Technical University of Denmark

Engineering Systems
Department of Management Engineering

Identification of safety and security cascading risks in Cyber-Physical Systems (CPS)

Nelson H. Carreras Guzman, PhD project

Relevance

Cyber-physical systems (CPS) are system of systems which tightly couple computational and physical processes to optimize physical performance. While taking other popular names depending on the specific area of application, e.g. Industry 4.0 and Internet of Things, the term CPS refers to the general and fundamental issue of merging the engineering traditions of the cyber and physical worlds. As CPS are being implemented progressively in our common daily tasks, a promising potential exists for enhanced efficiency and safety in systems such as transportation networks, power grids, and healthcare.

However, new vulnerabilities have risen as a product of the strong and real-time interdependencies between the cyber and physical layers of the systems. Failures can now propagate and evolve, sometimes in unexpected ways, exploiting the vulnerable connections and *cascading* throughout the whole system. These sources of potential failures may arise from accidents or intentional attacks, hence a comprehensive risk identification should consider both safety and security risks in an integrated way.

In this project, an approach will be developed to identify cascading risks in CPS and suggest preventive and mitigation measures. Furthermore, a validation of the approach will be conducted in collaboration with companies and consultant experts. The project will be carried out in close collaboration between the Technical University of Denmark (DTU) and the Norwegian University of Science and Technology (NTNU).

Research questions (RQ)

- RQ 1: How to classify cascading failures considering both safety and security risks in CPS?
- RQ 2: What mode of representing CPS is more appropriate in order to identify cascading risks?
- RQ 3: Which methodology is recommended to identify cascading risks in CPS?
- RQ 4: How to evaluate safety and security barriers to prevent or mitigate cascading risks in CPS?

Conceptual model/theory

- Safety and Security Risk Assessment
- Cyber-Physical Systems Modelling

Method

Exploratory sequential mixed design, a pragmatic approach:

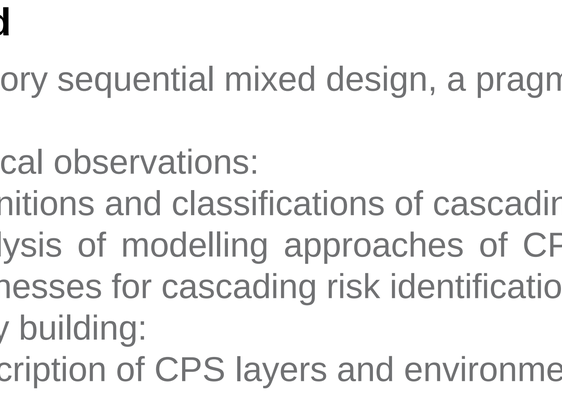
o Empirical observations:
- Definitions and classifications of cascading failures in the literature.
- Analysis of modelling approaches of CPS in the literature, focusing on potential opportunities and weaknesses for cascading risk identification.

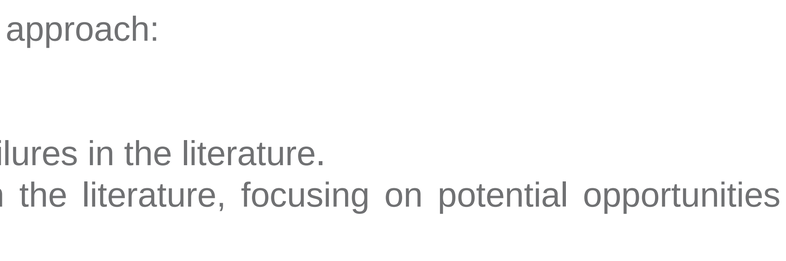
o Theory building:
- Description of CPS layers and environment representation and modelling.
- Develop approach for integrating safety and security techniques for cascading risk identification.

o Theory testing:
- Discussion in conferences and workshops with risk experts and research partners.
- Conducting a pilot study with industrial partner to evaluate method and validate results.

Expected results

- A safety and security framework to classify and analyse cascading risks
- Consistent set of CPS descriptions for trustworthy identification of cascading risks
- A cascading risk identification approach for CPS
- Validated integrative approach with regard to predictive power





Contact:
Nelson H. Carreras Guzman, PhD student
Produktionstorvet, Building 424
DK-2800 Kgs. Lyngby
nelca@dtu.dk
www.man.dtu.dk

Supervisor/co-supervisor:
Igor Kozin, Senior Researcher DTU
Mary Ann Lundteigen, Professor NTNU
Robert Taylor, Guest Researcher DTU

Start and completion date:
1 November 2017 – 31 October 2020

Collaborating partners:

NTNU

Funded by:

DTU

Scan to learn more about the project