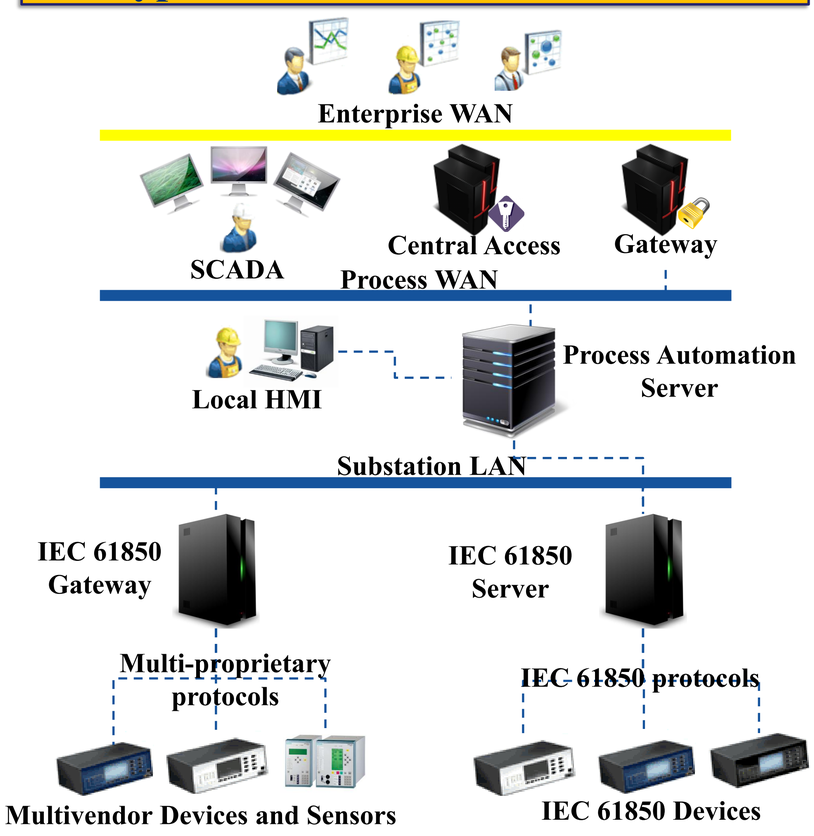
ABSTRACT

IEC 61850, as part of the International Electro-technical Commission's Technical Committee 57, defines an international and standardized methodology to design 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 TCP/IP 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 paper describes the design and the implementation of the testing framework focusing on the IEC 61850 previously mentioned protocols implementations.

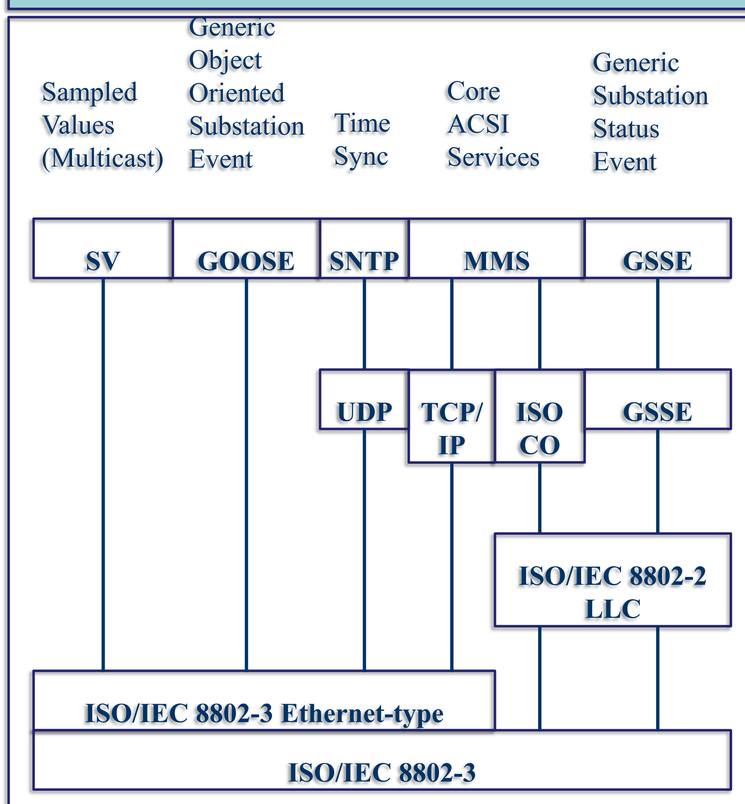
Smart Grids and Cyber Security

Smart grids are electrical power systems that are more efficient, more resilient, more advanced — hence “smarter” — than old , electromechanical power grids. Unlikely than the latters, smart grids use digitalized information and communication technology to drive the industrial process operations on the base of consumers’ needs; they are also capable of integrating diverse energy resources and emerging technologies. 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, but not only, 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. As shown in the figure the standards foresee different types of communication load according to the specific service level:

- this goes from **MMS (Manufacturing Message Specification)** over TCP/IP to Ethernet protocols. Normally the application object model is mapped to the MMS application layer, but time critical data messages make use directly of the Ethernet layer.
- Moreover the definition of several performance classes has been defined on the basis of the specific communication flow:
  - So **GOOSE (Generic Object Oriented Substation Event)** messages – like trip, interlocks and low level signals- represent critical communication and therefore must be transmitted within a maximum delay of 10ms (Performance Class P1), or for some signals even within 3ms (Performance Class P2/3).
  - The performance classes (M1, M2, M3) for **Sampled Values (SV)** messages are defined in IEC 61850-5, which are normally used for raw data messages.

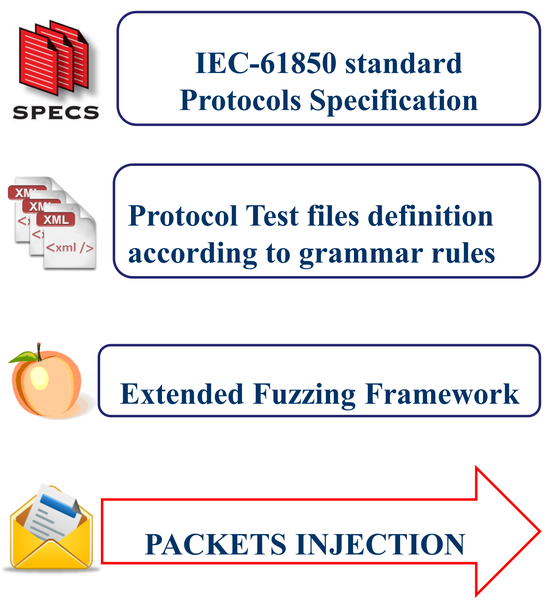
It is obvious, then, that our security evaluation has to take into account all of these performance requirements.

International Security Standards and Regulations

Among the latest activities to regulate and standardize security aspects in smart-grid systems, we could mention:

- the **North America Electric Reliability Corporation (NERC)** reliability standards define the requirements for planning an operating on the base of risk-analysis results. In particular the NERC **Critical Infrastructure Protection (CIP)** provide 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)** published a three-volume document: the **NISTIR 7628** presents an analytical framework for the developing of effective cyber security strategies tailored to the specific combinations of Smart-Grid-related characteristics.
- The technical specification **IEC 62351** represents another effort to secure the IEC 61850 communication in the substations real-time environment
- **ISA Security Compliance Institute (ISCI) Communication Robustness Testing (CRT)** program which has been produced on the basis of ISA-99 security standards specifications.

Testing Process



Fuzzing and Grammar-based Security Testing

Our approach to evaluate the robustness of the IEC 61850 communication model implementations is mainly based on **fuzzing** and **grammar** techniques. 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. To achieve that the knowledge of communication experts has been translated into **XML files**, which define specific grammars to generate sequence of malformed messages into a systematic manner. Grammars consist of a set of syntactic and semantic rules to cover specific context (generally protocol headers); if the protocol implementation cannot properly handle invalid packets, anomalous behaviour may occur and possible **security breaches** could be detected. These XML grammar-files are used as input of the **Peach fuzzing framework**, whose software components have been be extended and chained together to generate customized non-standard complex IEC 61850 data flows.

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, which contain the protocol specifications translations 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 current strategy has already proven to be effective at detecting communication robustness issues, and at the same time generic enough to be adapted to any communication protocol. “Security-by-Obscurity” is not anymore a valid paradigm to secure any system: it could work in the past when the industrial networks were totally isolated and disconnected by the external environments; today any industrial system needs to be provided with a better design which takes care not only of the functional but also of the security aspects.

CERN EN Engineering Department