CC and Industrial Security

Markus Bartsch
• **Availability, Integrity** and **Confidentiality** of transferred consumption and supply data

• **Security of energy supplies**
  Elimination of malfunction as well as potential manipulation of large quantities of smart meter devices

• **Secured Operation** of smart meter devices in unsecured environment

• **Privacy requirements**
  Prevention of creation / transfer of consumer profiles as defined by law

• **Access Control based on defined roles**
Future Energy Sources

- Solar
- Wind
- Geothermal
- Biomass
- Gas
- Oil
- Coal
- Nuclear

2010 - 2050

volatile
Smart Energy – Metering and Grids
The Future: ICT is an essential part

- Centralized and distributed volatile Energy Supply
- Load management in distribution networks
- Flexible Billing
- Secure Data Processing for consumer and management data
<table>
<thead>
<tr>
<th><strong>Organization</strong></th>
<th>Different Roles changing Partners</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Demand Control</strong></td>
<td>for large customers / end consumers</td>
</tr>
<tr>
<td><strong>Metering</strong></td>
<td>distributed Smart Metering</td>
</tr>
<tr>
<td><strong>IT Systems</strong></td>
<td>complete networked IT Systems</td>
</tr>
<tr>
<td><strong>Pricing</strong></td>
<td>time dependant, application dependent</td>
</tr>
<tr>
<td><strong>Renewable</strong></td>
<td>Plan: much more than 20% (~50%) Grid characteristics because of Renewable Virtual power stations</td>
</tr>
<tr>
<td><strong>eMobility</strong></td>
<td>extensive roll-out, beginning of V2G</td>
</tr>
</tbody>
</table>
Smart Grid – Information and Communication

Smart Meter / ICT Gateways

- Managed Agents

Maintenance

Portals

eMobile Charging Stations

Communication, e.g.
- Network: RFID, LAN, WAN
- WebServices,...
Smart Grid: Model

Source: http://www.nist.gov/smartgrid/
Problems in Process Control Technology (PCT) ... also in Smart Grid

- Use of traditional IT for PCT – which were designed stand-alone Systems:
  - Standard Protocols
  - Commercial Off The Shelf-Software
  - Connection to Office IT
  - Internet Connection
  
  → Threats of Office IT

- Different Requirements
  
<table>
<thead>
<tr>
<th>Traditional (Office) IT</th>
<th>CIA</th>
<th>PCT</th>
<th>AIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>(High)</td>
<td>Confidentiality</td>
<td>(Low)</td>
</tr>
<tr>
<td>Integrity</td>
<td>(Medium)</td>
<td>Integrity</td>
<td>(Medium)</td>
</tr>
<tr>
<td>Availability</td>
<td>(Low)</td>
<td>Availability</td>
<td>(High)</td>
</tr>
</tbody>
</table>

→ Traditional IT Security Concepts are not sufficient
Critical Infrastructures

Sectors & Branches

Transport / Traffic
- Aviation
- Maritime traffic
- Rail traffic
- Road traffic

Energy
- Electricity
- Nuclear power
- Gas
- Oil

Production
- Chemical
- Biologic
- Pharmaceuticals
- Defence

IT & T
- Telecom
- IT

Finance / Insurance
- Bank
- Insurance
- Stock exchange
- Clearing center

Supply
- Health care
- Rescue service
- Civil protection
- Food & Water
- Disposal

Government
- Federal Gov.
- State Gov.
- Municipalities
- Defense
- Police

Misc.
- Media
- R&D
- Culture goods & buildings
### Sectors & Branches

#### Transport / Traffic
- Aviation
- Maritime traffic
- Rail traffic
- Road traffic

#### Energy
- Electricity
- Nuclear power
- Gas
- Oil

#### Production
- Chemical
- Biologic
- Pharmaceutics
- Defence

#### IT & T
- Telecom
- IT

#### Finance / Insurance
- Bank
- Insurance
- Stock exchange
- Clearing center

#### Supply
- Health care
- Rescue service
- Civil protection
- Food & Water
- Disposal

#### Government
- Federal Gov.
- State Gov.
- Municipalities
- Defense
- Police

#### Misc.
- Media
- R&D
- Culture goods & buildings
## Sectors & Branches

### Transport / Traffic
- ISO 270xx
- Standard 100 (BSI)
- Common Criteria

### Energy
- VGB R 175
- **ISO 270xx** (BDEW WP)
- IEC 62351
- NISTIR 7628
- WIB M2784-X-10
- Common Criteria

### Production
- ISA 99
- IEC 62443
- Namur NA115
- ...

### IT & T
- ISO 270xx
- ITSEC
- Common Criteria (ISO 15408)
- FIPS 140-2
- ...

### Finance / Insurance
- ZKA
- EMVCo
- PCI
- ...

### Supply
- Standard 100 (BSI)

### Government
- Standard 100 (BSI)
- ISO 27001
- Common Criteria
- FIPS 140-2

### Misc.
- ?
Industrial Security – Norms and Standards

- „only“ Guidelines or Best Practice
  → must, shall, could

- Different Norms – not harmonized
  → ISO/IEC JTC 1 / SC 27

- Roles (Operator, Vendor) partly differed

- Prioritization / Scaling
  (Security Level, Specification Detail) not defined

- No concrete Vulnerability Analyses defined

- Evaluation Scheme is missing
  → Comparability

- Synergy between Security and Safety is missing
  → Threats vs. Hazards
IT Security and IT Safety

Security SECURITY Security

Hazards by IT → Protection of man

ISO 61508 SIL

Common Criteria EAL

Threats by man → Protection of IT

© TÜV Informationstechnik GmbH – Member of TÜV NORD Group
Smart Meter potential System Architecture

- Plant
- Transport
- Distribution
- Supplier
- Metering Service
- ICT Service
- Device Vendor

Communication Protocols
- PKI
- Cryptography
- Access Control
6. External DMZ / Internet
5. Office IT
   Email, Data Server, Office IT
4. Business Unit IT
   Data Management
3. Supervisory Control / Process Control Access Domain
   Logging and Control
2. Process Control
   BuB, Engineering, Online-Optimization and Diagnostic
1. Field Instrumentation
   Field Bus, Actors, Sensors
Process Automation

typical IT Security Components

- (industrial) Firewalls
- VPN
- Remote Access Components

Future:

- Device: ID/Auth
- Signatures / Time
- Security Modules
- Access Control
- Logging / IDS
- Security Management
Automotive (1)
Examples of PPs

- Digital Tachograph
- Alcohol Interlock
- Boordcomputer Taxi
Automotive (2)
future Topics

- Car Configuration
- Internet Connectivity
  - Entertainment Services
  - Traffic Information
  - Navigation / Localization Services (eCall)
  - Car Configuration – downloadable features
  - Remote Maintenance
- Car 2 X
- eMobility
  - Charging Infrastructure
Automotive (3) Internet Connectivity

- Method
  - Cell Phones / Entertainment System
  - OBD Interface

- Potential Security Features
  - Information Flow Control
  - ID / Auth
  - Access Control
  - Monitoring
1. IT Security and IT Safety

2. AIC instead of CIA
   - Availability / Reliability
   - Real-Time Requirements

3. Complexity – more important:
   - IT Systems / Processes
   - Maintainability

4. Harmonization
   - Industry
   - Policy
Thank you very much for your attention!

TÜV Informationstechnik GmbH
Member of TÜV NORD Group

Markus Bartsch
IT Security

Langemarckstr. 20
45141 Essen
Germany

Phone: +49 201 8999 – 616
Fax: +49 201 8999 – 666
E-Mail: m.bartsch@tuvit.de
URL: www.tuvit.de