11TH INTERNATIONAL CONFERENCE ON CRITICAL INFORMATION INFRASTRUCTURES SECURITY

10-12 October 2016
UIC HQ Paris

CRITIS 2016

A Methodology for Monitoring and Control Network Design

Istvan Kiss, Bela Genge

"Petru Maior" University of Tirgu Mures

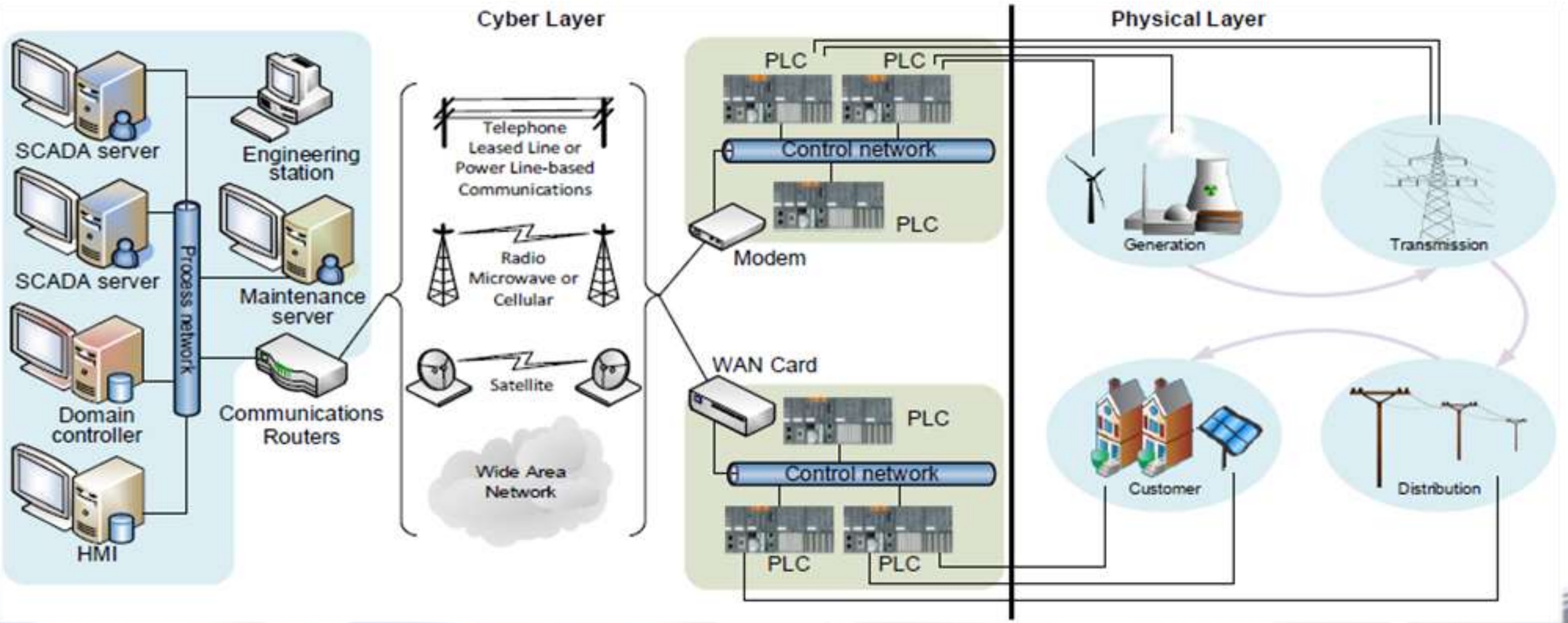
UNIVERSITATEA
Petru Maior
TÂRGU-MUREȘ

Content

- Introduction
- Risk assessment procedure
- Optimal security-aware network design
- Experimental assessment
- Conclusions

Introduction – ICS – the core of CI

- Architecture includes the cyber and physical domains.
  - Physical layer: sensors, actuators.
  - Cyber layer: Transmitters, PLC, SCADA servers, HMI, communication infrastructure.

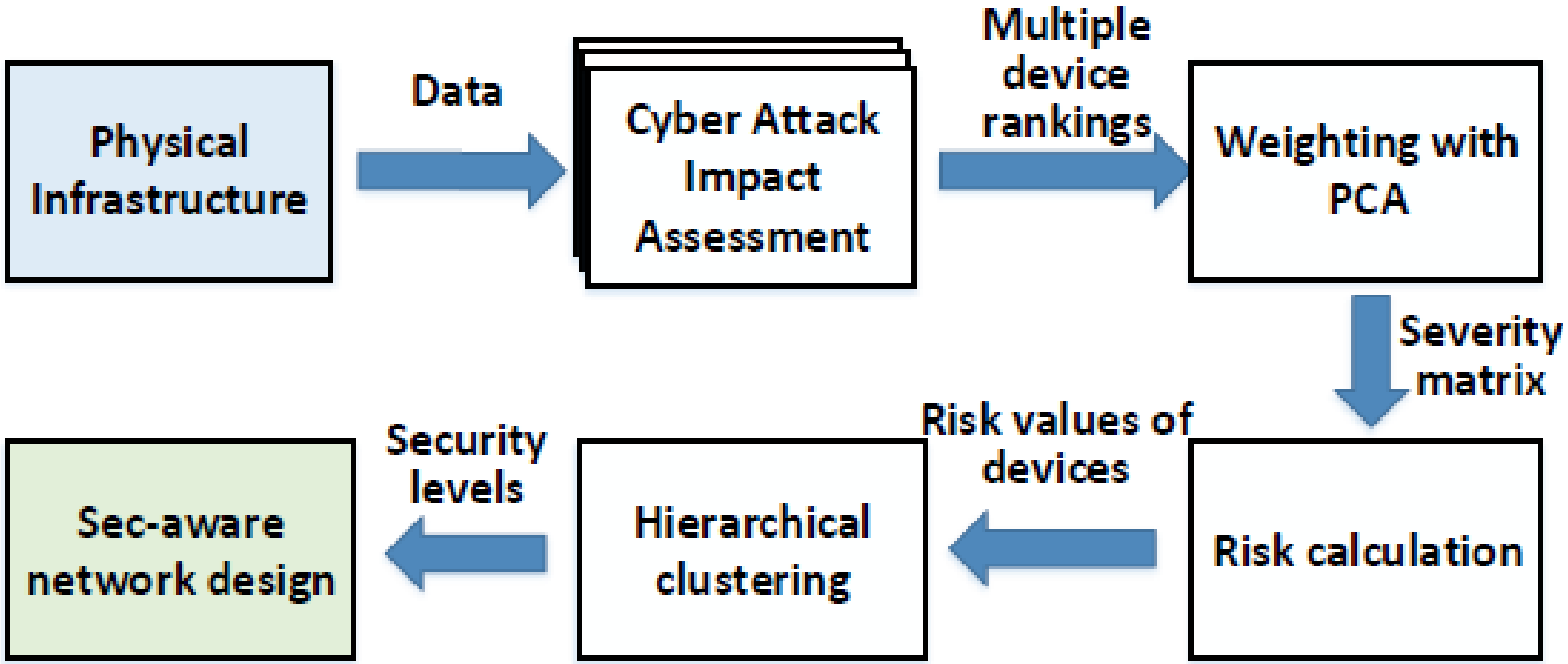


Overview of the proposed technique

- Measure the impacts of various cyber threats on the physical equipment.
- Summarize the impact values and determine a risk value for each cyber device of the ICS.
- Group the devices in a predefined number of security groups.
- Make the communication links to the concentrator nodes (switch, router, firewall, IDS) as desired by the security requirements.

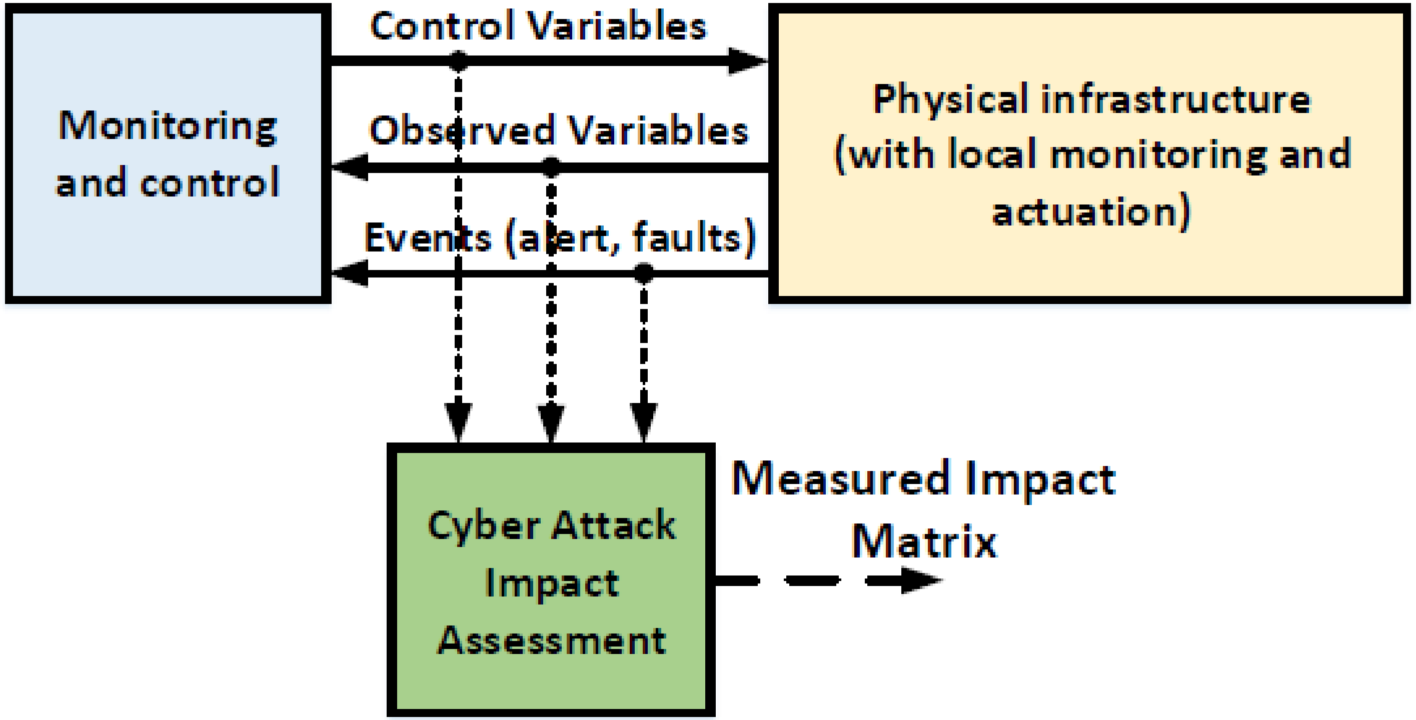
Cyber risk assessment

- How to measure the risk values associated with physical process/equipment?



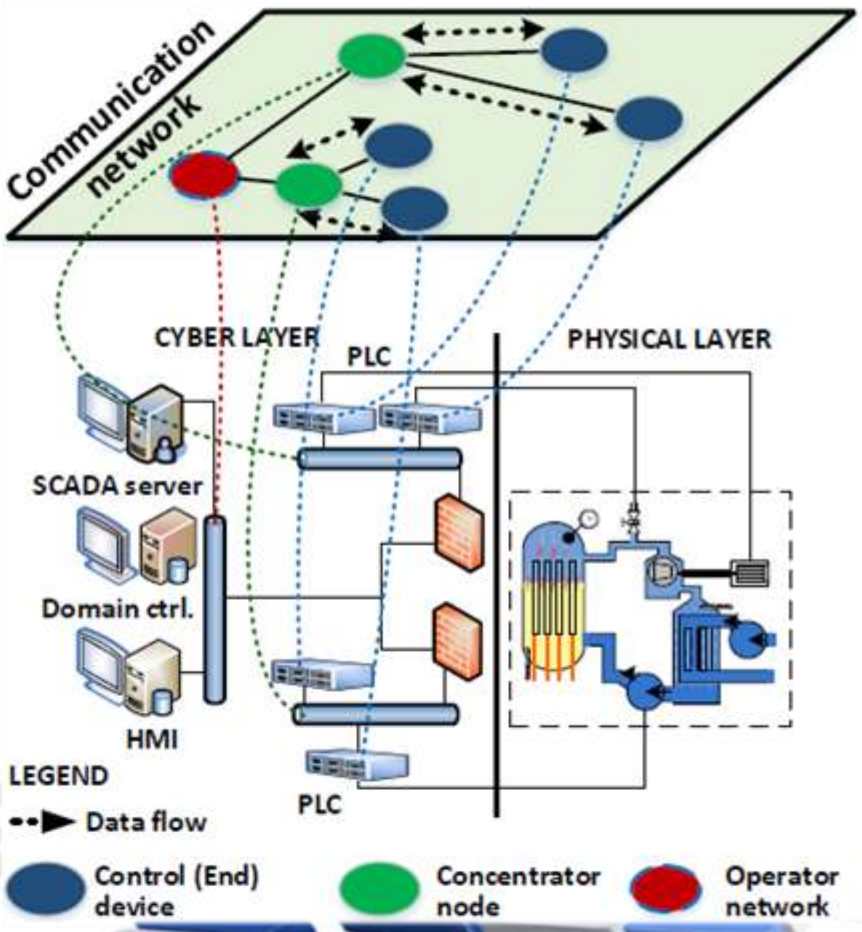
Cyber attack impact assessment

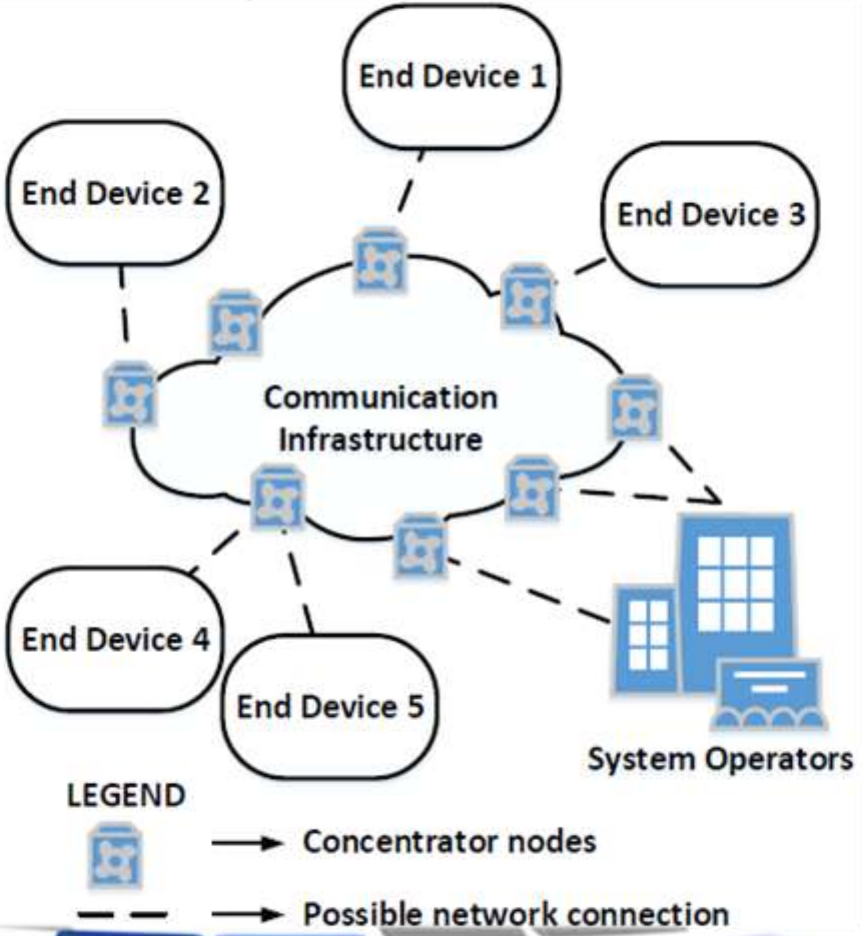
- How to measure the effects of cyber incidents on physical process/equipment?



Optimal security-aware network design

- Minimize End device - Concentrator node (switch, router, firewall + IDS) distances and maintain performance & **security constraints.**





Optimal, security-aware network design

- ILP problem
- Some mathematics
  - (10) – connection constraint
  - (11) – security constraint
  - (12) – link capacity constraint

Cost function

$$min\left(\sum_{\imath\in\mathcal{C}}\sum_{\jmath\in\mathcal{D}}[(x_\imath^{\mathcal{C}}-x_\jmath^{\mathcal{D}})^2+(y_\imath^{\mathcal{C}}-y_\jmath^{\mathcal{D}})^2]\cdot\nu_{\imath\jmath}\right), \tag{9}$$

With the following constraints:

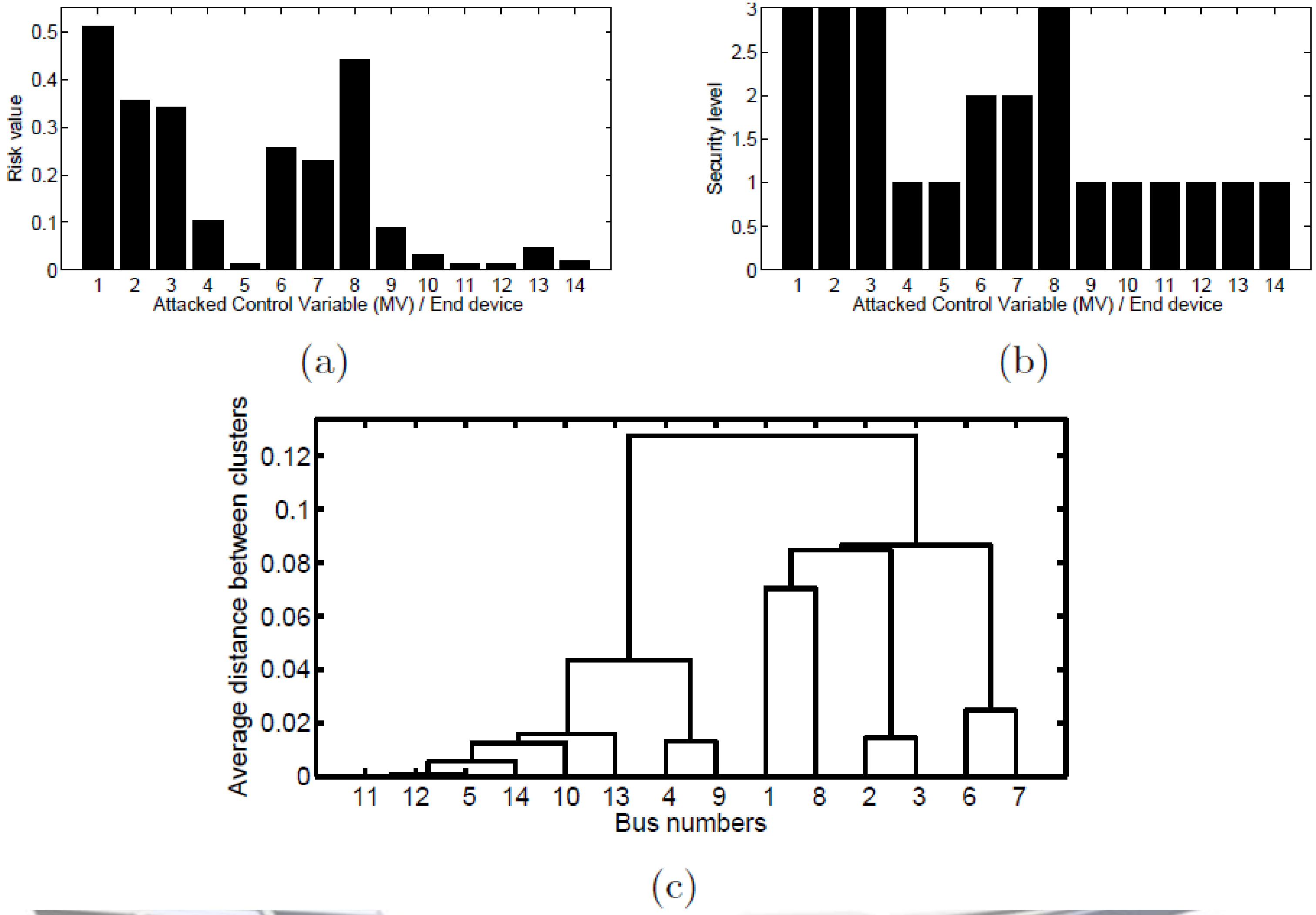
$$\sum_{\imath\in\mathcal{C}}\nu_{\imath\jmath}=1,\forall\jmath\in\mathcal{D}, \tag{10}$$

$$s^{\mathcal{D}}_{\jmath\kappa}\cdot\nu_{\imath\jmath}\leq s^{\mathcal{C}}_{\imath\kappa},\forall\imath\in\mathcal{C},\jmath\in\mathcal{D},\kappa\in\mathcal{S}, \tag{11}$$

$$\sum_{\jmath\in\mathcal{D}}\xi^{\mathcal{D}}_{\jmath}\cdot\nu_{\imath\jmath}\leq\zeta^{\mathcal{C}}_{\imath},\forall\imath\in\mathcal{C}, \tag{12}$$

Experimental assessment

- IEEE 14-bus electricity grid
  - (a) Pure risk values;
  - (b) Risk values enforced in 3 groups with different security levels;
  - (c) Risk assessment dendrogram.



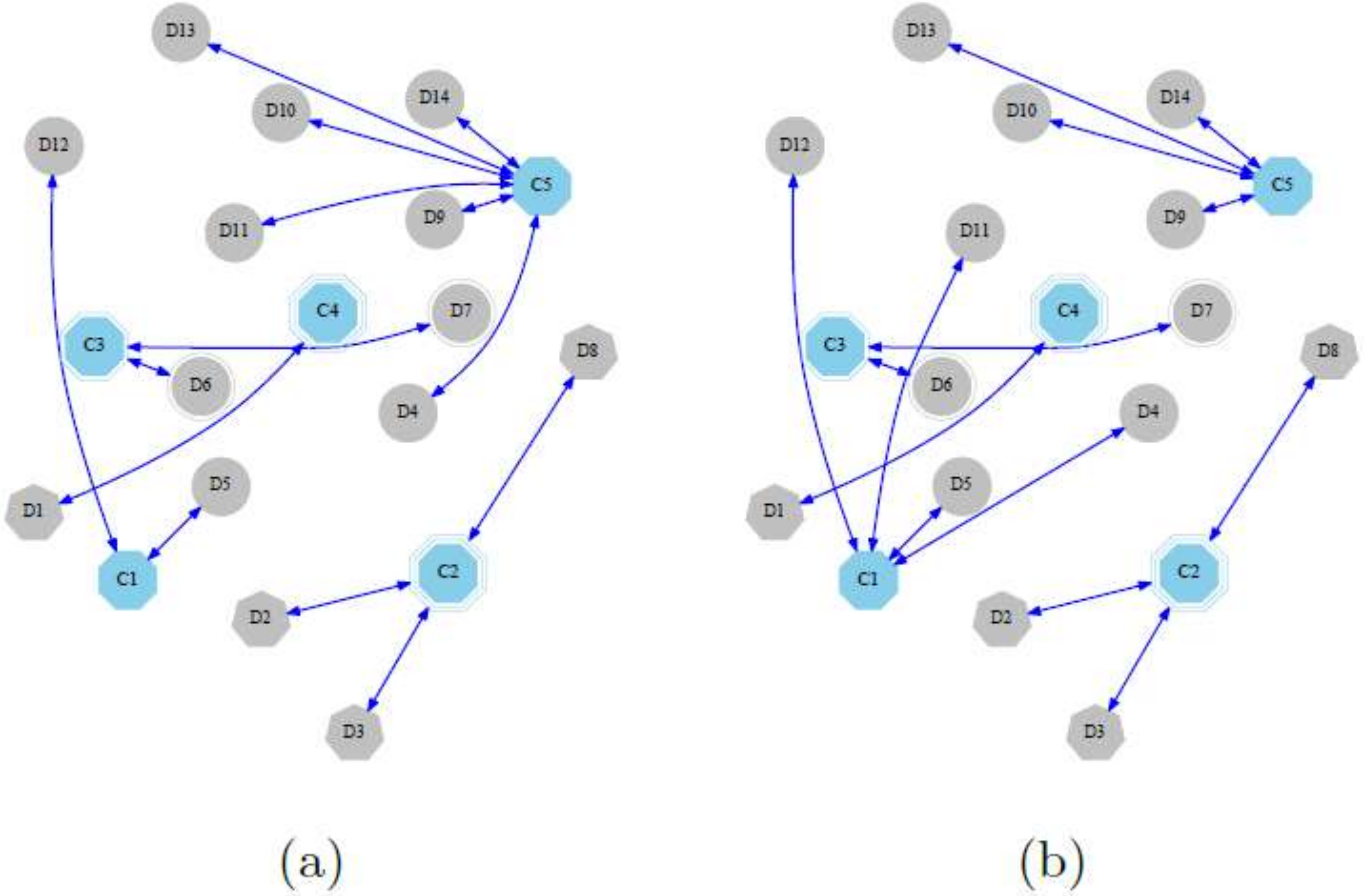
(a)

(b)

(c)

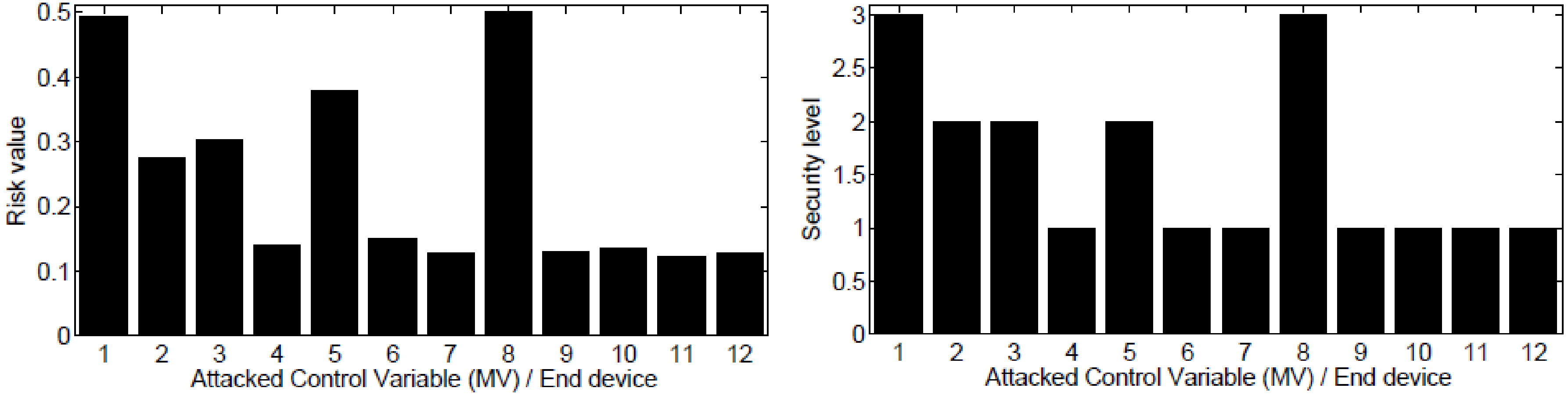
Experimental assessment

- IEEE 14-bus electricity grid
  - (a) unconstrained;
  - (b) constrained by the link capacity of C5.



Experimental assessment

- Tennessee Eastman chemical plant
  - (a) Pure risk values;
  - (b) Risk values enforced in 3 security level groups

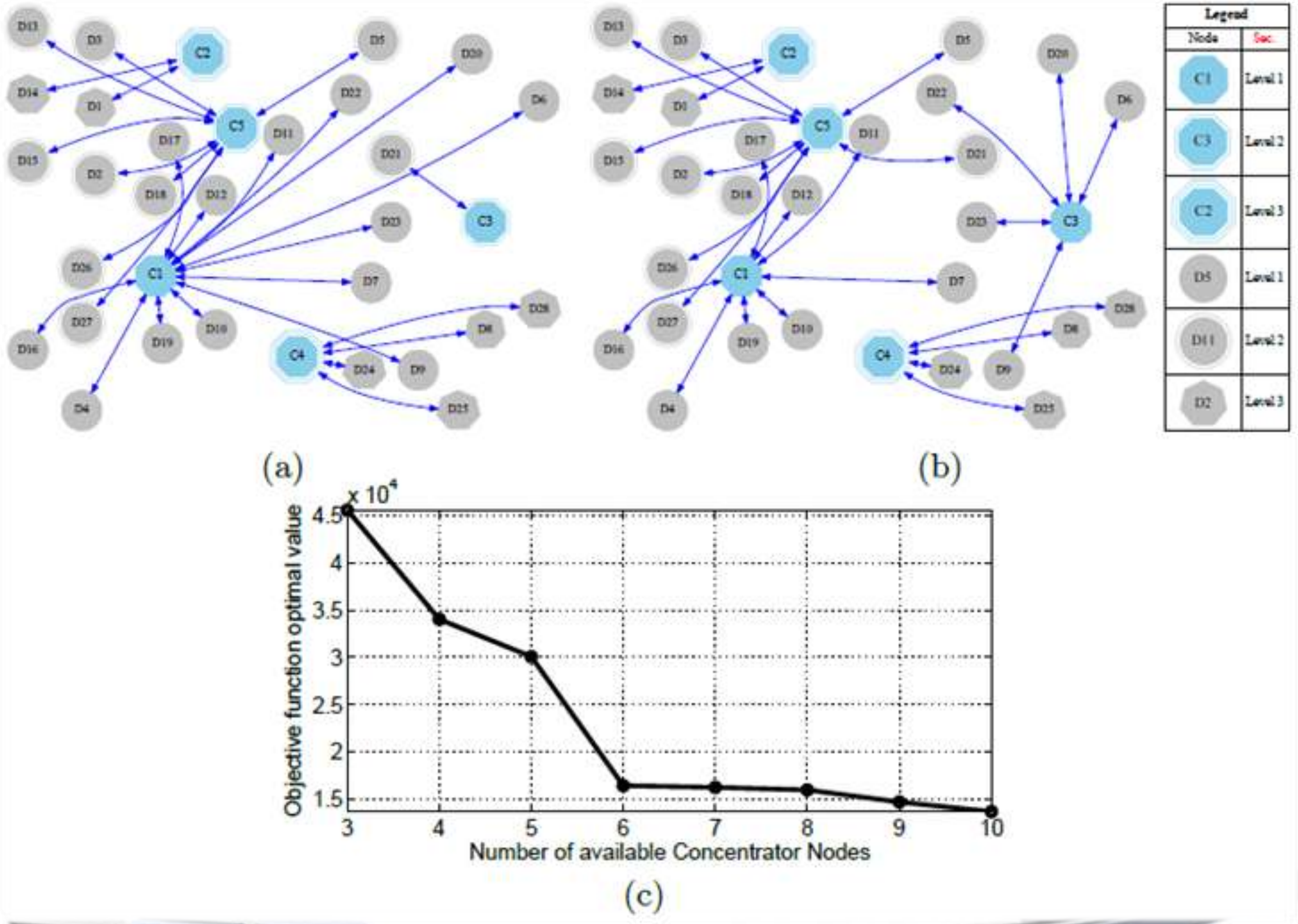


(a)

(b)

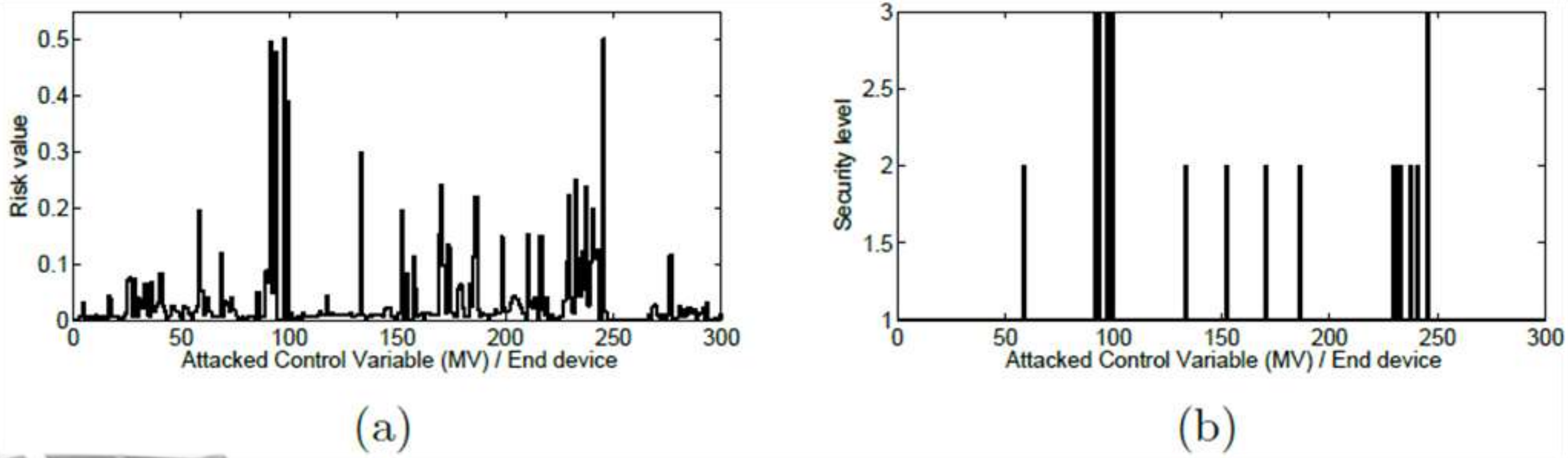
Experimental assessment

- Tennessee Eastman chemical plant
  - (a) with initial parameters;
  - (b) with C3's security level changed to 1;
  - (c) Objective function's optimal values for different number of CN.



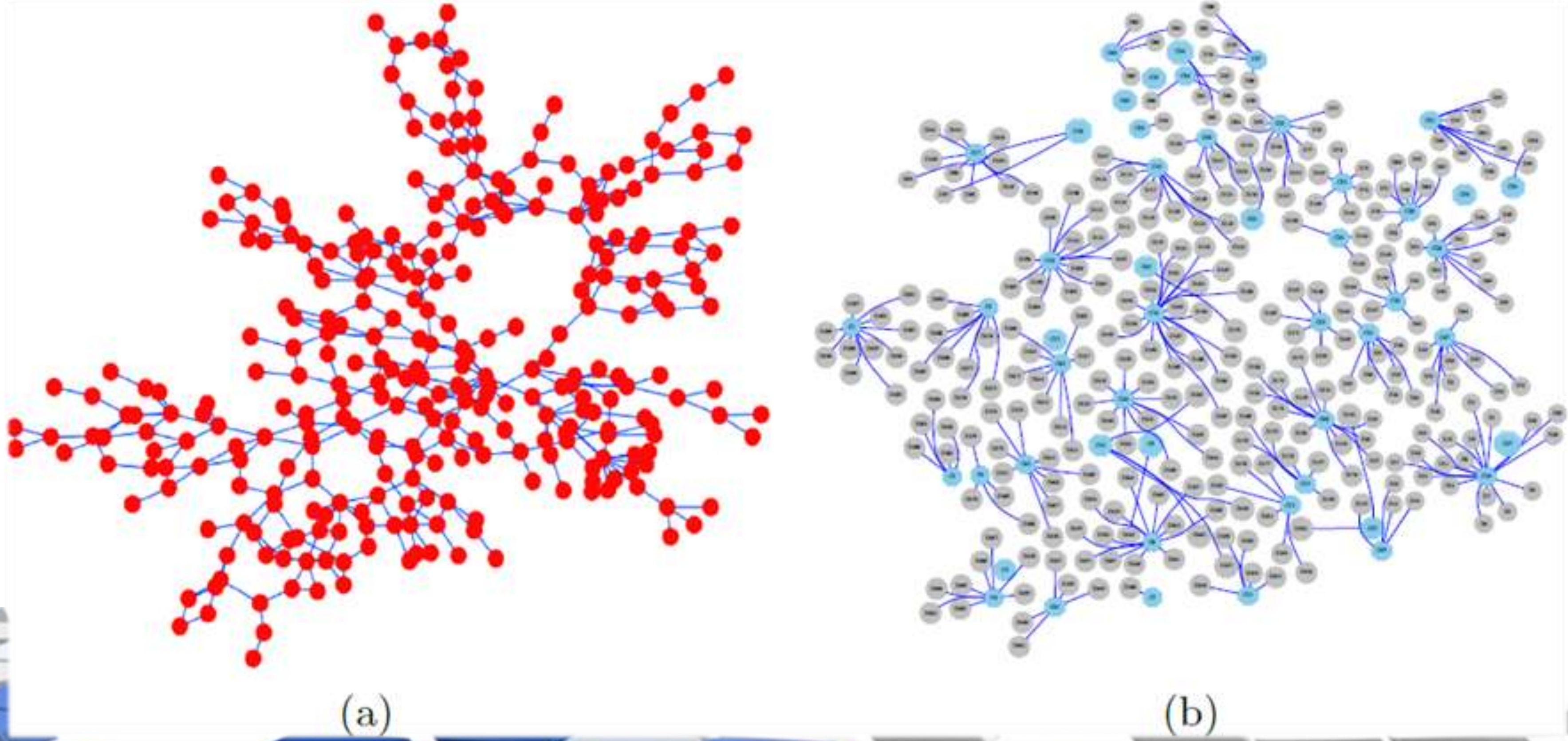
Experimental assessment

- IEEE 300-bus large-scale electricity grid
  - (a) Pure risk values;
  - (b) Risk values enforced in 3 security groups.



Experimental assessment

- IEEE 300-bus large-scale electricity grid
  - (a) electrical topology[1];
  - (b) communication infrastructure with 50 CN.



[1] P. Hines, S. Blumsack, E. Cotilla Sanchez, and C. Barrows. The topological and electrical structure of power grids. *In System Sciences (HICSS), 2010 43rd Hawaii International Conference on*, pages 1-10, Jan 2010.

Conclusions

- We developed a methodology for the optimal design of industrial networks.
- The approach relies on a risk assessment technique and an optimization problem to minimize connection distances, while enforcing security and capacity requirements.
- The preliminary studies and the experiments revealed the importance of considering cyber security in the design phase of ICS.

Thank you!

István Kiss
"Petru Maior" University of Targu Mures, Romania
istvan.kiss@stud.upm.ro