Enabling the Experimental Exploration of Operating Procedures on Critical Infrastructures

Christos Siaterlis, Béla Genge, Marc Hohenadel, and Marco Del Pra

www.jrc.ec.europa.eu

Serving society
Stimulating innovation
Supporting legislation
Overview

• Introduction

• Motivation of the work

• Proposed approach: conceptual aspects & implementation

• Experimental validation

• Real-time demo of cyber attack targeting a simulated Power Grid

• Conclusions
Human operators and operating procedures

- Human operators are central components of today’s CIs

- Today’s large scale infrastructures are split in different administrative domains with multiple actors

- Their main role:
  - Supervision of physical infrastructures
  - Act based on largely predefined procedures
  - Taking decisions with local/global impact

- Interaction with the infrastructure:
  - Human Machine Interfaces (HMI)
  - Direct actions, e.g., turning on/off machines or configuring a firewall
  - By contacting other human operators
Motivation of the work

• The outcome of contingencies can be determined by operating decisions

• Human operators close an important loop in the operation of today’s CI: how physical-space might affect cyber-space
Motivation - Proposed approach

• “What-If” analysis needed

• *How can we explore the space of possible system states due to human operator procedures and decisions?*

• Our approach goes beyond Human-in-the-loop testing
• We follow an experimental approach

• We incorporate the human aspect in the cyber-physical testbed through real-time simulation
• Human aspect is modeled based on a predefined plan of operator procedures, e.g., operator manual
• Lack of human operator in cyber-physical system testbeds
Proposed approach – conceptual aspects

• Starts from existing testbed architecture
• Simulates operator procedures and HMIs
• Translates operator actions to real actions on the physical testbed and simulated physical process
• Interconnects multiple operator simulators
**Proposed approach – modeling operational procedures**

\[
\begin{align*}
\dot{T}_1 &= u_1 R + u_2 O_2 - u_2 O_1, \\
\dot{T}_2 &= u_2 O_1 - u_2 O_2, \\
\dot{\theta}_1 &= -0.0018 u_2 t_1^{0.8} + 0.9 u_1 - 0.15 u_2, \\
\dot{\theta}_2 &= (0.075 u_1 - 0.016) t_1^{0.8} - 0.1 x_2, \\
\dot{\theta}_3 &= (141 u_1 - (1.1 u_1 - 0.19) x_1) / 85, \\
y_1 &= x_1, \\
y_2 &= x_2, \\
y_3 &= 0.05 (0.1307 x_2 + 100 x_4 + c_x / 3 - 67.975), \\
... \\
M_k &= M_k - u_3 M_k, \\
\dot{M}_k &= T_{mix} - T_k, \\
\dot{T}_{sp} &= T_{mix} - T_{sp} + \frac{M_k (T_k - T_{sp})}{M_c}, \\
M_c &= \frac{M_k (T_k - T_{sp})}{T_k - T_{sp}}.
\end{align*}
\]

Mathematical model

Modeling

Simulink model

Running Matlab Real Time Workshop

Simulated operating procedures
Proposed approach – implementation

- Simulation environment for HMI & operator procedure models: Simulink

- Extension of our previously developed framework with a new Decision Unit

- Model outputs are translated to actions

- Each action can:
  - Run external scripts, e.g., configure firewall
  - Send commands to the simulated physical process
Proposed approach – implementation

- Operator procedures models are seen as “black-boxes” with inputs and outputs configured using external XML files

- Operator procedure model inputs:
  - Values read from sensors of simulated physical processes
  - Values provided by scripts/sensors running in the cyber/physical realm
  - Values provided by other operator procedure models

- Operator procedure model output:
  - The first output is always the action ID
  - The rest of the outputs are the action parameters, e.g., generated power

- The developed prototype was implemented in C# and C++
Experimental scenario – cyber attack on a simulated Power Grid (IEEE 30bus)

- Goal: experimental exploration of how distributed operators can react in case of contingencies
Experimental scenario basic assumptions

- Power grid divided into 4 regions of different administrative domains, 4 operators
- Adversary model: the control systems of one region (#3) get compromised and attacker controls loads trying to cause large-scale black-outs
- Operators of the remaining regions try to keep grid stable by load shedding & injecting additional power
Experimental scenario – operator procedure models

- The operator monitors the bus voltages and follows the operating procedures:
  - First, it tries to reduce loads, e.g., shut down street lights
  - If this is not sufficient, he starts additional back-up generators
- For region 3 & 4 control algorithms run in parallel
- The control algorithm in region 2 is activated on the command of the control in region 3
  -> simulate operator interactions
Experimental scenario – effect of attack

- Affects most buses; in 4 cases voltages drop below 95%
Experimental scenario – countermeasures in reg. 3 & 4

- Region 3: load shedding + inject power
- Region 4: inject power
Experimental scenario – countermeasures in reg. 2, 3 & 4

- Region 3: load shedding + inject power
- Region 2 + 4: inject power
Conclusions

• Human operator procedures play a crucial role in the resilience of cyber-physical infrastructures against attacks

• With today’s interconnected Power Grids operators need to interact in order to restore normal operation

• Operator procedures can be complex and their effect is not fully understood under different scenarios

• Automated What-if scenario testing is needed

• Existing testbeds need to incorporate the acts of human operators → by closing this loop we enable more realistic experiments
Real-time demo of a cyber attack on the IEEE30-bus grid
Questions?

Critical Infrastructure Protection (CIP)

Contact details:

M. Hohenadel, Head of CIP action
marc.hohenadel@jrc.ec.europa.eu