THE FACIES TESTBED

Dr. Estefanía Etchevés Miciolino, PhD Student
University Campus Bio-Medico of Rome

Workshop - 14th December 2013
OVERVIEW

- Simulative scenario
- Solution proposed
- Configurations
- Realisation
- SCADA and interface
- System control
- Utilisation
- Types of attacks
- Comparison with other models
- Local network
- Future development
Water distribution system of Highlake City:

- Main water source
- Two residential areas
- One industrial area
Solution Proposed

Complex Systems & Security Laboratory – www.coseritylab.it
28 different configurations

- Serial
- Parallel
- Crossed connections
- Combined
REALISATION – GENERAL SCHEMA

- Sensors
- Pumps
- Valves

PLC

Modbus
TCP/IP

SCADA
HMI
- 5 tanks
- 1 reservoir
- 4 pumps
- 20 electric valves
- 6 manual valves
- 5 level sensors
- 1 PLC
REALISATION - USED COMPONENTS

- Structure:
  - 3m and 2m Aluminium profiles (40 mm x 40 mm)
  - 1 m x 1 m Expanded polyurethane panels
  - 50 cm x 50 cm PVC panel

- Tanks: PE (polyethylene) barrels
  - Main sources: 2 x 25 L
  - Residential areas: 2 x 10 L
  - Industrial area: 1 x 15 L
  - Reservoir: 1 x 125 L

Tank caps provided with an expanded polyurethane module using a watertight gasket, where the sensors are fixed.

- Pipes: Multilayer system, PE-Xb (cross-linked polyethylene), d = 16 mm
On/Off Pumps:

- Reservoir - Main sources: 3 x mini-type Pipe Pumps
  \[ Q_{\text{max}} = 20 \, \frac{L}{\text{min}}, \quad H_{\text{max}} = 10 \, \text{m}, \quad 220 \, \text{V}, \quad 0.09 \, \text{W} \]

- Main source - Industrial tank: 1 x EK-DCP 2.2 pump
  \[ Q_{\text{max}} = 6 \, \frac{L}{\text{min}}, \quad H_{\text{max}} = 2.2 \, \text{m}, \quad 12 \, \text{VDC}, \quad 6.5 \, \text{W} \]

- Sensors: 5 x GEMS Pressure/Level transducer series 11700
  - 1 ½’ G thread male connector, 0 – 1 \( m_{H_2O} \) (0 – 0.1 bar)
  - 4 – 20 mA Output
Valves:

- 18 x Evian Solenoid Series 263
  - ¼” G thread female connectors, On/Off (nOFF), 0 – 1 bar, 24 VDC input
  - 6 x Residential demand
  - 2 x Industrial demand
  - 8 x Main sources loss
  - 1 x Main sources by-pass
  - 1 x Residential tanks by-pass

- 2 x 2/2 Way Solenoid Valves
  - ½” G thread female connectors, On/Off (nOFF), 0 – 14 bar

- 2 x Non-return valves for pumps
  - Main tanks drain to Reservoir

- 5 x Manual valves + 1 x Manual valve (to drain)
Control system:

1 x PLC Schneider Modicon M340 (BMX P34 2020)
MODBUS communication over TCP/IP
PC interface over GE Fanuc IFix 5.0

PLC Modules:

- Digital I/O: Schneider AMM600 (Analog mixed I/O module, 4 U/I, 2 Out U/I)
- Analog I/O Modules: Schneider DDM 16025 (Digital mixed I/O module, 8 I 24 VDC 8Q relays)

Valves connected to relays (4 modules of 8 relays)
4 splitters (modules) of 8 pins
2 splitters (cable) of 16 pins
Digital Outputs of PLC of 32 pins
REALISATION

Complex Systems & Security Laboratory – www.coseritylab.it
- Empty weight ~ 100 kg
- Total weight ~ 250 kg
- Filling and emptying times:

<table>
<thead>
<tr>
<th>TANK</th>
<th>FILLING TIME</th>
<th>EMPTYING TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>2m 12s</td>
<td>3m 53s</td>
</tr>
<tr>
<td>T2</td>
<td>1m 38s</td>
<td>3m 49s</td>
</tr>
<tr>
<td>T3</td>
<td>2m 22s</td>
<td>4m 28s</td>
</tr>
<tr>
<td>T4</td>
<td>2m 10s</td>
<td>3m 34s</td>
</tr>
</tbody>
</table>
UNITY PRO XL v7.0:

- TCP/IP Communication
- I/O Modules configuration
- Variable creation and addressing
- Ladder programming:
  - Pumps activation
  - Valves activation
  - Sensor measurements
  - Level control
  - Automatic control configuration
- Modbus addressing
PLC PROGRAMMING AND SYSTEM CONTROL

- **PLC Addressing:**
  - Digital outputs: %Q 0.c.#
  - Analog inputs: %IW0.c.#

- **Modbus Addressing:**
  - Digital: %M#
  - Analog: %MW#
Types of control:

- Level control by settable setpoint
- Maximum level control

PLC PROGRAMMING AND SYSTEM CONTROL
iFIX v5.0:

- TCP/IP Communication
- Modbus database creation
- HMI Creation
SCADA AND INTERFACE
SCADA AND INTERFACE

<table>
<thead>
<tr>
<th>Tank</th>
<th>Manual Control</th>
<th>Active Control</th>
<th>Set Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tank 1</td>
<td></td>
<td>1500</td>
<td></td>
</tr>
<tr>
<td>Tank 2</td>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Tank 3</td>
<td></td>
<td>2000</td>
<td></td>
</tr>
<tr>
<td>Tank 4</td>
<td></td>
<td>2000</td>
<td></td>
</tr>
<tr>
<td>Tank 5</td>
<td></td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

Diagram with tanks, pumps, and flow lines.
DATABASE IMPLEMENTATION
DATABASE IMPLEMENTATION
TYPES OF ATTACKS

- Sensor fault emulation
- Valve fault emulation
- Pump fault emulation
- Communication fault
- Control fault
- Water loss emulation
- Manual noise generation
Single tank analytic model:

\[
\begin{aligned}
    x(t+1) &= x(t) + \frac{T_s}{A_t} \cdot \left( -A_p \cdot \sqrt{2gx(t)} + u(t) \right) \\
y(t) &= A_p \cdot \sqrt{2gx(t)}
\end{aligned}
\]

- **State variable** $x(t)$: water level at time $t$
- **Output variable** $y(t)$: output flow $Q_0$
- $T_s$ sampling time, $A_t$ tank cross-section, $A_p$ pipe cross-section

**Output flow** $Q_0$

**Input flow** $Q_i$
Simhydraulics model:

- **Settings:**
  - Initial tank volume = 0 L
  - Initial reservoir volume = 120 L
  - Tank diameter = 25 cm
  - Pipes diameter = 2 cm
  - Simulation time = 100 s
  - Pressure = 1 atm

- **Outputs:**
  - Time array
  - Input flow \( u = 1.492 \cdot 10^{-4} \text{ m}^3/\text{s} \approx 8.95 \text{ L/min} \)
  - Output flow
  - Tank volume
SIMULATION RESULTS
LOCAL NETWORK

Sensors

Pumps

Valves

PLC

SCADA

HMI

SWITCH
FUTURE DEVELOPMENTS

- Remote communication for attacks
- LabView interface via Modbus