Security in Power System Automation
Status and Application of IEC 62351

Steffen Fries, Siemens Corporate Technology, June 13th, 2017
Interoperability through security standards for the power utility ecosystem involves vendors, integrators, operators (Results from SEG-CG 2016)

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Integrator</th>
<th>Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC 62443.02.01 Establish IACS Sec. Program</td>
<td>IEC 62443.02.02 Operating IACS Sec. Program</td>
<td>ISO / IEC 15408 &amp; ISO/IEC 18045 Evaluation Criteria for IT Security</td>
</tr>
<tr>
<td>IETF RFC 7030 Enrollment over Secure Transport</td>
<td>IETF RFC 2752 CoAP Constrained Application Protocol</td>
<td>Power Systems - Data and communication security</td>
</tr>
</tbody>
</table>

### Guideline

- **Vendor**
  - Security Requirements for Components (IEC 62443.04.02)
  - System Security Requirements (IEC 62443.03.03)
- **Integrator**
  - Security Assurance Levels (IEC 62443.04.02)
  - Requirements for Substation Automation Protection and CS (IEEE C37.240)
- **Operator**
  - Security Requirements for IACS suppliers (IEC 62351-10)
  - Security Assurance Levels for IACS suppliers (IEC 62443.04.02)

### Requirement

- **Vendor**
  - Crypto module requirements (ISO/IEC 19790)
  - Substation IED Cyber Security Capabilities (IEEE 1686)
  - OCSP Algorithm Agility (IETF RFC 6960)
- **Integrator**
  - IEC 62451 Security Protocol support for GDOI
  - IETF draft-ietf-websig-doi-iec62351-9 Security Protocol support for GDOI
- **Operator**
  - Enrollment over Secure Transport (IETF RFC 7030)
  - ISO/IEC TR 27019 ISMS for Power Systems
  - Guidelines for Smart Grid Cyber Security

### Realization

- **Vendor**
  - Critical infrastructure protection
  - Guidelines for Smart Grid Cyber Security
- **Integrator**
  - Security Assurance Levels
  - Requirements for Substation Automation Protection and CS
- **Operator**
  - Security Requirements for IACS suppliers
  - Security Assurance Levels for IACS suppliers

---

*Source: [http://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx](http://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx)*
Digital Grid security involves vendors, integrators, and operators

Coverage of standards (Results from SEG-CG 2016)

Standards have different importance for

- Product and system vendor
- Integrator
- Operator

as they target

- specific technical means ensuring interoperability
- procedural requirements
- addressing risk based security requirements
- auditability of actions

Source: http://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx
Core communication standards for Digital Grids
IEC TC57 reference architecture with domain-specific cyber security

- IEC 61970 / 61968 Common Information Model (CIM)
- IEC 62325 Market Communication using CIM
- IEC 61850 Substation, Distribution, DER Automation
- IEC 60870 Telecontrol Protocols (serial/TCP)
- IEC 62351 Security for Power Systems
Cyber security in Digital Grids

IEC 62351 provides technical security measures and guidelines

Security means defined for

- Authentication and authorization (RBAC)
- Secure IP-based and serial communication
- Secure application level exchanges
- Security monitoring and event logging
- Test case definition
- Guidelines for applying specific security measures

by utilizing or profiling

- existing standards and recommendations
IEC 62351 Overview
Introduction to the standard, guidelines, and recommendations

The standard comprises several technical reports, which either provide overview about applications or a specific solution examples

- **Part 1 and 2**: Introduction and glossary
- **Part 90-1**: Guidance for using role-based access control (RBAC) specifically the handling of custom based roles
- **Part 90-2**: Guidance for supporting deep packet inspection (DPI) when using encrypted communication links
- **Part 90-3**: Guidance on applying monitoring and logging in power systems (using SNMP and syslog)
- **Part 10**: Overview and typical requirements to security architectures in power automation
- **Part 12**: Recommendations for the incorporation of decentralized energy resources DER in the power grid
- **Part 13**: Recommendations for editors of standards and specifications regarding the handling of security specific requirements in power systems
Part 3: Profiling of the existing security protocol Transport Layer Security (TLS) to protect TCP based communication. This part is used in conjunction with other parts of IEC 62351 and enables a re-use of existing solutions.

Part 4: Utilizes part 3 to protect the TCP based IEC 61850 communication (T-profile) and defines additional security mechanisms on application layer (A-profiles) to protect end-to-end security in scenarios with classical communication (e.g., control center to substation) or web-based approaches (e.g., for the introduction of DER using publish-subscribe mechanisms)

Example applications are control center communication and substation automation.
**Part 3:** Profiling of the existing security protocol Transport Layer Security (TLS) to protect TCP based communication. This part is used in conjunction with other parts of IEC 62351 and enables a re-use of existing solutions.

**Part 5:** Utilizes part 3 to protect the TCP based IEC 61850 communication (T-profile). Additionally, security mechanisms are defined to protect serial communication (IEC 61850-5-101) and CNP3 (IEEE 1518)

**Example applications** are control center communication and substation automation.
**Part 3:** Profiling of the existing security protocol Transport Layer Security (TLS) to protect TCP based communication. This part is used in conjunction with other parts of IEC 62351 and enables a re-use of existing solutions.

**Part 6:** Utilizes part 3 to protect the TCP based IEC 61850 communication (T-profile in conjunction with Part 4). Additionally, security mechanisms are defined to protect GOOSE and SV supporting multicast communication.

**Example applications** stem from substation automation, specifically the data exchange of protection devices or between PMUs in the transmission network.
IEC 62351 Overview
Data exchange via XML based files – Yes, but secure!

- **Part 11**: Provides protection of XML based data, which can be enhanced with RBAC elements
- **Example applications are provided by the data exchange between energy providers**
Part 7: Defines monitoring events for network management, which can be utilized over standard protocols for management to exchange monitoring information. The definition is in form of a Management Information Base (MIB) and is explicitly mapped to SNMP.

Example applications are network management and enable, e.g., the joint analysis of power system specific monitoring events in the context of an existing network management. This in turn enables the closer exchange of IT and OT relevant information to derive a system view.
- **Part 8**: Defines 3 profiles for role-based access control. They enable the assignment of roles to authorized users or applications, which can be dynamic. The assignment of one or more rights to a role has a more static character. The role information is either provided directly to the user/application or may be fetched by the accessed entity, e.g., via LDAP.

- **Example applications** target access control of local applications (HMI) but also remote administration and maintenance.
Part 9: Provides the base for the management of credentials and keys to be used in the security mechanisms of the different IEC 62351 parts. It addresses the management of certificates and corresponding private keys, which are utilized in almost every part of IEC 62351. Additionally it defines the group based communication security in the context of multicast communication scenarios.

Example applications for certificate and corresponding private keys comprise the user and component authentication. Group based security is applied in substation communication using GOOSE.
**Part 14:** Defines security events to be logged by the components used for error analysis and auditing. The events are defined in a general format, while the transport mapping is done to syslog specifically.

**Example applications are substation automation, specifically events generated in protection devices and substation controllers.**
IEC 62351 Overview
Conformance testing

- **Part 100**: Umbrella standard for conformance test descriptions of the IEC 62351 parts to help implementers to provide standard compliant functionality. The conformance test descriptions are intended to be applied in context with the associated communication standards (e.g., IEC 61850, IEC 60870, etc.)

- **Part 100-1**: Test cases associated with IEC 62351-5 and companion standards. Focus is on secure telecontrol over TCP and serial protocols in the context of IEC 60870-5-7.

- **Part 100-3**: Test cases associated with IEC 62351-3 as general base to be used by other test specifications

- **Part 100-4**: Test cases associated with IEC 62351-4

- **Part 100-6**: Test cases associated with 62351-6
### IEC 62351 Part

<table>
<thead>
<tr>
<th>IEC 62351 Part</th>
<th>Release</th>
<th>Activities (by June 2017)</th>
<th>Planned Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC/TS 62351-1: Introduction</td>
<td>2007</td>
<td>May need to be updated eventually</td>
<td><strong>No revision (New)</strong></td>
</tr>
<tr>
<td>IEC/TS 62351-7: Network and System Management (NSM) data object models</td>
<td>2010</td>
<td>CDV issued 12/2015,</td>
<td>Issue RR for IS after TR 90-1and 61850-90-19 issued</td>
</tr>
<tr>
<td>IEC/TS 62351-8: Role-Based Access Control</td>
<td>2011</td>
<td>Discussions on developing categories of roles</td>
<td>CD in late 2016, IS in late 2017</td>
</tr>
<tr>
<td>IEC/IS 62351-9: Key Management</td>
<td>2017</td>
<td>CDV in early 2016</td>
<td>TR 10/2012</td>
</tr>
<tr>
<td>IEC/TR 62351-100-2: Conformance test for IEC 62351-4/5 and companion standards</td>
<td>NWIP 2017</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEC/TR 62351-100-3: Conformance test for IEC 62351-3</td>
<td>NWIP 2017</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEC 62351-14 Cyber Security Event Logging</td>
<td>NWIP</td>
<td>Based on existing security logging</td>
<td>NWIP for 100-3 6/2017</td>
</tr>
<tr>
<td>IEC/TR 62351-90-2 Deep Packet Inspection</td>
<td>DC</td>
<td>TR to discuss the issues around deep packet inspection</td>
<td>DC 10/2016, comments received 01/2017, DTR 08/2017</td>
</tr>
<tr>
<td>IEC/TR Part 90-19: Using Role Based Access Control (RBAC) and IEC 61850</td>
<td>WG10</td>
<td>Joint effort with WG10</td>
<td>??</td>
</tr>
<tr>
<td>IEC/TR 62351-90-3 Guidelines for Network Management</td>
<td>Hold No PWI</td>
<td>Hold until ready to start document – Wait to submit PWI</td>
<td>PWI, DC 12/2017</td>
</tr>
</tbody>
</table>