La cyber security per l' operatore della rete elettrica
modelli per il supporto alle decisioni

Electrical grid operator challenges in cyber security
models for a Decision Support System

E. Ciancamerla, B. Fresilli, M. Minichino, T. Patriarca

ENEA

Roma, 24 Settembre 2015
Sfide ed opportunità per l’operatore elettrico

• Soluzioni per prevenire o mitigare
  – (larghe) indisponibilità (black out) di energia elettrica ai clienti
  – danneggiamento dispositivi
    • elettrici (i.e. trasformatori/sottostazioni)
    • ICT based (SCADA & corporate network)

• validare le soluzioni con test beds

• nuovi scenari di rete elettrica (attiva) e di sistemi SCADA (internet of things)
  – generazione elettrica distribuita anche da altre reti (i.e. rete gas ed idrica): bilanciare la imprevedibilità della generazione da rinnovabile
  – SCADA (TCP-IP based) non più monolitico e isolato, ma basato su dispositivi ICT capillarmente diffusi tra le reti ed anche geograficamente
  – nuovo ruolo delle interdipendenze: non solo propagazione di guasti ma anche per miglioramento di efficienza e resilienza delle reti ed i sistemi SCADA

• sistemi di supporto alle decisioni (DSS)
  – vulnerabilità dei sistemi SCADA e processo di attacco
  – prevenire e mitigare le conseguenze su rete fisica e dispositivi SCADA
  – migliorare la Cyber Security dei sistemi SCADA, con nuovi sistemi, alimentati da modelli, capaci di proteggere l’intera catena di valore della rete elettrica.

• modelli per DSS: modelli eterogenei coesistenti con dispositivi reali
Operatori elettrici e contesto

- **Operatori elettrici**
  - Israel Electric Corporation - Israel,
  - Lyse - Norway,
  - CREOS - Luxemburg

- **Operatori interdipendenti**
  - gas: CREOS - Luxemburg; ASEC – Catania, Italy
  - water: La Société Wallonne des Eaux – BE; SIDRA – Catania, Italy;

- **Partner industriale**
  - SELEX-ES of Finmeccanica

- **Decision Support System (DSS)**
  - To predict, detect, analyze and react to cyber attacks (and other adverse events) on SCADA system which controls a Medium Voltage electrical grid

- **Models**
  - To support DSS development cycle (requirements, design, implementation and verification)

- **DSS validation**
  - by using hybrid test bed from electrical operator

The research activity funded by sequential EU projects: **MICIE** ([www.micie.eu](http://www.micie.eu)) and **CockpitCI** ([www.cockpitCI.eu](http://www.cockpitCI.eu)) - Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures - and the italian **SINERGREEN** project ([http://sinergreen.cdc.unict.it/index.php/it/](http://sinergreen.cdc.unict.it/index.php/it/)). Also the core of Horizon 2020 proposals
the Cyber domain
• a virtual domain created by man
• where everything is possible (with a click)
• continuously exposed 24/7
• everything is on sale
  • bots, vulnerabilities, hacker kits,…

Attacks are going on all the time !
Cyber threats to SCADA systems

Cyber Weapons - Stuxnet
An F16 just flew over a 1st World War Battlefield

@ Jart Armin & Raoul Chiesa, 2011.

Threats are just as sophisticated as needed!
Top operating systems in Industrial Control Systems

The search engine for Power Plants
Shodan is the world’s first search engine for Internet-connected devices.
Until 2010 ....... great attention but no evidence

then Stuxnet

the first cyber attack against a SCADA system!
Cybersecurity in SCADA

**FACT**: Evolution from proprietary and closed architectures to open, standards-based solutions for ICS based infrastructure

**CONSEQUENCE**: Cyber-attacks can come from any part of the infrastructure:

1. **FIELD Network** as SCADA systems
2. **OPERATION Network** as Telco system or monitoring/management system
3. **IT Network** as enterprise devices and services

and can target any part of it
SCADA functionalities

• In electrical grids, failures may cause the de-energisation even of large part of power customers and need to be located, isolated and repaired quickly and safely.

  – Failure location consists in the progressive re-energisation of electrical sections of the grid, by closure/aperture of circuit breakers, starting from the most upstream section of the grid to the most downstream section of the breaker originally tripped.
  – The process ends when the feeder protection at substation is activated and the faulty section is located and isolated.
  – Finally, on the repair of the faulty section, the grid is restored to its original configuration.

• FISR: Fault Isolation and System Restoration - procedure is based on grid monitoring, sensing of loss of power, circuit breakers operations, performed throughout Remote Terminal Units (RTUs).

  FISR degradation affects the quality of electricity supplied to grid customers.
Interconnected networks supporting FISR

*Electrical 22 KV grid portion*

Confidential
Interconnected networks supporting FISR

SCADA and corporate network
A single heterogeneous model supporting FISR

Power grid, SCADA system, Telco network

Confidential
DSS in CockpitCI

- Integrated Risk Prediction (IRP)
- Secure Mediation GateWay
- SCADA adaptor
- Cyber Detection and Analysis
- Public Network
- Services
- TLC field
- ELE field
- Smart RTU
- CockpitCI
DSS in SINERGREEN

*Italian project – active electrical grid, gas and water networks: interdependency versus energy efficiency*

- Interdependency: a key factor for energy efficiency
- Risk of disturbances propagation throughout dependency links
- Understanding of phenomenal complexity
- International research has made some progress
  - Holistic approach
  - Extensive use of modeling at adequate level of granularity, co-simulation, multi-formalism
DSS validation by electrical operator
i.e. by IEC Hybrid Test Bed

Confidential
Three kinds of cyber attacks and consequences

Once a vulnerability has been exploited specific adverse actions can be performed

- Malware spreading
- Denial of Service (DoS)
- and Man in the Middle (MITM)

- instantiated to topology and main devices of SCADA and corporate network

- Consequences on SCADA and the grid (QoS)
  - when SCADA executes FISR
  - when altering SCADA and grid status
Represent & compute cyber attacks, consequences and (prevention & mitigation) decisions

- Cyber attack process
  - Realistic SCADA devices, with specific cyber vulnerabilities
  - Realistic attacker strategies
  - Realistic cyber protection policies

- Consequences on SCADA and on electrical grid
  - Realistic simulation of SCADA & corporate network
  - Realistic simulation of the (active) electrical grid & of
    - gas network interdependences
    - water network interdependences
Heterogeneous modelling & test bed

to represent & compute cyber attacks, consequences and (prevention & mitigation) decisions

✓ heterogeneous modelling
  • to describe the (active and interdependent) electrical grid, in a simplified way
  • to represent SCADA devices
    – describing messages and message routes
  • to represent cyber attacks and to predict their consequences on SCADA and on electrical grid in a simplified way

✓ test bed
  • to reproduce the cyber attack process in more realistic way then modeling
Hybrid modelling approach for DSS

actual physical devices, emulators and simulators (as agent-based, discrete event, domain and traversal simulators) co-exist and are composed

✓ Cyber attack process: test bed
  • threats generators
  • Intrusion Detection systems
  • emulation or actual mock ups of SCADA devices (SCADA CC, RTU, links and actual protocols)

✓ Attack consequences on SCADA and electrical grid: heterogeneous models
  a good compromise between particular and general models shall be found (granularity)
  • electricity simulators: electricity parameters (i.e. efficiency) will requires a deep knowledge of the grid at physical layer
  • SCADA simulators: discrete event simulators
  • Interdependency simulators based on artificial intelligence, holistic and agent paradigms
Heterogeneous modelling tools already in use

- to model and analyze malware propagation in relation to the adopted SCADA & corporate network security policies, we use NetLogo, a programmable modeling environment for simulating natural and social phenomena;

- to compute consequence of Denial of Service (DoS) and Man In The Middle (MITM) attacks on specific SCADA devices, we use NS2, an open source tool for simulating communication networks;

- to calculate QoS values of the electrical grid, to estimate risk for final electrical customers, we use RAO.
• SCADA devices
  • SCADA Human Machine Interface (HMI): Vijeo Schneider
  • SCADA Control Server: Vijeo Schneider
  • Programmable Logic Controller (PLC): Modicon M340 Schneider
• cyber attack generation & monitoring
  • Attacker: Kali Linux Penetration Testing platform
  • Network Intrusion Detection System (NIDS): SNORT
Test bed: cyber attack generation & monitoring
Test bed: SCADA devices
How to measure attack consequences on SCADA and electrical grid?

The consequences on SCADA could be

- the lack or alteration of observability and controllability of the electrical grid and in turn the impossibility to execute adequate commands from SCADA

SCADA QoS indicators

- **DPR**, a global vision of how many packets are missing on the network;
- **TTBP**, Transmission Time Between two Packets;
- **RTT**, Packet Round Trip Time
- **Packets routing**;
- **LoV**, Loss of View,
- **LoC**, Loss of Control
- **Time Response**
Complete SCADA LoV & LoC on malware propagation: SIR model

Green: susceptible
Red: infected
Grey: resistant
How to measure attack consequences on SCADA and the electrical grid?

- The consequences on the grid could be the degradation of availability, reliability and quality of electricity to customers, typically regulated by a National Electric Authority.

- Electrical grid QoS indicators:
  - duration of electrical interruptions for customer for year
  - the number of long/short electrical interruptions for customer per year
  - SAIDI - System Average Interruption Duration
  - SAIFI - System Average Frequency Interruption
  - CAIDI - Customer Average Interruption Duration
  - overvoltage values and duration dangerous levels - damages to equipment or to customers.

\[ Tn = \sum (KVA \times \text{Duration}) / \text{Installed KVA} \]

Tn : equivalent time of complete loss of electricity for all the customers while executing FISR. More the FISR process takes, greater the Tn is.
Cyber attack on (Radio VHF Unit 1 of) SCADA: Tn computation on different segments of the electrical grid by RAO

Cyber attack scenario: no attack

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Electrical grid segment number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Duration, min</td>
<td>10</td>
</tr>
<tr>
<td>Tn, min</td>
<td>5.28</td>
</tr>
<tr>
<td>Commands sent</td>
<td>6</td>
</tr>
<tr>
<td>Delivery time, min</td>
<td>0</td>
</tr>
</tbody>
</table>

Cyber attack scenario:

<table>
<thead>
<tr>
<th>Time</th>
<th>Element</th>
<th>Up</th>
<th>Degraded</th>
<th>Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>2 (Radio VHF Unit 1)</td>
<td>0.0</td>
<td>1.0</td>
<td>0.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Electrical grid segment number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Duration, min</td>
<td>16</td>
</tr>
<tr>
<td>Tn, min</td>
<td>9.28</td>
</tr>
<tr>
<td>Commands sent</td>
<td>6</td>
</tr>
<tr>
<td>Delivery time, min</td>
<td>1.333</td>
</tr>
</tbody>
</table>
Future work

- integration
  - heterogeneous modelling platforms
  - modelling and test bed environments
  - ENEA environment with test beds of electricity operators