Cybersecurity of industrial systems. Open problems and some ideas.

Stéphane Mocanu,
Laboratoire d’Informatique de Grenoble/INRIA
CTRL-A
stephane.mocanu@inria.fr
A cross-disciplinary viewpoint
- process
- control system
- computer science
INDUSTRIAL CONTROL SYSTEMS (SCADA)

Main asset: the physique plant

Intelligent sensors and actuators
Hard real-time communication

Controllers
Soft real-time communication

Supervisory and journaling
No real-time

Remote connections

IT

OT
Operational Technology
Cybersecurity triad revisited
- Availability is paramount (keep running under attack)
- Non-repudiation may be crucial (emergency stop)
- Real-time properties are important
- Reaction time to attacks is very short

Attacks targets the physical process
- Stuxnet, BlackEnergy, Industroyer, ....

Behavioral classification
- Event-based: sequential systems (aka Manufacturing) PLC controlled
  - All manufacturing systems
- Time-based: continuous systems (aka Process)
  - Feedback control based processes
  - Electrical transport and distribution (hybrid)
Primary attacks (Source BSI-CS005E Top 10 Threats and Countermeasures 2019)

<table>
<thead>
<tr>
<th>Top 10 Threats</th>
<th>Trend since 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infiltration of Malware via Removable Media and External Hardware</td>
<td></td>
</tr>
<tr>
<td>Malware Infection via Internet and Intranet</td>
<td></td>
</tr>
<tr>
<td>Human Error and Sabotage</td>
<td></td>
</tr>
<tr>
<td>Compromising of Extranet and Cloud Components</td>
<td></td>
</tr>
<tr>
<td>Social Engineering and Phishing</td>
<td></td>
</tr>
<tr>
<td>(D)DoS Attacks</td>
<td></td>
</tr>
<tr>
<td>Control Components Connected to the Internet</td>
<td></td>
</tr>
<tr>
<td>Intrusion via Remote Access</td>
<td></td>
</tr>
<tr>
<td>Technical Malfunctions and Force Majeure</td>
<td></td>
</tr>
<tr>
<td>Compromising of Smartphones in the Production Environment</td>
<td></td>
</tr>
</tbody>
</table>

Secondary attacks

- Privilege escalation
- Unauthorized access to internal systems
- Manipulation of fieldbus communication
- Manipulation of network components

Important remark
Recent mediatic events are Big Game Hunting
- Norsk Hydro
- Southwire
- Altran
- CHU Rouen
- Bouygues Construction
60% RDP attacks
RAAS is today golden mine
Source ANSSI CERTFR-2020-CTI-001
BEYOND RANSOMWARE ATTACKS

- Process oriented attacks
  - Malicious controls sent to the process (actuators) using legal frames
  - Injection of false data sensors using legal frames
  - Exploitation of IT/OT and physical process vulnerabilities

- Leads to
  - Loss of view
  - Loss of control
  - Physical process damage

- Proof of concept
  - “Aurora vulnerability” (thunderbolt-like effect attack) – Idaho National Laboratory
    - Current spikes on the secondary circuit of a generator, faster than the protections relay timing
  - Stuxnet
  - Blackout 2003
2003: Blackout of the north-eastern part of U.S.

- False sensor data (maintenance error)
- True state estimator image
- An overloaded generator is stopped
- A transport line is overloaded
- Vulnerability: a wrongly pruned tree (too high)
- A HV line is lost
- Vulnerability: a race condition bug is blocking the alarm system
- The network falls

Over 6 billion $ lost, 100 casualties

http://www.creos-net.lu/creos-luxembourg/infrastructure/reseau-delectricite

NERC Node Breaker Model Representation Webinar

LIGNES HAUTE TENSION (HTA)

Network running normally
BLACKOUT 2003

- Starting event: (accidental) false sensor data injection
- Exploits cyber and physical system vulnerabilities
- Loss of view (false supervisory view)
- Loss of control
- Physical system damage
- Human causalities (collateral)
- No protocol syntax or semantics violation
THE SYSTEM APPROACH

Control room (supervision)
- e.g. target control, diagnostics, alarms

High level controller
- e.g. trajectory control

Local controller
- e.g. speed and position control

Local loop

Supervisory control

Distributed control and synchronization

+ safety system
+ local HMI
SYSTEM APPROACH

- Everything, including communication system is part of the control function
  - Communication protocols are control oriented
- There is strong interdependence between control elements
  - Some control functions are distributed
- Security deployment has to be global
  - System oriented not global oriented
- The final target of the control function is the physical process integrity
  - Physical process model has to be taken into account
- Lots of ICS cybersecurity standards (IEC 61443, IEC 62351, etc)
- Improved device security
  - Signed firmwares
  - Some secured communication protocols
  - Logging systems
- Device and system access control
  - RBAC
- IDS
  - Flow inspection based
- Industrial protocols support in firewalls
  - Is this realistic?
- Data diodes
Controller side

- **Secured industrial communication protocols**
  - Not interoperable
  - Initial exchanges still using unsecured Ethertype communications

- **Certified PLC**
  - Control devices heavily rely on time synchronization
  - Interoperability

- **Certified SCADA**
  - Support for legacy (unsecured protocols) is unavoidable

Countermeasure side

- **Learn control model from (5 minutes) traffic aka “all by AI legend”**
  - Transients may take hours
  - Controllers are intended to compensate perturbations
    - Abrupt changes in control values are normal
Some open problems: a personal view
From controller to system
CONTROLLER : (CYBER)-SAFE PROGRAMMING LANGUAGES ?

- Controller periodic task

- Programming languages
  - 5 normalized (IEC 61131)
    - Sequential Function Chart (SFC)
    - Instruction Logic (IL)
    - Structured Text (ST)
    - Function Block Diagram (FBD)
    - Ladder (LD)
  - A non-standard one: Continuous Function Chart (CFC)
How Resilient is PLC Programming?

- **A simple control program**
  
  \[
  \text{Switch}_{\text{closed}} \quad \text{Lamp}
  \]
  
  Reads: if the switch is closed activate the lamp for one cycle
  
  Implicit action: if the switch is open do not activate the lamp

- **Alternative program**
  
  \[
  \text{Switch}_{\text{closed}} \quad \text{Lamp}
  \]
  \[
  \text{Switch}_{\text{closed}} \quad \text{Lamp}
  \]
  
  Reads: on a raising edge of the switch set the lamp on (permanently)
  
  Reads: on a falling edge of the switch set the lamp off (permanently)

- **First solution is more resilient to cyberattacks than the second one!**

- **Open problem:** evaluate the 61131 programming languages and define cybersecure programming patterns
WRITE YOUR VARIABLES EVERY CYCLE?

- Not always possible
- What about timed operations?

**Diagram**

```
Start_operation
                  Motor
                  (S)
```

```
TON_0
TON
EN ENO
IN Q
Motor
(R)
```

```
t#1h
PT ET
```

Reads: Start a motor and a timer
At timeout: stop the motor

Between “Start” and TON.Q variable Motor is never refreshed!

**Homework**: is the following program safe?

```
                 Lamp
                 /     \      
     Lamp       Lamp
```

Traditional PLC programming languages (LD, IL) are digital logic based
Everything else (e.g. mathematical operations) are (graphical) function calls

Decompilation shows that parameter values are not checked but types are
- overflow and divide by zero are possible, but apparently handled

Open problem: tools for FB vulnerabilities check
- Static analysis (decompilation) possible
- Needs an execution platform for dynamic analysis

Open problem: embedder OS vulnerabilities
- often VxWorks (commercial version 7, PLC manufacturer version 3.10 or earlier)
- development libraries may include old open source code (e.g. 2002 versions found in 2019)
Only network-based IDS are possible today
  ► End devices are too loaded to support host-based IDS

Network is part of the control function
  ► Process-aware detection need to include the process model

Open problem: cyber-physical models for intrusion detection
  ► Sequential systems
  ► Continuous systems
  ► Control functions modeling

Open problem: distributed detection

Open problem: cross-domain correlation
  ► Multiple attack surfaces
  ► SCADA log correlation
Sequence attacks

- Normal behavior:
  - T0: E↓, VP1↑
  - T1: P1↑, VP1↓, VP2↑
  - T2: P2↑, VP2↓, M1↑
  - T3: M1↓, VE↑
  - T4: P2↓
  - T5: P1↓
  - T6: VE↓

- Qualitative Attack:
  - VP2↑
  - M1↓
  - VE↑

- Quantitative Attack:
  - VE↓VE↑VE↓VE↑

PhD Oualid Koucham (co-supervised UGA/CentraleSupelec/DGA)

- Security patterns LTL (Dwyer) and MTL (Konrad)
- Runtime monitoring
- Cross-domain correlation (monitors and network activity)
Which security properties
- Stability
- Response-time
- Boundedness
- Static error
- …..

Which formalism
- STL seems to be a good candidate
- Monitorability of security properties

Handle the under-sampling problem
- At network level signals are sampled at a lower frequency than the controller
- Degraded view of the dynamics

Correlation
- Correlate with diagnostic system (physical level system deviation detection)
A general approach is difficult excepting for
- Well known control functions (PID for instance)
- Electrical grid protection functions

Timed-hybrid system
- STL model or another logic?

RTE Substation Protection Automation and Control Systems IEC 61850 Model
In large systems distributed monitoring seems more reasonable
  ► Due to network segmentation
  ► Large distances
  ► A probe per local loop seems more reasonable

Some global security properties may not be decomposed in local properties
  ► “hierarchical detection”?

Ex. Security property: “the four tanks are not simultaneously empty” cannot be locally decomposed.
Modern devices are multi-network, and multi-protocol

- 4 IP network interfaces
- 2 fieldbus interfaces
- 7 communication protocols

An internal variable may be accessed by different protocols at different addresses.
In Modbus there are several different possible requests to write the same variable.

Multinetwork-address normalization?
Cross network attack scenarios?
Several configuration files available on devices
  ► SCL, AutomationML, OpenPLC, etc

Flow and network cartography, device configuration and versions

Open problem: risk analysis oriented DSML
  ► Automatic data extraction and architecture model construction
  ► Risk assessment
  ► Network and flow segmentation
  ► IDS probes deployment policy
The end ?