NORCICS

SFI Norwegian Centre for Cybersecurity in Critical Sectors

Unified IT&OT Modeling for Cybersecurity Analysis of Cyber-Physical Systems

Aida Akbarzadeh and Sokratis Katsikas

Critical Infrastructure Security and Resilience (CISaR) group, IIK NTNU

NTNU | Norwegian University of Science and Technology

Motivation (1)

- IT-OT integration (**not** convergence):
  - Cyber–physical, physical–cyber, cyber–cyber, and physical–physical interactions within a CPS --> different types of dependency exist in CPSs.
  - Local measurements on a power system sample the voltage magnitudes **(physical–cyber interaction)**. Next, by means of communication networks, this data will be transferred to the control center **(cyber–cyber interaction)**. In the control system, to keep the system in the desired state, pertinent computation will be conducted based on the received data, and appropriate control commands will be sent to the related actuators. Then, these actuators will take proper action based on the received control commands **(cyber–physical interaction)**. Finally, the physical states of the power system will gradually reach the desired point as a consequence of the changes that have been made by actuators **(physical–physical interaction)**.

Motivation (2)

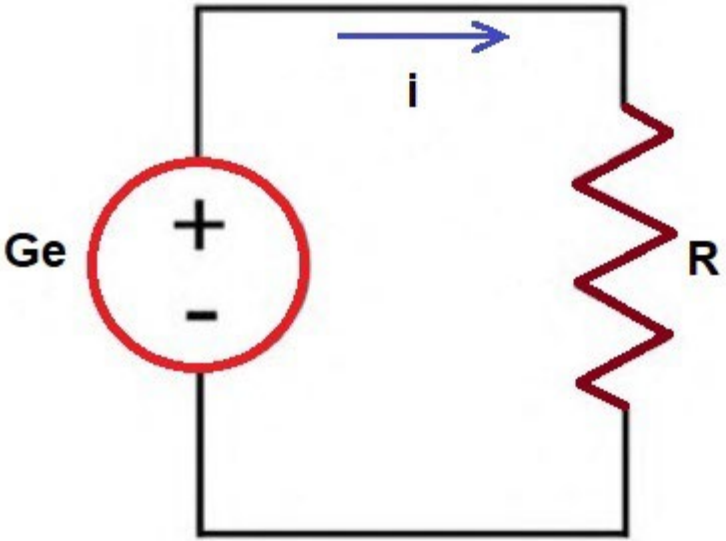
- IT-OT integration (**not** convergence):
  - Focus has mainly been on information security, protecting access, and ensuring secure delivery of packets, rather than on securing process operations.
  - Analysis of the cyber components, the physical components, and particularly of the interactions between the system components is needed.
  - Need for collaboration between communities from different backgrounds, including control theory, power systems, safety engineering and cyber security.
- Need to develop a generic, yet easy to understand model to represent physical and logical facets as well as the interactions within the system components.

Background

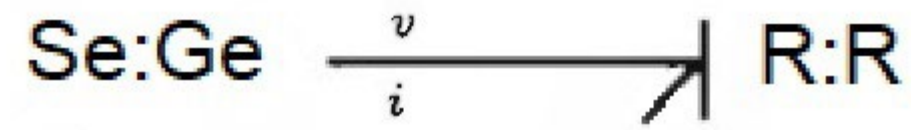
- A Bond Graph (BG) is a graphical representation of a physical dynamic system in the form of a directed graph. A BG is composed of **bonds** (edges) and **elements** (nodes).
- BG modeling is based on the power transfer principle between the different components of a system, since in each energy domain, the amount of power transferred is equal to the product of two physical quantities, i.e., Power = Effort × Flow.
- Therefore, the physical interaction among components of a system is done by the allocation of Effort (e) and Flow (f) variables on them.

Domain name	Energy	Electronic	Hydraulic	Thermodynamic	Mechanics
First variable	Effort (e)	Voltage (V)	Total pressure (P)	Temperature (T)	Force (F)
Second variable	Flow (f)	Current (I)	Volume flow (Q)	Entropy flow ($S\cdot$)	Velocity (V)

An example



(a)

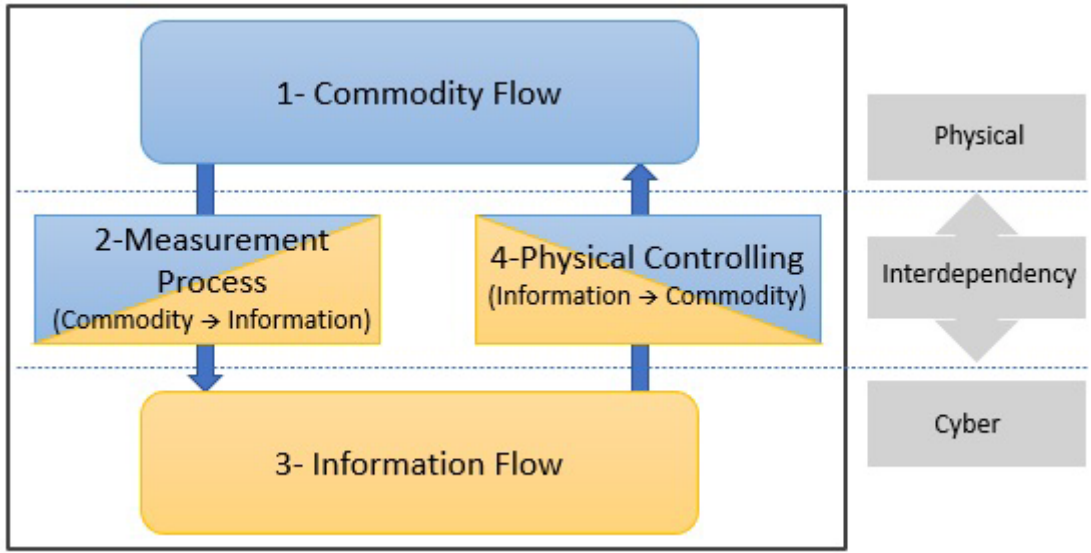


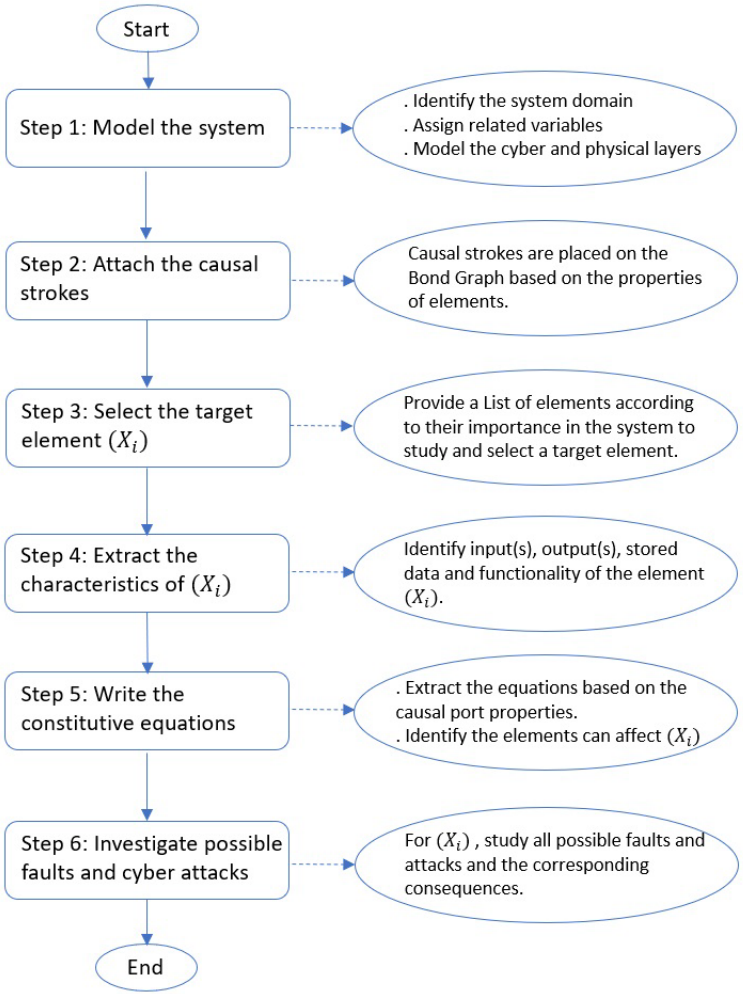
(b)

Modeling interactions in CPSs

NORCICS

- The purpose of adding the cyber layer (ICT) to traditional systems is to improve system control and monitoring to ensure that the primary objective of the system, which is delivering a service or commodity to the consumers (end-users), is properly met.
- Therefore, we need two types of flow to model CPSs, namely **commodity flow** and **information flow**.

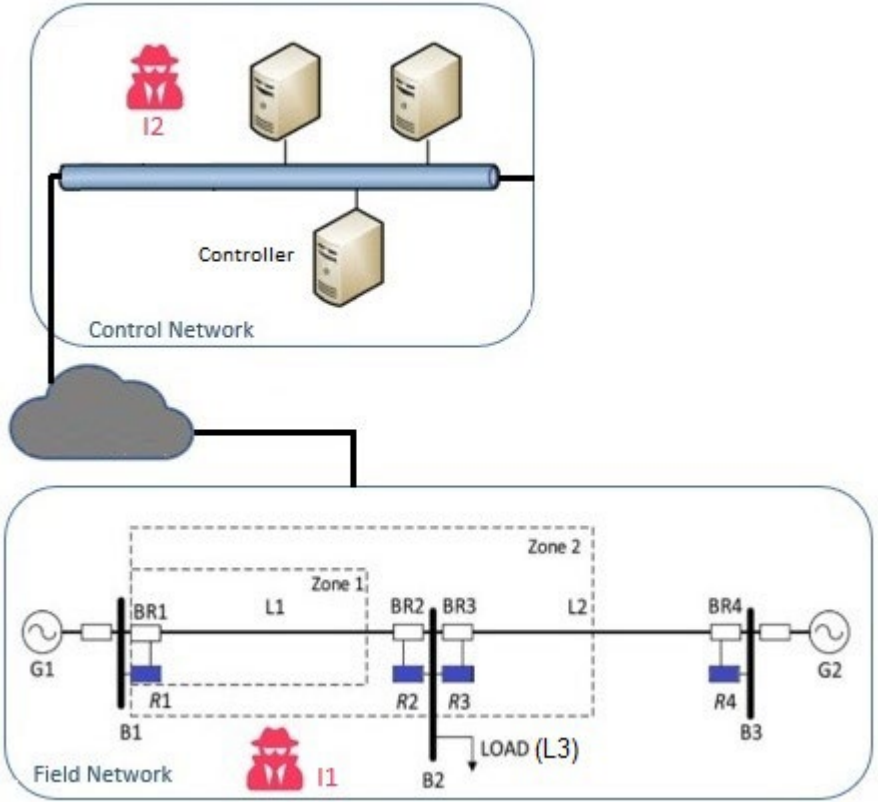




Causal strokes represent the direction of the effort variable

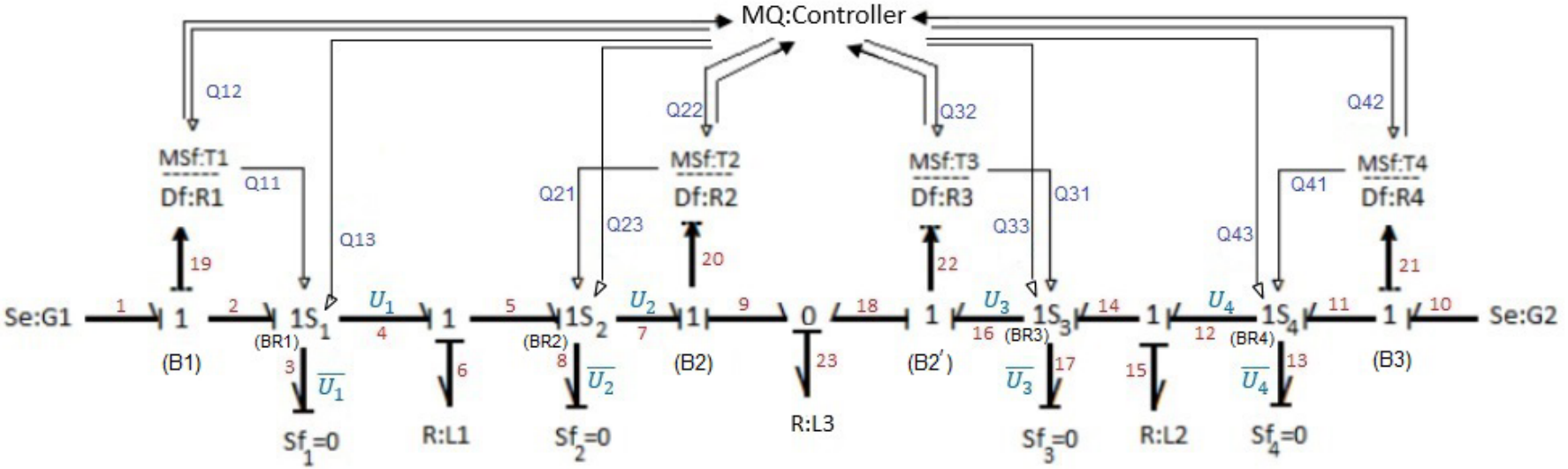
Some elements have stored data like a set point or threshold values to compare with the input; in this case, the stored data should also be considered

Case study



- Two network zones: a field network, and a control network to control the system.
- The field network illustrated is a three-bus two-line transmission system that is a modified version of the IEEE nine-bus three-generator system.
- G1 and G2 are power generators, L1 and L2 are transmission lines, BR1 through BR4 are circuit breakers and R1 through R4 are relays.
- Each relay includes integrated phasor measurement unit (PMU) functionality and is able to trip and open the related breaker when a fault occurs on a transmission line.

The corresponding BG



Example: R1

NORCICS

- R1 is composed of two elements of the BG, a **sensor** to measure the current and an **actuator** to trigger the corresponding circuit breakers
- Df:R1 denotes the flow detector (sensor), and MSf:T1 refers to the modulated source of flow (actuator).
- The communication between R1 and its connected elements (circuit breaker and controller) is not protected as there is no protected channel.
- Therefore, adversaries may inject or replay commands into the relay to change the threshold T1 (i.e., stored data), they may alter or replay sensor measurements (Df) to cause upstream algorithms to take incorrect control actions (controller MQ or R1), or they may alter or replay control commands (from MSf to the breaker) to directly cause incorrect system actions.

Identified attack scenarios against R1

NORCICS

- **Trip command injection attacks**: An attacker sends an unexpected relay trip command to relay R1 to open associated breakers. Here, we assume that the attacker aims to trip the breaker BR1 at the ends of transmission line L1 to force L2 to carry more power flow and put the system under stress.
- **Data Injection Attack (or 1LG fault):** In this case, an attacker imitates a valid fault, such as a single line to ground (1LG) fault. This attack leads to loss of view and may cause an operator to take invalid actions.
- **Relay Disabled Attack:** An attacker changes the settings of relay R1 to disable its operation. As a result, R1 will not trip breakers even in the presence of the pertaining stimulus.
- **Relay setting change Attack:** To disturb the functionality of R1, an attacker increases the stored value of T1 in relay R1. Then the transmission line L1 experiences over current, which can damage the system and cause safety issues. Likewise, decreasing the threshold can cause degradation of service and affect the system performance.

Conclusions

NORCICS

- Modeling the cyber layer along with the physical layer can provide a holistic view of a CPS and allow to evaluate how adversaries might attack the physical part of the system through attacking the cyber part.
- The proposed method allows one to follow the sequence of interactions based on the topological parts of the model and utilize process physics to investigate dependencies and relations between the components of a CPS to extract potential fault points, attack surfaces, and the consequences of attacks.

NORCICS

SFI Norwegian Centre for Cybersecurity in Critical Sectors

Thank you!

sokratis.katsikas@ntnu.no

NTNU | Norwegian University of Science and Technology