Substation Automation
Cyber Security
Cyber security in your Relion Solutions Agenda

- IEC61850 based substation automation
- Why cyber security is an issue
- Threats, features and solutions
- Typical security architectures
- Security Features in RTU560
- Security Features in REB500
- Conclusions
Substation Automation Solution
System Overview (1)
Substation Automation Solution
System Overview (2)
Substation Automation Solution
Functional allocation

Functions
- Station Automation
- Monitoring
- Fault evaluation
- Event & Alarm Viewing and Acknowledgement
- Remote Communication for Telecontrol & Supervision
- Protection
- Control
- Monitoring
- Interlocking
- Data acquisition
- GIS or AIS Switchgear
- Instrument Transformers
- Power Transformers
- Surge Arresters
- Non-conventional trfrs
Substation Automation Solution
Product portfolio

Station Level
- MicroSCADA Pro
  - SYS600
  - SYS600C
- RTU560
  - RTU560A,C,G
- COM600

Comm
- AFS Family
  - AFS670, 675, 677
  - AFS650, 655

Bay Level
- Relion
  - 670 Series
  - 650 Series
  - 630 Series
  - 620 Series
  - 615 Series
Cyber security in your Relion Solutions

Agenda

- IEC61850 based substation automation
- Why cyber security is an issue
- Threats, features and solutions
- Typical security architectures
- Security features in RTU560
- Security features in REB500
- Conclusions
Cyber Security for Substation Automation

Why is Cyber Security an issue?

- Cyber security has become an issue by introducing Ethernet (TCP/IP) based communication protocols to industrial automation and control systems. e.g. IEC60870-5-104, DNP 3.0 via TCP/IP or IEC61850

- Connections to and from external networks (e.g. office intranet) to industrial automation and control systems have opened systems and can be misused for cyber attacks.

- Cyber attacks on industrial automation and control systems are real and increasing, leading to large financial losses

- Utilities need to avoid liability due to non-compliance with regulatory directives or industry best practices;
Cyber Security for Substation Automation
Drivers and attackers

Main Benefit
Reduce risk of damage by cyber attacks

Current drivers
Currently many initiatives and activities driven by technology and solutions
Cyber security approaches should be based on an understanding of risk

Who are the attackers?
Accidents / Mistakes
Rogue insider
Malware
Thieves / Extortionists
Enemies / Terrorists

Bottom line is
likelihood is unknown
consequences are potentially huge

Likelihood
## Cyber Security for Substation Automation

### Key Cyber-Security initiatives

<table>
<thead>
<tr>
<th>Standard</th>
<th>Main Focus</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST SGIP-CSWG</td>
<td>Smart Grid Interoperability Panel – Cyber Security Working Group</td>
<td>On-going *</td>
</tr>
<tr>
<td>NERC CIP</td>
<td>NERC CIP Cyber Security regulation for North American power utilities</td>
<td>Released, On-going *</td>
</tr>
<tr>
<td>IEC 62351</td>
<td>Data and Communications Security</td>
<td>Partly released, On-going *</td>
</tr>
<tr>
<td>IEEE PSRC/H13 &amp; SUB/C10</td>
<td>Cyber Security Requirements for Substation Automation, Protection and Control Systems</td>
<td>On-going*</td>
</tr>
<tr>
<td>IEEE 1686</td>
<td>IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities</td>
<td>Finalized</td>
</tr>
<tr>
<td>IEC 62443 (ISA S99)</td>
<td>Industrial Automation and Control System Security</td>
<td>Partly released, On-going *</td>
</tr>
</tbody>
</table>

* On-going: major changes will affect the final solution
Cyber Security for Substation Automation
Standards and their scope

- Graphical representation of scope and completeness of selected standards

*) source DTS IEC 62351-10 : Security architecture guidelines
Cyber Security for Substation Automation
Cyber Security in the system lifecycle

- **Development**
  - Verify
    - Security testing
  - Realize
    - Secure design
    - Secure code
  - Prepare
    - Threat modeling
    - Developer security training

- **Installation / migration**
  - Security testing
  - Secure configuration
  - Plant security architecture
  - Plant security assessment
  - Customer Security training

- **Operations**
  - React
    - Incident handling
  - Detect
    - Monitoring & audits
  - Protect
    - Security architecture maintenance
    - Platform patch management

---

© ABB Group
October 8, 2012 | Slide 12
Cyber Security for Substation Automation
Back to the basics

- Accept responsibility
- Security is about processes
- Ignore compliance - at least at first
- There is no such thing as 100% security
- Security does not come for free
Cyber security in your Relion Solutions

Agenda

- IEC61850 based substation automation
- Why cyber security is an issue
- Threats, features and solutions
- Typical security architectures
- Security features in RTU560
- Security features in REB500
- Conclusions
Cyber Security for Substation Automation

Cyber security and robustness threats

Network disturbance, malware, Cyber attacks

Security measures

1. Physical perimeter protection
2. Electronic perimeter protection
3. Defense in depth
Cyber Security for Substation Automation
Physical Perimeter Protection

- Physical protection
  - Physical fence
  - Concrete walls
  - Locked doors

- Physical access control system
  - Electronic key
  - Finger print, code, …

- Video surveillance
  - Motion detection
  - Perimeter violation
  - Loitering
  - Camera tampering
Cyber Security for Substation Automation
Customer concerns and ABB solutions

Protect
Is my system protected against an attack?

Manage
Can I sustain the security of my system?

Verwalten
Kann ich die Sicherheit meines Systems aufrecht erhalten?

Security Organisation
Sicherheitsorganisation

Product and System Hardening
Produkt- und Systemhär tung

Monitor
Do I know what happens on my system?

Überwachen
Weiss ich was in meinem System passiert?
ABB’s cyber security initiatives
Security organization & involvement

- **Customer Needs**
  - Same high level of security for all products & solutions
  - Fast response and reliable partner in case of a cyber security issue

- **ABB’s Solution**
  - Since many years ABB has a global, cross-functional cyber security organization
  - Security is well established in all process areas
    - Security assessment and robustness testing
    - Patch management process
    - Actively working in security standard committees
ABB’s cyber security initiatives
Product and System Hardening

- Customer Needs
  - Robust and reliable products and solutions

- ABB’s Solution
  - Centralized security testing center guarantees a common and best practice robustness testing of all products
  - Regular regression tests on ABB products and systems ensure a high level of robustness against cyber security attacks
Monitor
Do I know what happens on my system?

- **Customer Needs**
  - Alert about critical security alarms in real-time to enable fast corrective actions

- **ABB’s Solution**
  - Logging & Alarming: All security related events are recorded, severe events are sent as an alarm to the remote center
  - Reporting & Auditing: Produce necessary data, reports and documentation for an audit
Monitor Security events logging / Audit trail

RTU560 Features

- Event logs are stored secured
- Security event logs can be displayed via the device tools
- Send security events to external security log clients using syslog
- Security events can be sent via host protocol to remote control centers
Protect

Is my system protected against an attack?

- Customer Needs
  - Ensure reliable system operation (availability and performance)

- ABB’s Solution
  - Malware Protection: Prevent, detect, and remove malware, e.g. viruses, worm, …
  - Perimeter Protection: Restrict access by blocking / filtering inbound and outbound connections
  - Secure Communication: Encryption to prevent unauthorized users from reading and manipulating data
Protect
Integrated Virtual Private Network (VPN)

- VPN is prerequisite for using public networks (e.g. Internet)
- The VPN tunnel provides confidentiality, integrity, and authenticity.
- Confidentiality is keeping the data secret from the unintended listeners on the network.
- Integrity is ensuring that the received data is the data was actually sent.
- Authenticity is providing the identity of the endpoint to ensure that the end point is the intended entity to communicate with.
- Network equipment with VPN capability are expensive
- Integrated VPN is implemented in RTU560, for example
Protect
Secure communication via VPN

- **AFF650 VPN Features**
  - Secure tunneling of private communication through an insecure network (e.g. the Internet). Function of VPNs:
    - Authentication
    - Encryption
  - Applications: Connecting geographically distributed participants
    - Connection of RTU in substation to control center (through public or private network)
    - Connection of remote offices to headoffice.
RTU560 Features

- The RTU560 offers encrypted channel between the RTU and the IPsec Router on customer's side.
- The VPN tunnel provides confidentiality and integrity and authenticity.
- A secure communication via public networks (e.g. internet) is possible.
Can I sustain the security of my system?

- Customer Needs
  - Keep the security of the system up to date
- ABB’s Solution
  - Patch Management: Reduce risk of vulnerability for windows based system components
  - Backup & Restoration: Ensures complete data security and enables fast restoration in case of data loss /manipulation
  - Accounts & Authentication: Restrict access to intended users only, protected by high password complexity
Manage
User management, strong passwords

- Features
  - Enforced password complexity (min. password length, upper/lower case, number, non-alphanumerical)
  - Encrypted password storage
  - Administration of user accounts (Add new users with initial password, change passwords, delete users, assign and change user roles and permission for each role)
  - Applies to all ABB station level devices
Cyber security in your Relion Solutions

Agenda

- IEC61850 based substation automation
- Why cyber security is an issue
- Threats, features and solutions
- Typical security architectures
- Security features in RTU560
- Security features in REB500
- Conclusions
SAS 600 Series
Standard Security Architecture

Legend:
- Disabled ports / services
- Removable media access
- Individual User Accounts
- Malware protection
- Firewall
SAS 600 Series
Enhanced Security Architecture

Legend:
- Disabled ports / services
- Removable media access
- Individual User Accounts
- Malware protection
- Firewall
- Router
- Encrypted communication
SAS 600 Series
Advanced Security Architecture

Legend:
- Disabled ports / services
- Removable media access
- Individual User Accounts
- Malware protection
- Firewall
- Router
- Encrypted communication
- Industrial Defender Agent
Cyber security in your Relion Solutions

Agenda

- IEC61850 based substation automation
- Why cyber security is an issue
- Threats, features and solutions
- Typical security architectures
- Security features in RTU560
- Security features in REB500
- Conclusions
Cyber security for RTU560 products
Cyber security features in station level

- Overview of security features
  - Individual user accounts
  - Role based access control
  - Enforced password policies
  - Session management
  - Detailed audit trails
  - Secure remote management connection
  - Built-in VPN capabilities
  - Disabled unused ports and services
Cyber security for RTU560 products
Standard Compliance

- Our RTU560 products are compatible and support the following security standards:
  - NERC/CIP
  - IEEE 1686
Cyber security for RTU560 products

User Account Management

- User login and logout
  - Secured user login
  - Possibility to log off

Possibility to log off
Cyber security for RTU560 products

User Account Management

- **Password construction**
  - Following password complexities can be enforced by administration
    - Minimum password length
    - At least one upper and one lower case character
    - At least one number
    - At least one non-alphanumerical character
  - Encrypted password files can be exported or distributed to other RTUs via file transfer
Cyber security for RTU560 products

User Account Management

- Change user accounts
- Administration of user accounts is possible for:
  - Adding new users with initial password
  - Change passwords
  - Delete users
Cyber security for RTU560 products

User Account Management

- Change user roles
  - For each user account different user roles can be assigned.
  - User accounts can be modified and deleted
  - For each user role account permissions can be modified
  - Each user can be assigned to a role name
  - For each role permission can be assigned
Audit trail/user activity logging

RTU560 is able to record security relevant events (security event log/audit trail)

- The security event log is stored secured on the compact flash card in the RTU560 communication unit (CMU)
- The security event log can be displayed via the RTU560 web server if the user has the required access right.
- The security event log can be uploaded as CSV file.
Cyber security for RTU560 products
Secure communication

- **https support for web server (1)**
- Encrypted communication between PC and RTU560
- Standard browser can be used (e.g. Internet Explorer, Firefox)
- Selection of http:// or https:// possible by configuration
- Self-signed certificates, pre-installed at web client are used
- Installation example is documented
Cyber security for RTU560 products
Secure communication

- **https support for web server (2)**
- Certificate has to be installed on the Web client
- Installation procedure is described in the security deployment guideline Appendix A for:
  - Internet Explorer
  - Firefox
Cyber security for RTU560 products
User Activity Logging

- Support of Syslog/ArcSight clients
- Security events of RTU560 can be sent to external security log clients
- Syslog and ArcSight is a de-facto standard for logging of security events
- Syslog UDP/TCP, ArcSight TCP are supported
- Up to 3 clients per Ethernet port on a CMU can be configured
Cyber security for RTU560 products
User Activity Logging

- Security related events and alarms are required to be received at Network Control Center (NCC)
- Process information and security information should be available in the same environment
- Less complexity at NCC. No need for separate system for security issues.
Cyber security for RTU560 products
User Activity Logging

- NCC can also monitor security events
- Security events and alarms are now available in host communication protocols, PLC, HMI, process archive & logic functions
- New logic functions:
  - Security indication: an indication is generated for 100ms, if one or several security events occur
  - Security Alarm: if one or several security events occurs “x” times in a period. (configurable)
- Up to 32 security events can be mapped to one single indication/alarm
Cyber security for RTU560 products
Integrated Virtual Private Network (VPN)

- Using VPN channel, RTU560 can be connected to control system via the public internet.
- The data exchange is secured via the VPN connection.
- From the user point of view it looks like the RTU560 resides within the NCC network.
The RTU560 establishes a VPN connection to the IPsec router.

The VPN tunnel connects virtually the RTU560 network with the NCC network. Therefore a network to network connection is established which is transparent and secured.

If a connection is established, the RTU560 can be accessed by a control system using the internal virtual IP address. All IP based protocols can run on this connection.

The RTU560 can be remote configured and supervised using a web browser.

Authentication is handled by pre-shared keys.
Cyber security in your Relion Solutions

Agenda

- IEC61850 based substation automation
- Why cyber security is an issue
- Threats, features and solutions
- Typical security architectures
- Security features in RTU560
- Security features in REB500
- Conclusions
Cyber security for REB500
Standard Compliance

- REB500 is compatible and support the following security standards:
  - NERC CIP
  - North-American Electric Reliability Corporation Critical Infrastructure Protection
  - IEEE1686
  - Standard for Substation Intelligent Electronic Devices (IED) Cyber Security Capabilities
REB500 V7.60
User Access Management

Remote
- Manage user accounts
- Diagnostic

Central Unit
- Diagnose
- Maintenance
- Parameter Setting

Bay Unit
- Diagnose
- Parameter Setting
### REB500 V7.60

#### UAM - User Roles & Permission

<table>
<thead>
<tr>
<th>Permission</th>
<th>Viewer</th>
<th>Operator</th>
<th>System Engineer</th>
<th>Protection Engineer</th>
<th>Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>User Logging</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Restart</td>
<td>-</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Configuration</td>
<td>-</td>
<td>-</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Reset Indication</td>
<td>-</td>
<td>-</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Test</td>
<td>-</td>
<td>-</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Time modification</td>
<td>-</td>
<td>-</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>FW modification</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Factory Reset</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>●</td>
</tr>
<tr>
<td>User Access Management</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Activity Log</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>●</td>
</tr>
</tbody>
</table>
User Management
- Create
- Assign Role
- Password reset

Role Management
- Create
- Assign rights
REB500 V7.60
UAM - Database create and management

Master – Test System
- Create
- Test
- Export
- Store

Field Installation
- Import
### Record all user activities

### SA Integration
- IEC 61850-8-1 GSAL
- SysLog

---

**REB500 V7.60**

**User Activity Logging**

<table>
<thead>
<tr>
<th>Seqnr.</th>
<th>Datum</th>
<th>Zeit</th>
<th>Zeit ungültig</th>
<th>Benutzername</th>
<th>Zeitzugriff</th>
<th>Quote</th>
<th>Ergebnis</th>
<th>Benutzer abgemeldet</th>
<th>Ergebnis</th>
<th>Log in erfolgreich</th>
</tr>
</thead>
<tbody>
<tr>
<td>4000</td>
<td>2011-05-15</td>
<td>10:12:11:542</td>
<td></td>
<td>Anker</td>
<td>12:01</td>
<td>logging</td>
<td>Login</td>
<td>Log in erfolgreich</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4001</td>
<td>2011-05-15</td>
<td>10:12:11:435</td>
<td></td>
<td>Egon</td>
<td>12:01</td>
<td>login</td>
<td>Logout</td>
<td>Log out (Benutzer abgemeldet)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4002</td>
<td>2011-05-15</td>
<td>10:20:08:474</td>
<td></td>
<td>Anny</td>
<td>11:20</td>
<td>login</td>
<td>Logout</td>
<td>Log out (Benutzer abgemeldet)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4003</td>
<td>2011-05-15</td>
<td>10:20:08:560</td>
<td></td>
<td>Alex</td>
<td>11:20</td>
<td>login</td>
<td>Logout</td>
<td>Log in erfolgreich</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4008</td>
<td>2011-05-15</td>
<td>10:20:16:963</td>
<td></td>
<td>Peter Test</td>
<td>12:10</td>
<td>login</td>
<td>Logout</td>
<td>Log out (Benutzer abgemeldet)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4009</td>
<td>2011-05-15</td>
<td>10:20:16:166</td>
<td></td>
<td>Peter Test</td>
<td>12:10</td>
<td>login</td>
<td>Logout</td>
<td>Log in erfolgreich</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cyber security in your Relion Solutions

Agenda

- IEC61850 based substation automation
- Why cyber security is an issue
- Threats, features and solutions
- Typical security architectures
- Security features in RTU560
- Security features in REB500
- Conclusions
ABB’s cyber security activities
Summary

Protecting
against threats to substation automation systems

Monitoring
security and health activities in real-time

Managing
critical activities, such as configurations, changes and patches

Product and System Hardening

- Perimeter Protection
- Malware Protection
- Patch Management
- Backup, Restoration
- Accounts, Authentication
- Accounts, Authentication
- Reporting, Auditing
- Logging, Alarming
- Secure Communication
- Protecting

© ABB Group
October 8, 2012 | Slide 56
ABB’s cyber security activities

Summary

- Cyber security from ABB
  - is embedded in substation automation products and solutions
  - is an integral part of product development and quality assurance
  - comprises the latest technology and high competence
  - enables customers to protect, monitor and manage their systems
  - safeguards substations in a changing world
Power and productivity for a better world™
Organization & Processes
Power Systems Security Council

Harmonize security throughout complete portfolio
Provide customers with end to end security approach

Is security formally established in your organization?