IEC 61850 Industrial Communication Standards Under Test

Author: Filippo Tilaro

Supervised by: Brice Copy

Engineering Department

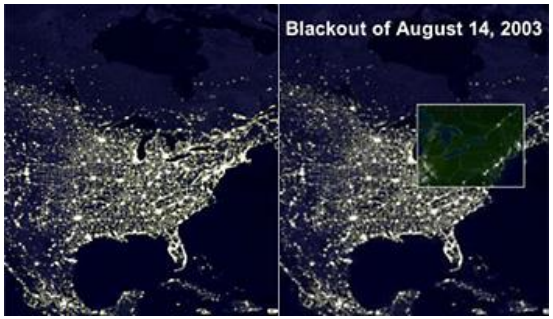
Overview

- Motivations and objectives
- Security standards and practical metrics
- Smart-Grid security requirements
- Testing techniques
- Test-bench implementation
- Security tests execution

Motivations

- Technological Evolution:
  - Growing interconnectivity between industrial control system (ICS) and Enterprise Resource Planning (ERP) network
  - IT functionalities expose ICS to existing cyber-attacks
  - Lack of exhaustive security standards and guidelines
- Growing number of discovered Industrial Control System (ICS) vulnerabilities
- Historically the efforts to secure ICS focused on physical protection and isolation
- Result:
  - recovery from attacks is expensive in terms of:

    time, cost, effort, reputability …



Scope and Objectives

- Objective:
  - To improve the Smart-Grid Control System security level
- Strategy:
  - Investigate cyber security standards
  - Determine key cyber security aspects relevant to CERN due to the heterogeneity and the openness of its experiments
  - Design and implement a test bench to assess the Intelligent Electronic Devices (IED) network robustness
  - Defining metrics for the evaluation of Industrial Control System (ICS) devices

Analyzed Security Standards

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.

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

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

IT and Industrial Security Model differences

- Performance requirements
  - best-effort vs. real-time
- Availability
  - reboot strategy vs. no downtimes allowed
- Service quality
  - general-purpose services (DNS, Domain Controller, …) vs. industrial services
- Updating and patching with possible “down-effect”
- Communication protocols
  - Public vs. Proprietary
- Software and component lifetime

ISCI CRT Testing Phases

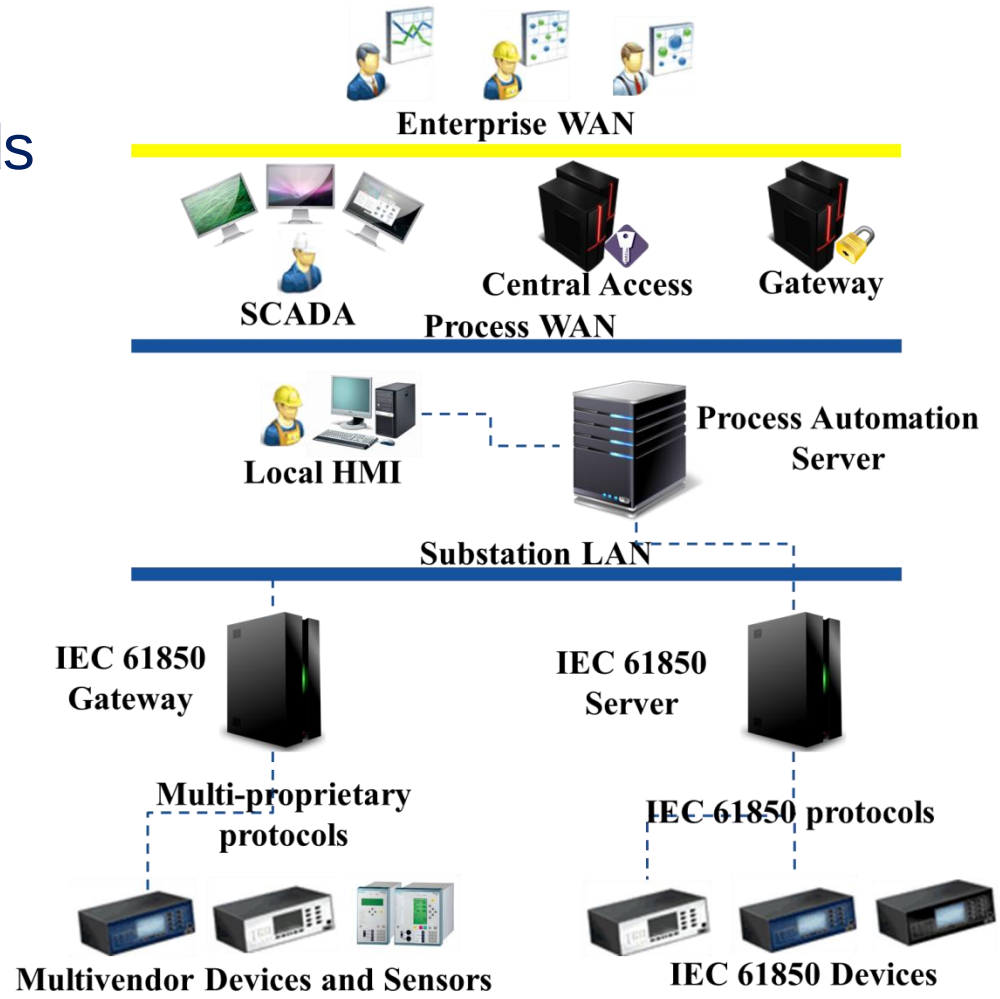
5 Main security testing phases:

1. Scanning
   - Definition of the Attack Surface and protocol functionalities
2. Load Tests
   - DoS protocol injection, communication and computation overload
3. Single Field Injection
   - Generation of values for each field maintaining constant the others
4. Combinatorial Fields Injection
   - Generation of values which involves two or more protocol fields
5. Cross State Fuzzing (for Stateful Protocols but not only!)
   - Generation of sequences

Security and Smart Grid

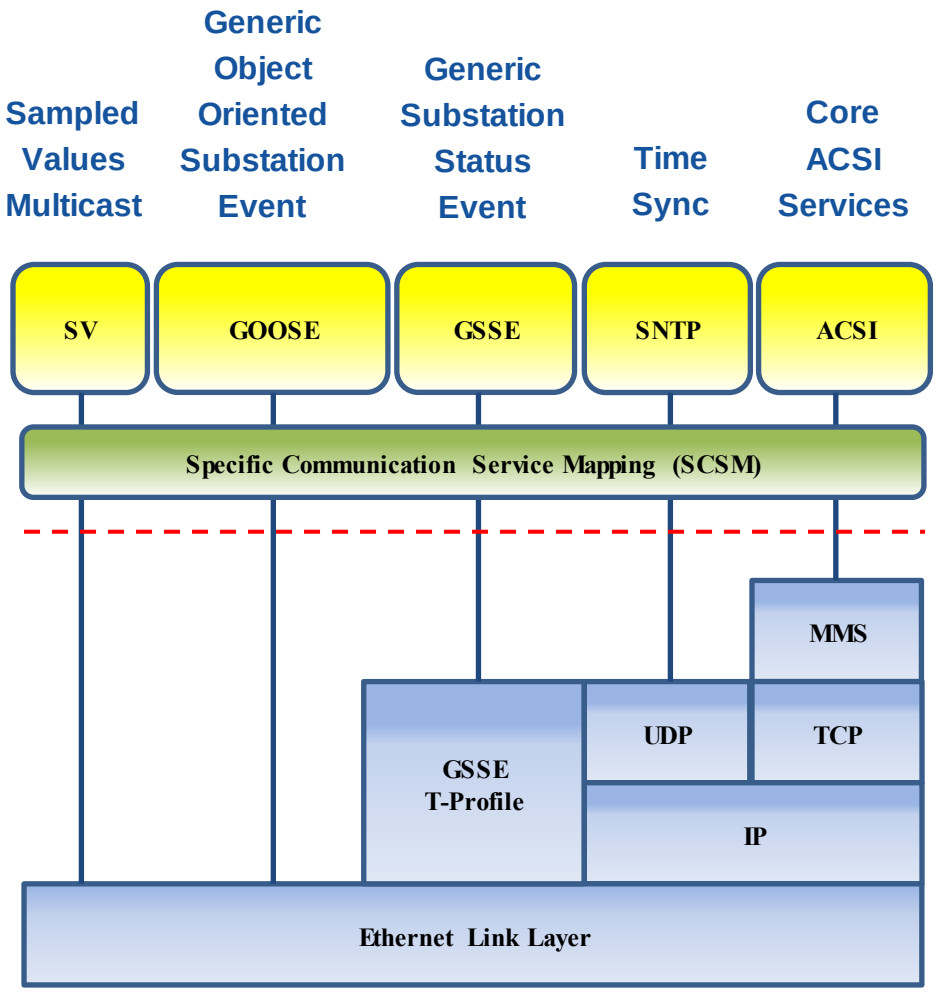
- More efficient than electromechanical power grids
- Integration of diverse energy resources and devices
- Make use of:
  - Digitalized information
  - Communication technology

Any vulnerability can affect the entire electrical system!



IEC 61850 Communication Model

- Different vendors system **interoperability**
- Different types of communication protocols:
  - MMS: application layer model
  - GOOSE: trip, interlocks and low level signals…
  - SV: critical raw data messages
- Different performance classes:
  - P1 (10ms), P2/3 (3ms) for GOOSE
  - M1, M2, M3 for SV



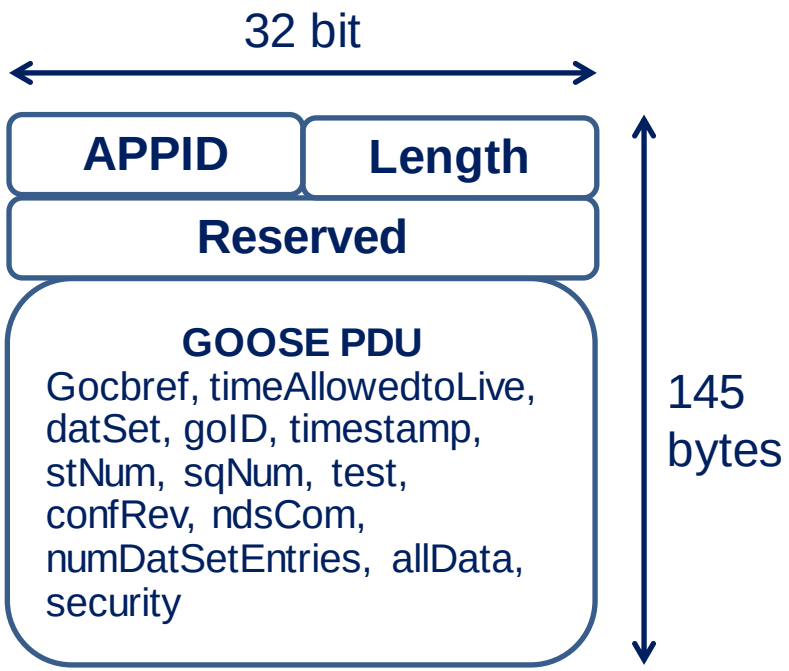
Protocol Robustness Testing

- IEEE defines robustness "*in the degree to which a system or component can function correctly in the presence of invalid inputs or stressful environmental conditions*."

- What is a robustness failure?
  - Failure to receive or send the expected packets
  - Inability to progress to next protocol state
  - Dropped connections
  - Lost or modified data
  - Any other incapability to communicate
  - MORE IMPORTANT: **Any unexpected effect in the control process** !

Why NOT Brute Force Testing?

- Simple but inefficient
  - Fields with varying length
  - Optional fields



For a basic sample of 145 bytes:

- 2^1160 =~ 1.566 e+349 combinations
- ~ 2^166 e+345 GB + Ethernet header
- It does not include sequences but single packets!

- Not all the combinations are interesting!
- The enumeration of all possible faulty messages for each IEC 61850 protocol is exponential in the number of protocol fields

Fuzzing and Grammar Testing

- Automated injection of valid/invalid data against the device under test
- Fuzzing is by nature “random”, but grammars make it reproducible: essential for debugging!
- Not exhaustive but we can cover specific sequences
- Grammar driven systematic domain ex
- Translation of the security specialists’ knowledge into grammar tests
- Tuning: find the right balance between random inputs (domain exploration) and static specifications (areas to cover)

Security Testing Requirements

- A Common Framework and not standalone scripts to inject traffic
  - Rely on stable software components and not “volatile” implementations
  - Easier to maintain
  - More scalable at handling the growing number of tests
- Tests Customization
  - Protocol header format
  - Protocol field values
  - Protocol state machine
- Reproducibility
  - Essential for any debugging activity

IEC 61850 Testing Process

Design Phase

- Analysis of the IEC-61850 protocol specifications: parts 8-2, 8-1, 5.

Implementation Phase

- Peach Fuzzing Extension
- XML Protocol Test files definition through grammar rules

Execution Phase

- Traffic injection against the IED (Intelligent Electronic Device) under test

Security Tests Execution

Client

GWT

JSON

Reverse Proxy & Access Control

APACHE

REST Web Service

Twisted Matrix Labs

Extended Peach Framework

Injection

IED Under test

- Authentication to run a test
- Built-in invariant test definitions
- No specific security knowledge
- OS Compatibility

Conclusions and Next Steps

- Achievements:
  - Design and implementation of a test-bench to assess the protocols communication implementation defined in IEC 61850 standards
  - ISA Secure Committee Institute (ISCI) - Certification Robustness Test (CRT) extension for IEC 61850 communication protocols

- Future activities:
  - Missing a standard reporting system
  - Further IEC 61850 communication protocols analysis
  - ICS Monitoring improvement

Any Questions

Thank you for attending!