Supply chain attacks – Understanding and investigating potential supply chain attacks in IEC 61850 substations

Marthe Kassouf & Deepa Kundur

October 29th, 2020

Hydro Québec

UNIVERSITY OF TORONTO

Presentation Outline

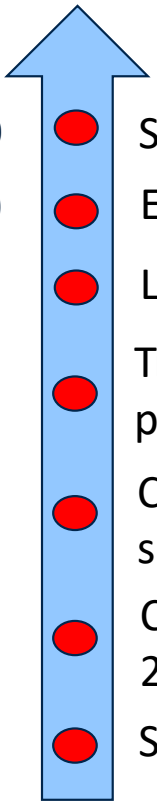
- Evolution of cyberattacks against critical infrastructures
- Supply chain vulnerabilities and attacks
- IT/OT convergence-based cybersecurity enhancement
- Use cases
- Recommendations

Evolution of cyberattacks against critical infrastructures

- The growing digitization and the increasing interconnectivity of automation and control systems are among the major drivers of critical infrastructures modernization and service enhancement.
- Benefits of power grid digitization include better monitoring and control of power generation, transmission and distribution processes, improved maintenance prediction and reduced costs, better management and integration of distributed energy resources (DERs) and enhanced customer services.
- The digital transformation of power grids comes with significant challenges such as leveraging the convergence of technologies, ensuring efficient system integration and standardization, and restricting the exposure to cyber threats!

Evolution of cyberattacks against critical infrastructures

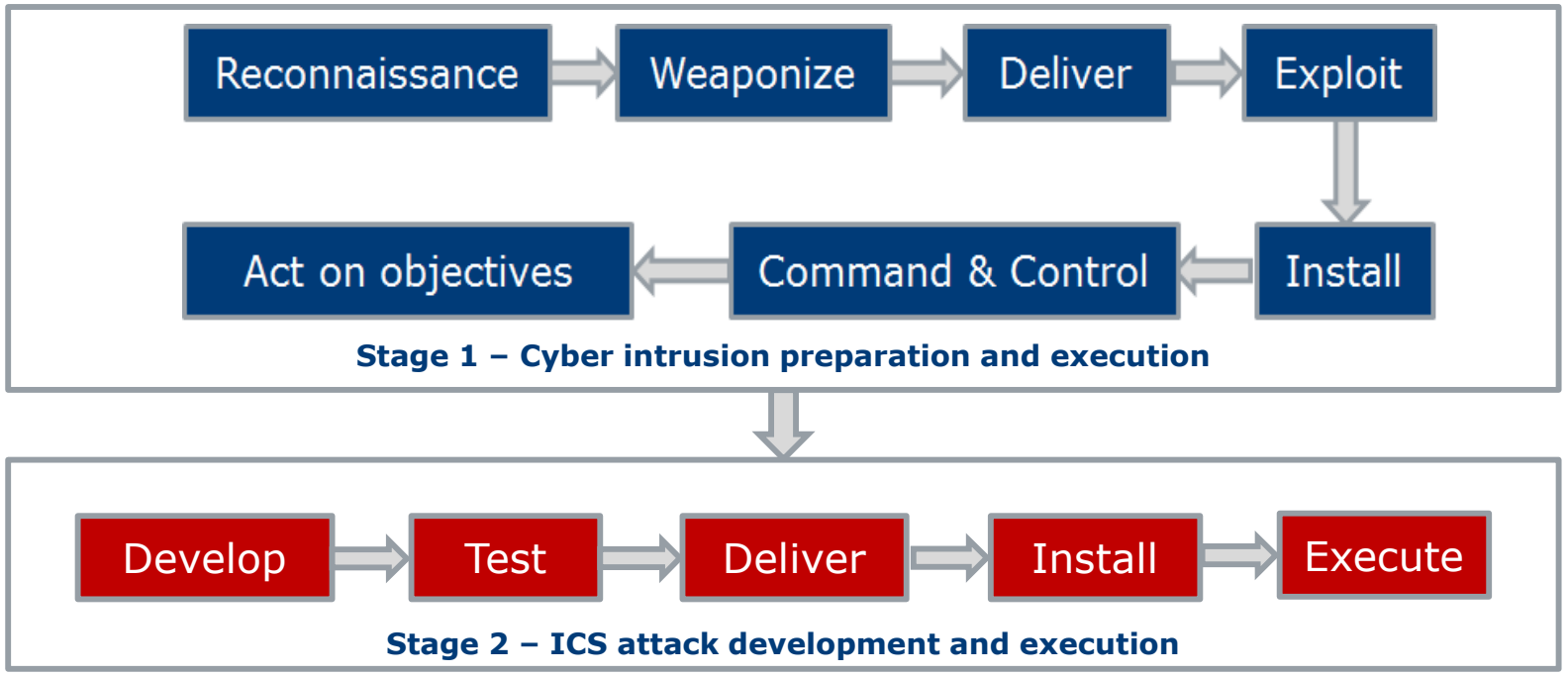
Recently reported cyberattacks against critical infrastructures:



2020	Sodinokibi ransomware attack targeting a Brazilian-based electrical energy company
2020	EKANS ransomware attack targeting ENEL and Honda
2019	LockerGoga ransomware attack disrupting the Norsk Hydro operations
2017	Triton attack against the safety instrumented systems of a Middle Eastern petrochemical facility
2016	Crashoverride malware used in an attack taregting a Ukrainian power transmission substation
2015	Complex cyberattack taking 27 power substations offline and creating outages for 225k customers in Ukraine
2010	Stuxnet malware attack targeting Iranian nuclear facilities

Evolution of cyberattacks against critical infrastructures

- Different vulnerabilities can be exploited in order to launch cyberattacks against industrial control systems (ICS) using a variety of adversary tactics and techniques such as those defined in the MITRE ATT&CK[1] knowledge base.
- ICS cyberattacks are better characterized using an exaggerated kill chain[2] or an ICS Cyber Kill Chain model:



1 https://attack.mitre.org.

2 Assante M. J. and Lee R. M., *The Industrial Control System Cyber Kill Chain*, SANS Institute Reading Room Site, October 2015.

Supply chain vulnerabilities and attacks

The NISTIR 7628 report (Rev. 1, 2014) power grid vulnerabilities can be classified in four categories:

- Software/firmware: software development and application programming interface vulnerabilities.
- Platform: design, implementation, security configuration and system operational vulnerabilities.
- Communication network: vulnerabilities associated with the communication protocols and networks interconnecting devices and systems.
- Policies, procedures and people!

Vulnerabilities belonging to these four categories can be found in the power grid supply chain!

Supply chain vulnerabilities and attacks

Controlling the supply chain vulnerabilities is difficult because of:

- The lack of manufacturing standards and the difficulty of ensuring the integrity of implemented standards.
- The lack of reliable product testing and certification processes.
- The lack of supply chain security approving authorities.
- The wide deployment of supply chain items with potential cyberthreats throughout the information and communication technology (IT) and operational technology (OT) power grid components.
- The need for power utilities to deal with different manufacturers, vendors, system integrators and service providers when acquiring IT/OT devices.

Supply chain vulnerabilities and attacks

Supply chain attacks can be executed when adversaries act on objectives using hidden backdoors that have been inserted through the manipulation of:

- Hardware and firmware components in IT/OT devices prior to delivery to the power utility.
- Software elements: compromise of application source code, compromise of software update and distribution mechanisms, and injection of malicious codes through the compromise of legitimate software and development tools' acquisition.
- The human element: luring service providers, equipment suppliers or vendor representatives in order to gain access to the targeted enterprise or operational power grid systems.

Supply chain vulnerabilities and attacks

- Preventing supply chain attacks is difficult and requires power utilities to take actions, such as:
  - ✓ Maintaining an updated IT/OT asset inventory.
  - ✓ Implementing reliable supply chain risk management (e.g. NERC-CIP-013-1) yielding risk assessment results that can be used for appropriate threat modeling and response planning.
  - ✓ Employing redundant hardware/software elements that are delivered to the power utility through different supply chains.
- Supply chain attack detection capabilities can be improved via thorough asset testing in almost-real/real environments prior to deployment and via rigorous monitoring mechanisms in operational environments.
- Supply chain attack mitigation should be part of a comprehensive cyberattack response plan.

IT/OT convergence-based cybersecurity enhancement

- Power utility operators and owners need to design structured approaches with efficient detection, mitigation and prevention actions to counter potential cyberattacks!
- First line of defense: Ensuring compliance with security standards
  - ✓ The IEC 62351 and IEC 62443 standard series
  - ✓ IEEE standards such as IEEE 1686 and IEEE C37.240
  - ✓ The NIST publications: NISTIR 7628 and the SP 800 specifications
  - ✓ The NERC CIP requirements
- The standards' recommendations provide only a minimal protection:
  - ➢ Implementations can embed different vulnerabilities
  - ➢ Insufficient immunity against attacks perpetrated by knowledgeable intruders or insiders
  - ➢ Inefficient protection against supply chain attacks!

IT/OT convergence-based cybersecurity enhancement

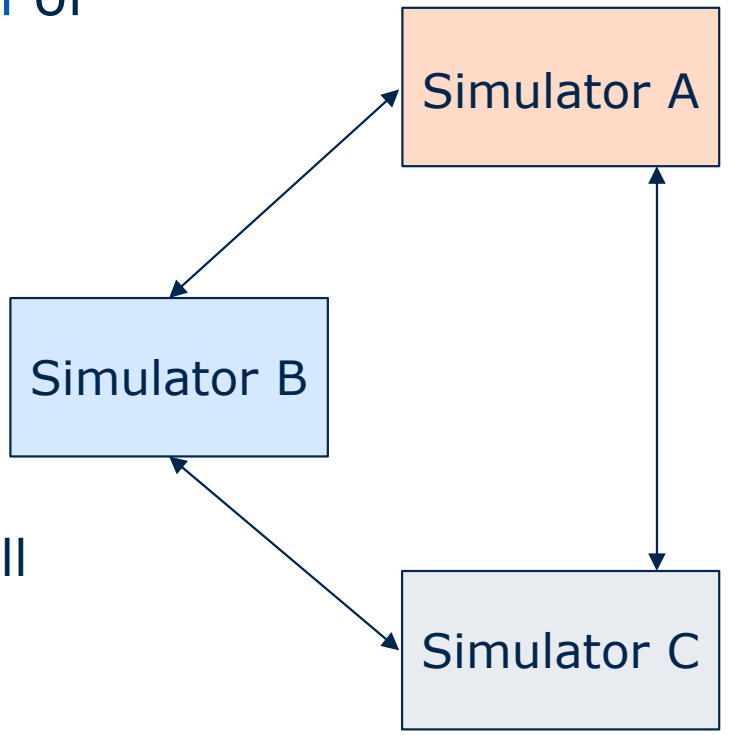
- A second line of defense can be added through the application of best security practices!
  - Logical separation of systems into functional groups with policies for monitoring and access execution control.
  - Defense-in-depth strategy: Information assets, power systems, and communications infrastructures are protected using layered defenses starting from securing the human elements, the physical perimeters, the communication networks, the applications and the data.
  - Real-time event monitoring, applications whitelisting and ICS-specific policy whitelisting for industrial protocols firewalls.
- Further cybersecurity enhancement is needed to improve utilities' response to the evolving cyberthreats including emerging supply chain cyberattacks!

IT/OT convergence-based cybersecurity enhancement

- Leveraging the IT/OT convergence allows the design of cyber-security solutions that use a larger set of parameters and lead to actions simultaneously spreadable across different IT/OT systems.
  - ✓ Improved cyberattack modeling and impact simulation through telecommunications – power system cosimulation.
  - ✓ Advanced system monitoring integrating complementary active and passive monitoring mechanisms as well as log analysis for IT and OT systems.
  - ✓ Cybersecurity data analytics employing sophisticated artificial intelligence and other data analysis methods that yield faster intrusion detection and more efficient attack mitigation methods!

IT/OT convergence-based cybersecurity enhancement: Cosimulation

- Process of tethering two or more simulators to provide an empirical operating depiction of an often complex multi-domain system
- Modeling and simulation conducted in a distributed manner
- Each individual simulator
  - models a critical component of the overall system
  - treated as a "black box"
  - Interfaced through well-defined input/output ports to enable exchange of relevant data at significant times



IT/OT convergence-based cybersecurity enhancement: Cosimulation

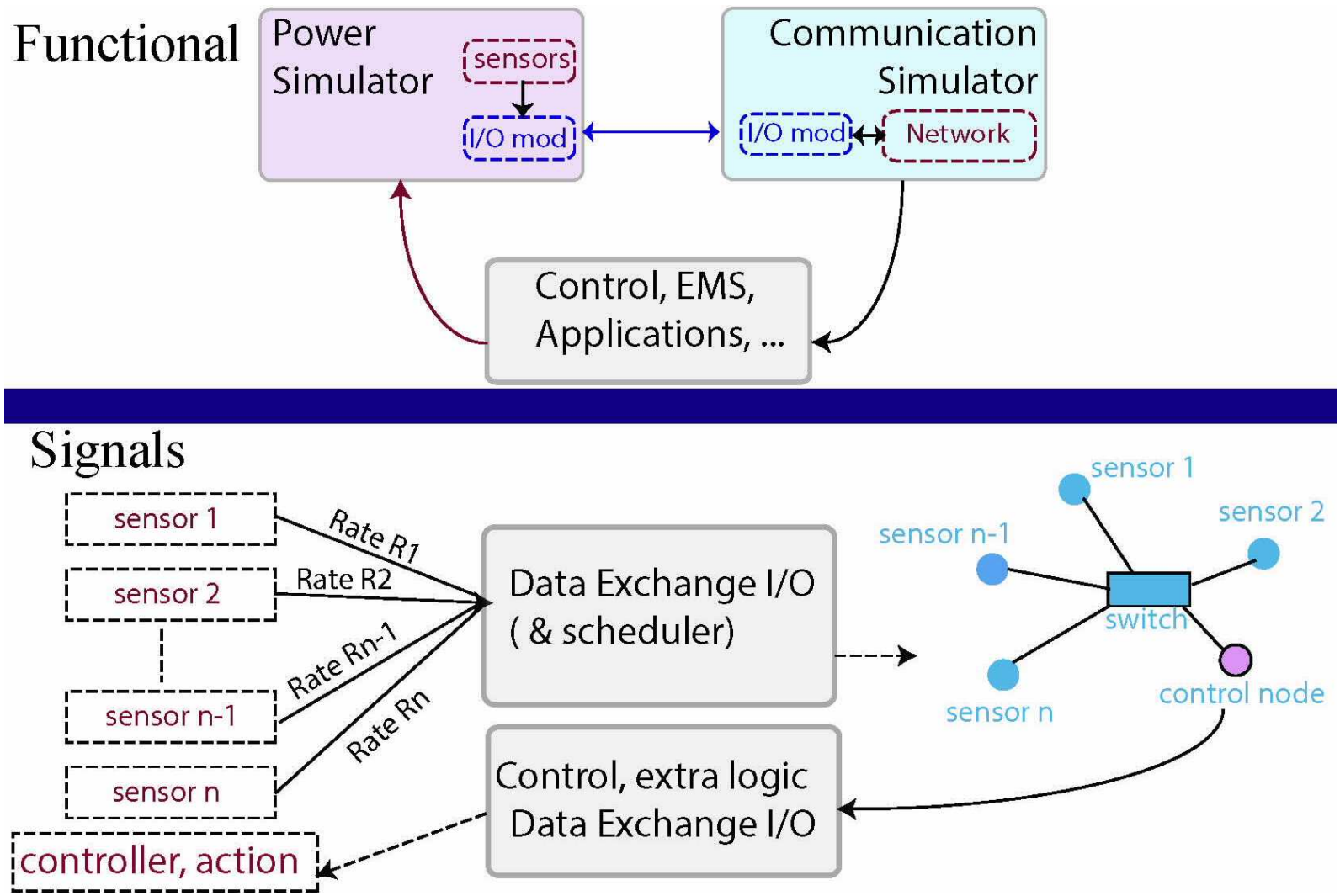
- Continuous-time
- Numerical solver
- Fixed or variable time step; user control

- Discrete-time
- Event-based
- Varying-time step; beyond user control

Types:

- Offline: cost-effective, accessible, more complex synchronization
- Real-time: hardware-in-the-loop, simpler synchronization, component simulators must be synchronized with “wall clock”

IT/OT convergence-based cybersecurity enhancement: Cosimulation architecture



IT/OT convergence-based cybersecurity enhancement: Real-time Cosimulation

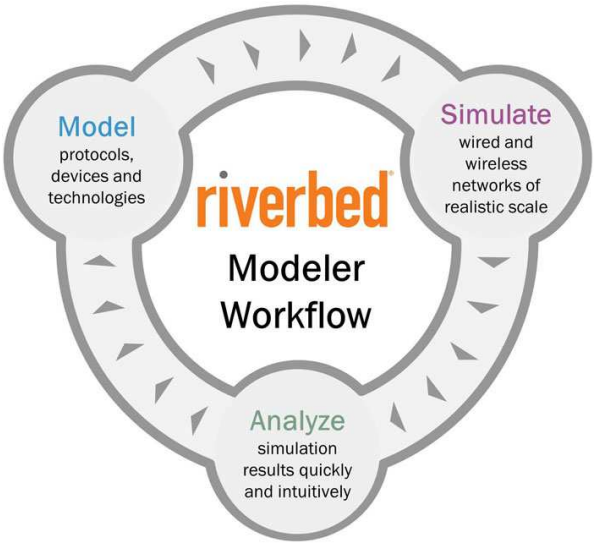
- All individual simulators must support real-time operation
- Synchronization must be organically managed with no additional modules
- Simulators must support bi-directional data exchange and processing of communication protocol to be studied

- Cosimulation components:
  - Power system simulator: HYPERSIM
  - Communication network simulator: Riverbed Modeler
  - Communication protocol: e.g., Ethernet IEC-61850 GOOSE

HYPERSIM

- real-time power simulator developed by Hydro-Québec
- commercially provided and supported by Opal-RT
- Combines high-performance dedicated hardware and suite of software tools
- HYPERSIM support of GOOSE via I/O hardware interfaces (Ethernet ports)
    - IEC-61850 GOOSE messaging used due to strict delay requirements useful for cyberattack impacts studies

Riverbed Modeler



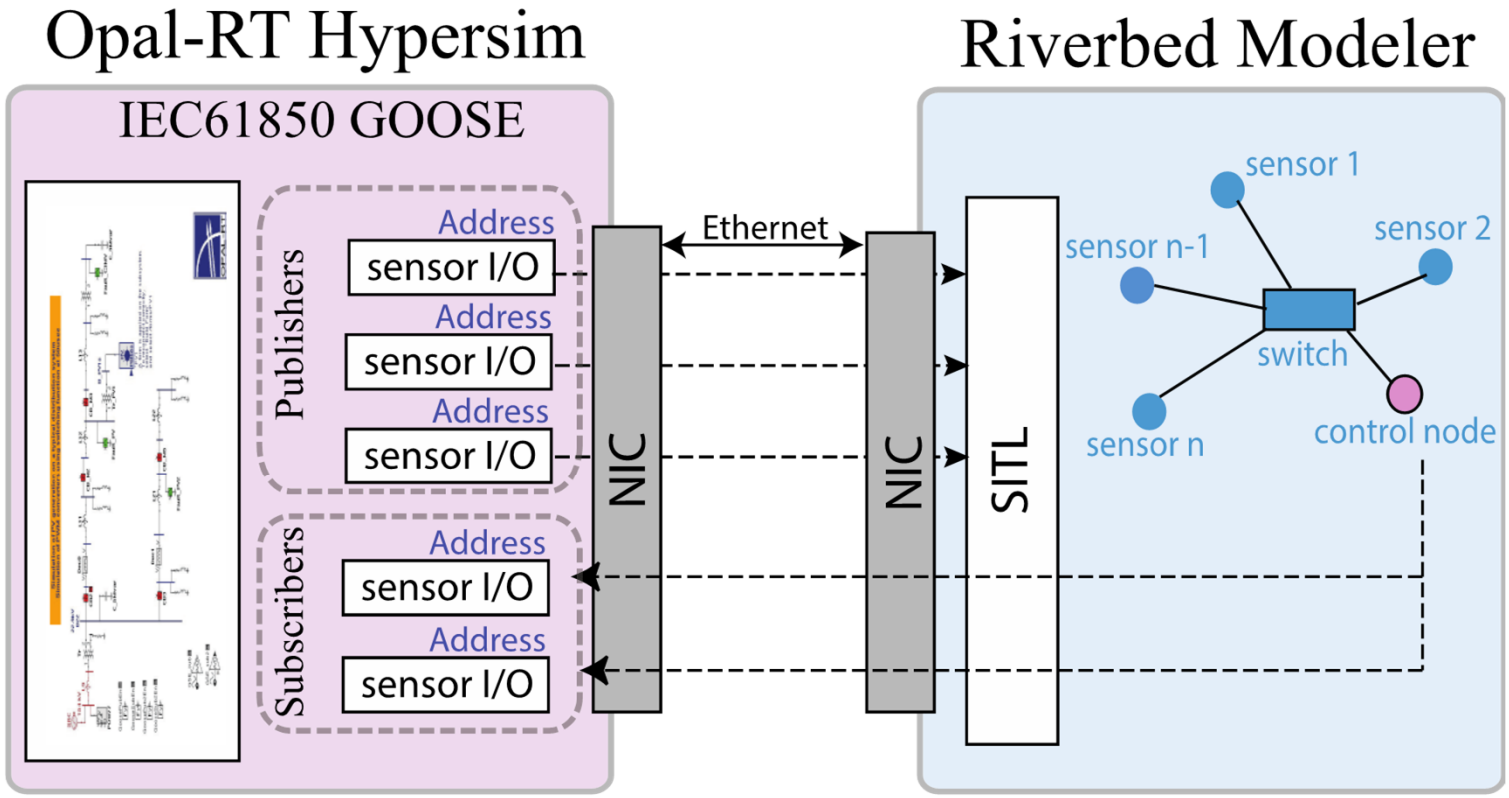
- Widely adopted communication network simulator with:
  - Real-time simulation support
  - System-In-The-Loop (SITL) module interfaces simulated communication network in Modeler with external (real) network
- SITL captures and routes real network traffic to simulated network:
  - Traffic packets can be translated into simulated packets for advanced flow processing based on packet data fields
  - Traffic packets can simply be routed in/out of Modeler as a pass-through traffic
- E.g., arrival rate of packets in variable rate protocols can be captured and processed across many points to correlate event.

GOOSE protocol support

- Both simulators support bi-directional flow of GOOSE frames between models in HYPERSIM and Modeler

- HYPERSIM:
  - supports generating GOOSE messages to communication measurements and control commands
  - Offers capability to interface communication protocols with outside hardware for HITL
- Modeler:
  - does not support IEC-61850 GOOSE in defined protocols library
  - Workaround: SITL behavior is modified to admit and route GOOSE frames in/out of simulated communication network

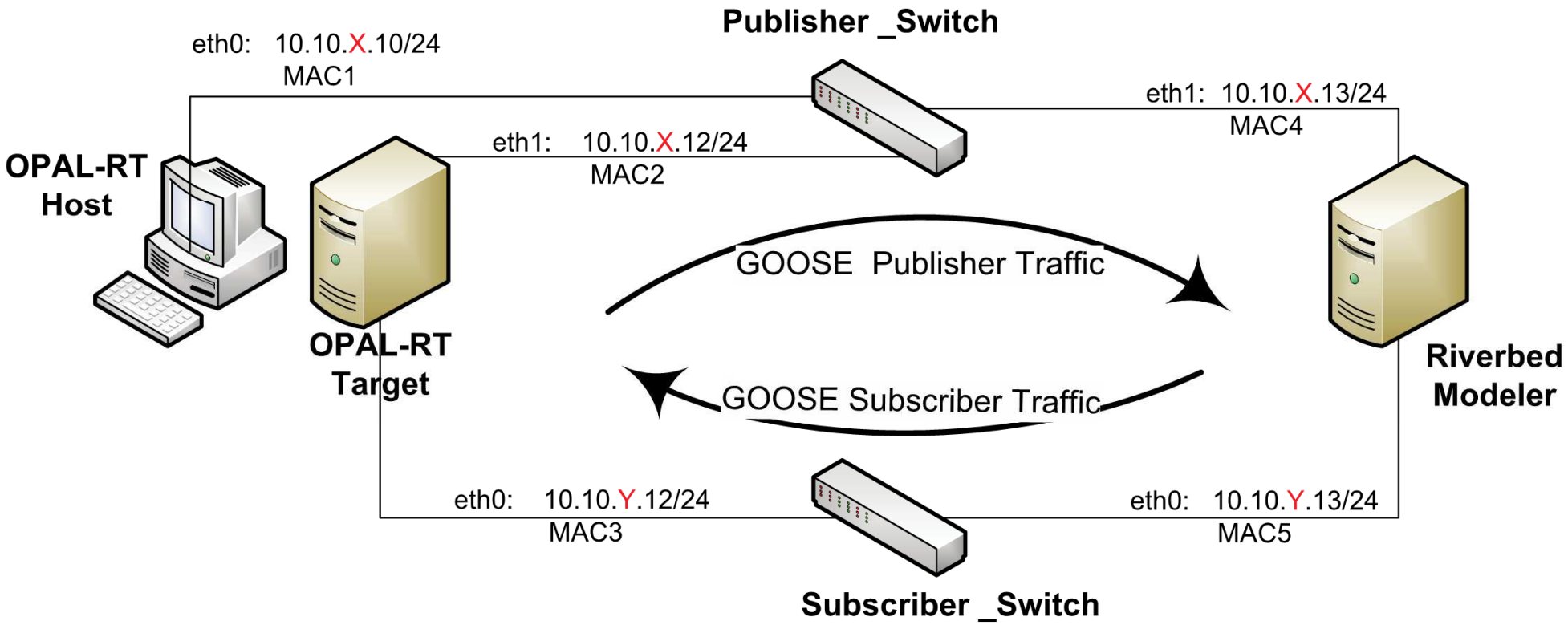
IT/OT convergence-based cybersecurity enhancement: Real-time Cosimulation



SITL System In The Loop

NIC Network Interface Card

IT/OT convergence-based cybersecurity enhancement: Real-time Cosimulation



IT/OT convergence-based cybersecurity enhancement: Data analytics

- Dynamic operating depiction
  - Comprehensive visibility and description of power grid environment
  - Used to develop novel enhancements: preventative maintenance, integration of DERs and cybersecurity
  - Completeness vs. complexity trade-off
    - Simplified dynamic operating depiction uses relevant subset of IT and OT data
- Enhanced attack detection and mitigation rely on the correlation and analysis of relevant IT and OT data sources

IT/OT convergence-based cybersecurity enhancement: Data analytics

OT Data Sources

- Grid behavioral data: Inputs/outputs of the power system functions and automation processes, and the resulting grid behavior data (i.e. sensor measurements, actuators actions and control schemes)
- Monitoring data: Passive/active monitoring and the logs
- Domain and status data: Outputs of grid estimators, statuses of circuit breakers and switches, grid statistics as well as the indicators of power quality, grid stability and system reliability
- Metadata: Information describing the grid connectivity and its supporting OIT infrastructure, operational constraints, control functions specifics, normalizing factors, calibration constants, …

IT/OT convergence-based cybersecurity enhancement: Data analytics

IT Data Sources

- Communication networks data: Network architecture, topology, protocols, routing and switching, interconnected devices and device configurations
- Utility information and applications data: IT-based applications running in the enterprise/business network, operators access information, customers and market information, geographic information systems, enterprise resources planning, …
- Monitoring data: Passive/active monitoring and the logs

…

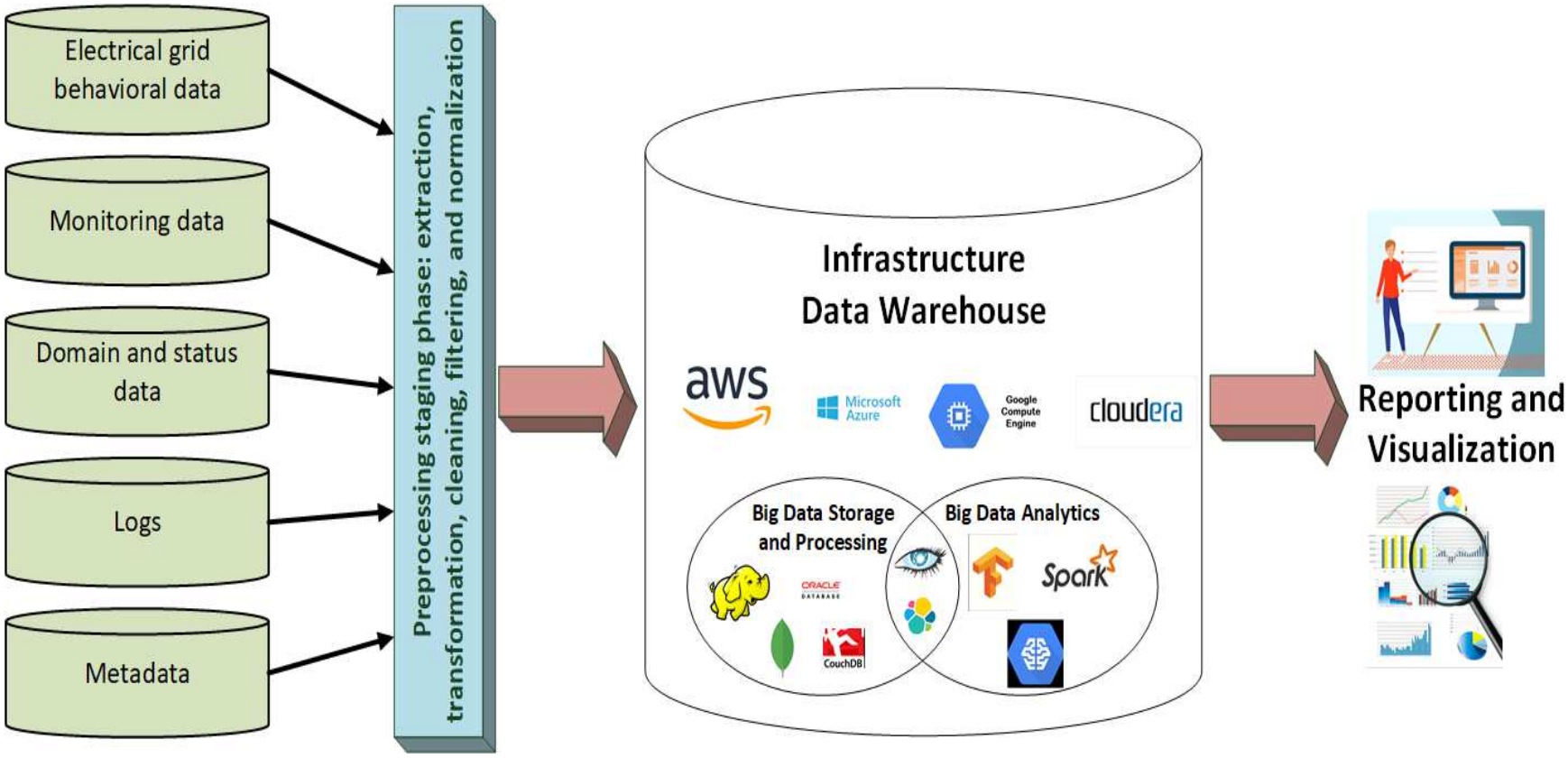
IT/OT convergence-based cybersecurity enhancement: Data analytics

Other Data Sources

- physical security systems: access card readers, surveillance cameras
- maintenance operations schedules and descriptions
- service providers and equipment vendors
- weather information
- news media and social media
- regulations and policies.

IT/OT convergence-based cybersecurity enhancement: Data analytics

- Generic data analytics platform architecture:



IT/OT convergence-based cybersecurity enhancement: Data analytics

- Descriptive
  - Aims to summarize *what has happened*
  - Communicates event effectively to stakeholders or other machines
  - Supply chain attack impact assessment
  - post-mortem forensic analysis
  - communicating analytics results to human operators, enhancing the corresponding HMI

IT/OT convergence-based cybersecurity enhancement: Data analytics

- Diagnostic
  - Aims to answer *why this has happened*
  - Provides stakeholders with information for operational improvements in the supply chain

IT/OT convergence-based cybersecurity enhancement: Data analytics

- Predictive
  - Models forecast *what could happen*
  - Linear regression, support vector machines and neural networks, Bayesian networks and clustering methods
  - Existing approaches forecast intermittent generation level of renewable sources, energy demand within a distribution region and consumer preferences
  - Effective for anomaly detection to identify existence of supply chain attacks

IT/OT convergence-based cybersecurity enhancement: Data analytics

- Prescriptive
  - Recommendations to address *what should be done*
  - Mathematical models (often based on physics), computational tools and machine learning paradigms
  - Real-time: Advising on reactive mitigation measures against supply chain attacks
  - Long-run: Strategize prevention of supply chain attacks and enhancement of incident response
  - Provides a human grid operator with prioritized options by quantifying and assessing multiple futures assuming different mitigation approaches are applied

IT/OT convergence-based cybersecurity enhancement: Data analytics

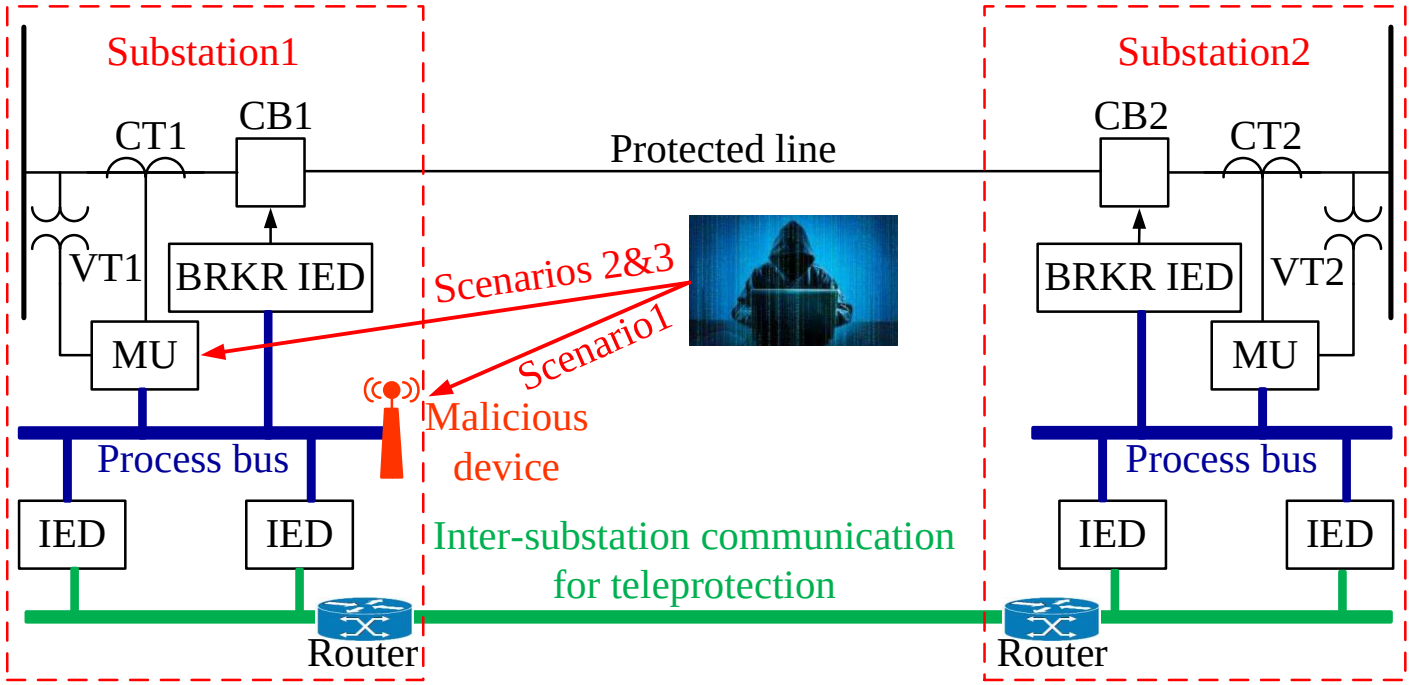
- Generative
  - training on data to characterize its statistics and generate new data sets exhibiting some variation from the training data
  - Provides answers to *what other scenarios are possible*
  - Coupled with prescriptive data analytics, could produce potentially unknown supply chain attack scenarios and predict new vulnerabilities in the supply network

Use cases

- Different cyberattack scenarios can be considered such as: False data injection (FDI), Denial-of-service (DoS), Man-in-the-Middle (MITM), replay and delay attacks, blended attacks, and supply chain attacks.
- The IT/OT convergence-based approach for cybersecurity enhancement can be applied to different environments across the electricity generation and transmission systems, such as:
  - Generation plants
  - Power substations
  - Wide area monitoring, protection and control systems
  - Control centers
  - Distribution automation

Use case 1: Compromise of IEC 61850 substation transmission protective relays

Combined MITM, FDI and replay cyberattacks against merging unit:



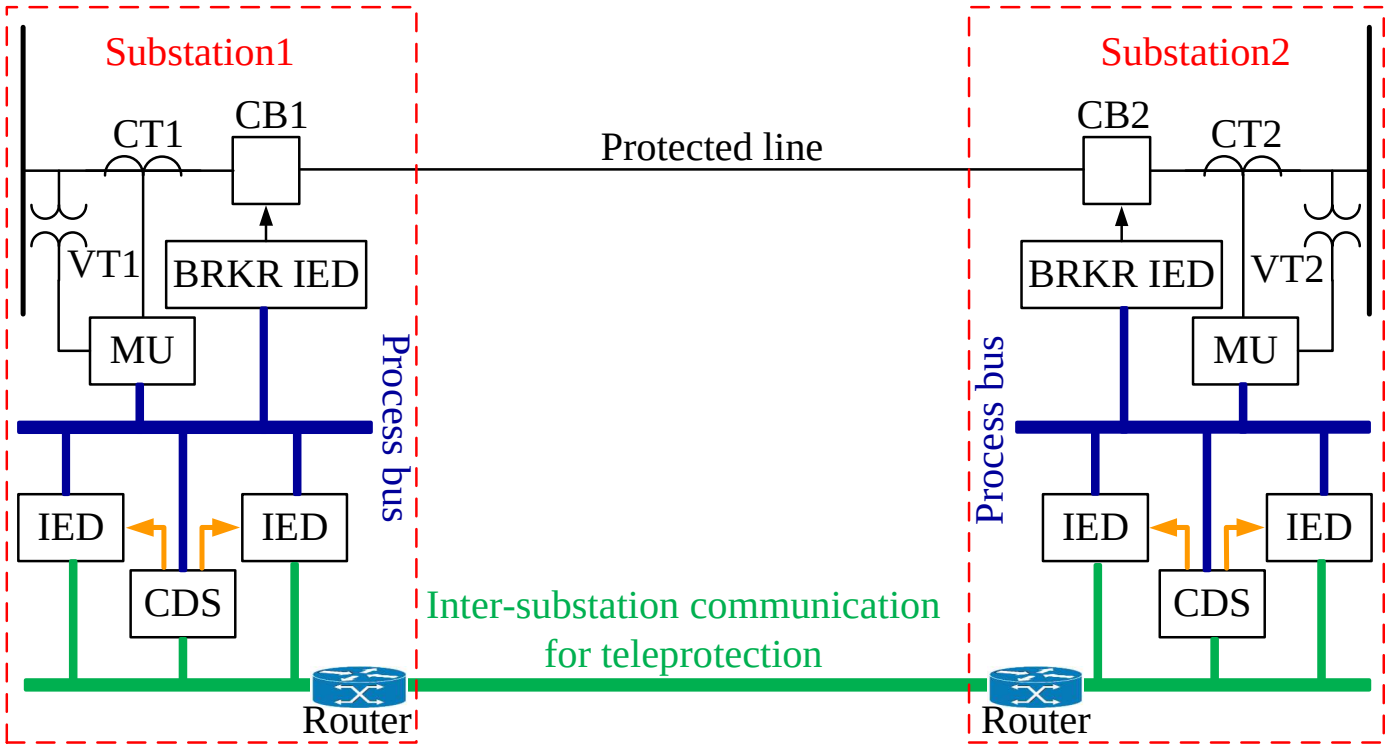
MU: Merging Unit
CB: Circuit Breaker

BRKR: Breaker
VT: Voltage Transformer

IED: Intelligent Electronic Device
CT: Current Transformer

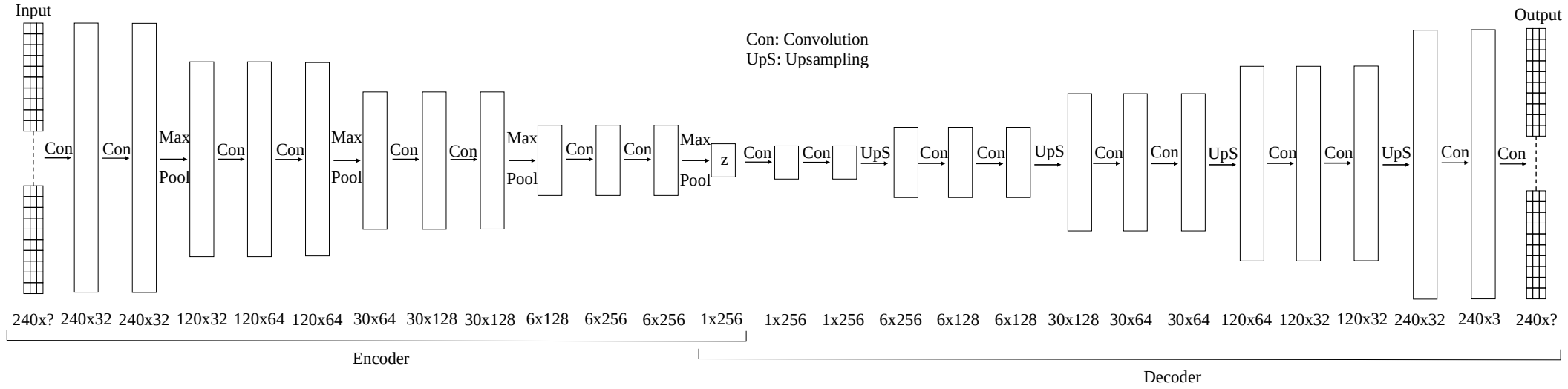
Use case 1: Compromise of IEC 61850 substation transmission protective relays

Combined MITM, FDI and replay cyberattacks against merging unit:



Use case 1: Compromise of IEC 61850 substation transmission protective relays

CDS: Deep Learning Based Autoencoder

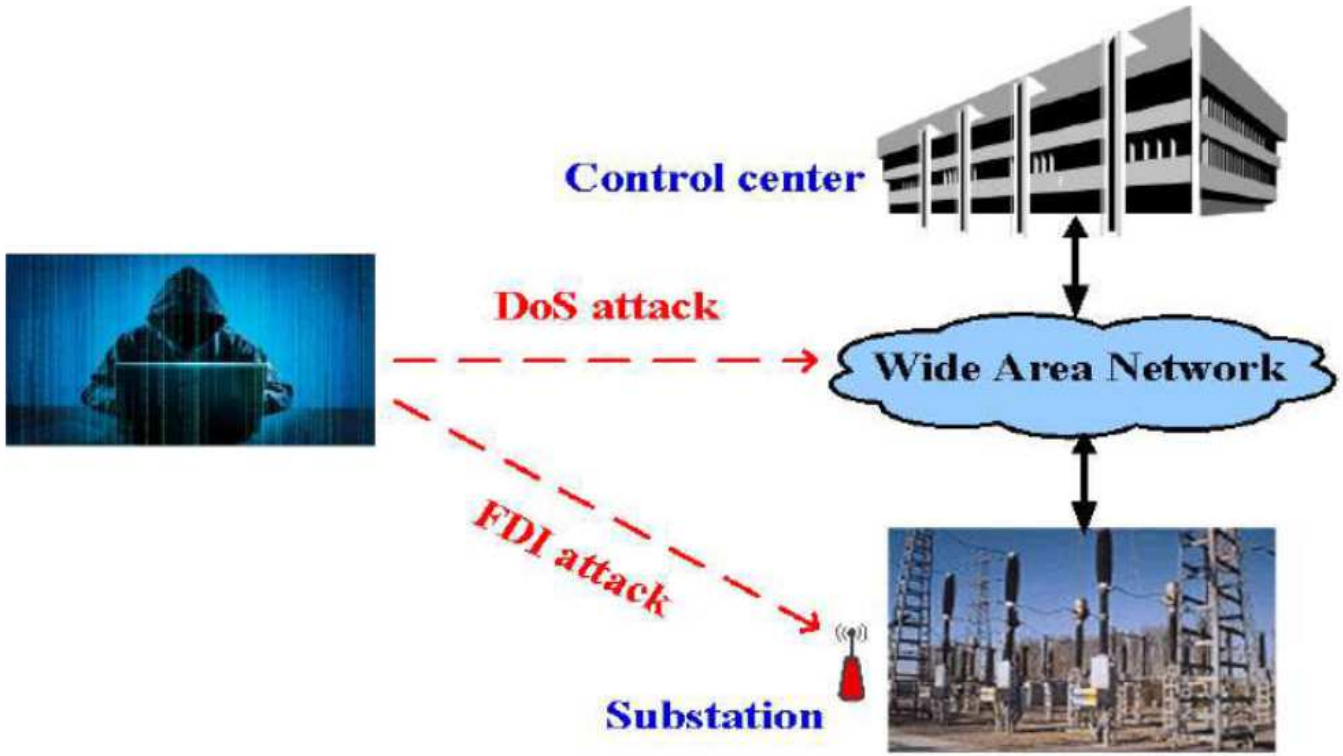


Use case 1: Compromise of IEC 61850 substation transmission protective relays

- Appropriate mitigation actions for this use case:
  - Cyberattack detection mode (generates alarm)
    - Anomaly detection of combined MITM and random FDI attack
    - Identification of tampering of instrument transformer tap settings
    - Detection of supply chain replay attack
  - Cyberattack detection and mitigation mode
    - Alarm from detection
    - Sends commands to IEDs to block anomalous measurements to avoid false transmission line tripping

Use case 2: Compromise of an IEC 61850 substation operations by third-party employees and telecommunication equipment suppliers

Combined FDI and DoS cyberattack against a telecontrol function:



Use case 2: Compromise of an IEC 61850 substation operations by third-party employees and telecommunication equipment suppliers

- Detection: Active monitoring through IT/OT network management (IEC 62351-7) and IEC 61850 specific mechanisms to poll device data objects and logical nodes providing relevant information.
- Appropriate mitigation actions for this use case:
  - Detecting and blocking rogue wireless devices;
  - Isolate infected networking devices and paths and restore secure communications;
  - Automated mitigation mechanisms in OT devices that can be activated upon GOOSE command rate disruptions;
  - Authentication and handshake procedures for more secure relay – merging unit communications;
  - Enhance the control and data processing capabilities in devices close to the switchgear, e.g. improving logical node implementation in merging units with more resilient interlocking and switching rules to block the execution of malicious commands.

Recommendations

- Leveraging the IT/OT convergence for the enhancement of cybersecurity requires power utilities to:
  - Implement collaborative solutions involving multidisciplinary teams from IT and OT groups.
  - Provide adequate training for their staff.
  - Exploit the potential of artificial intelligence and data analytics to design novel solutions using data generated across the power grid.
- Improving collaborations between power utilities and OT equipment manufacturers:
  - Enhanced cybersecurity-by-design integration and accelerated standards implementation;
  - Implementing “smart” and automated defenses in OT devices;
  - Better control over the supply chain vulnerabilities and risks!

Recommendations

- Investing further in cybersecurity research and development through industrial-academic collaborations:
  - Design novel scientific approaches to study and solve complex power grid problems
  - Training of highly qualified personnel in multidisciplinary fields
  - Develop appropriate tools for the application and assessment of smart grid solutions
- Securing critical infrastructures can be better achieved through:
  - Development of further security standards and regulations
  - Sharing security information among critical infrastructures owners/operators and national security agencies
  - Raising awareness of the general public!

Thank you!