Data Fusion Framework for Cyber Vulnerability Assessment in Smart Grid

SWITS'18
06.13
Stockholm

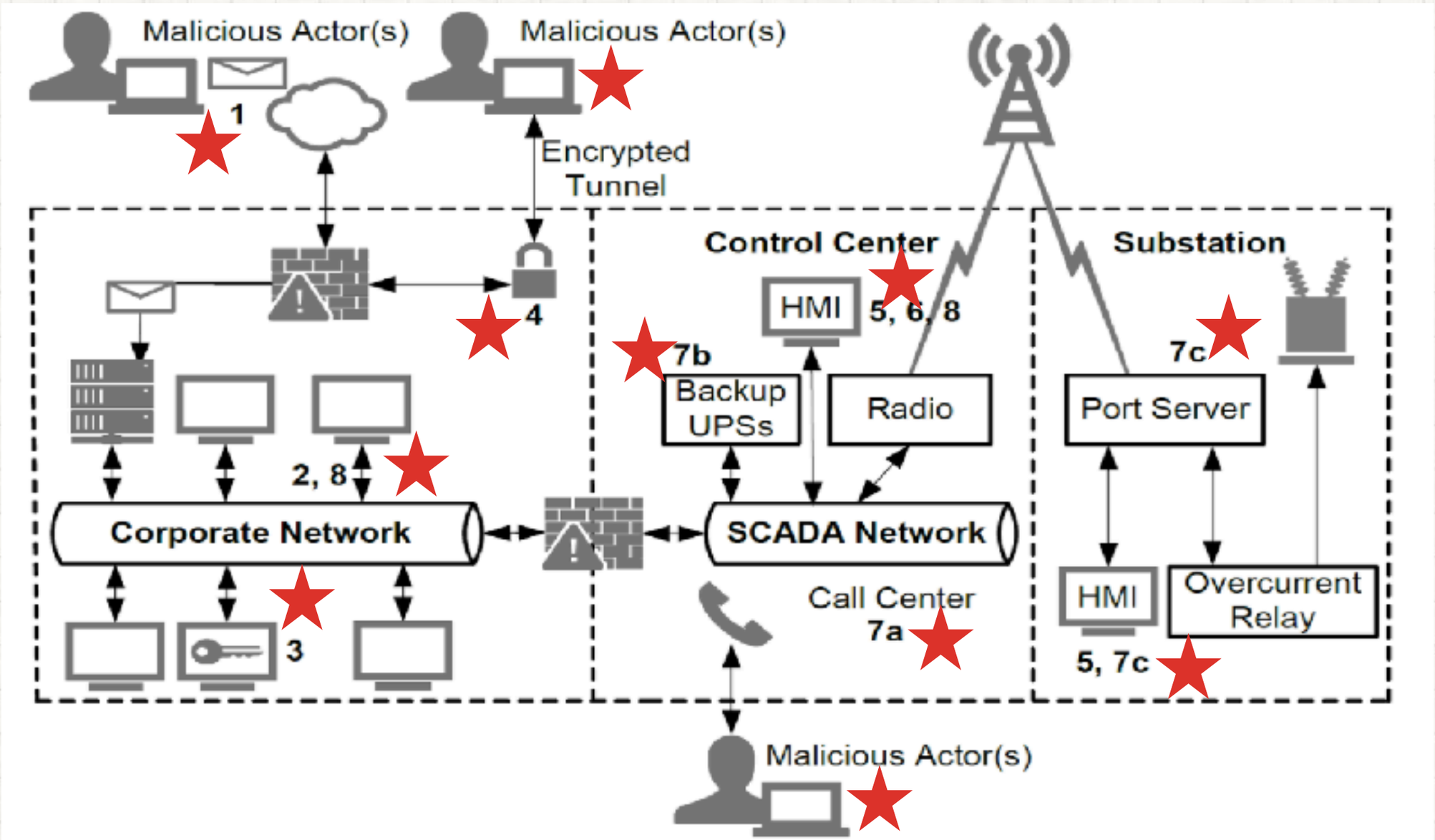
Yuning Jiang *(yuning.jiang@his.se), Yacine Atif, Jianguo Ding*
School of Informatics, University of Skövde

OUTLINE

- Motivation
- Research Question
  - Q1: Data Fusion
  - Q2: Vulnerability Assessment Framework
- Conclusion

BACKGROUND

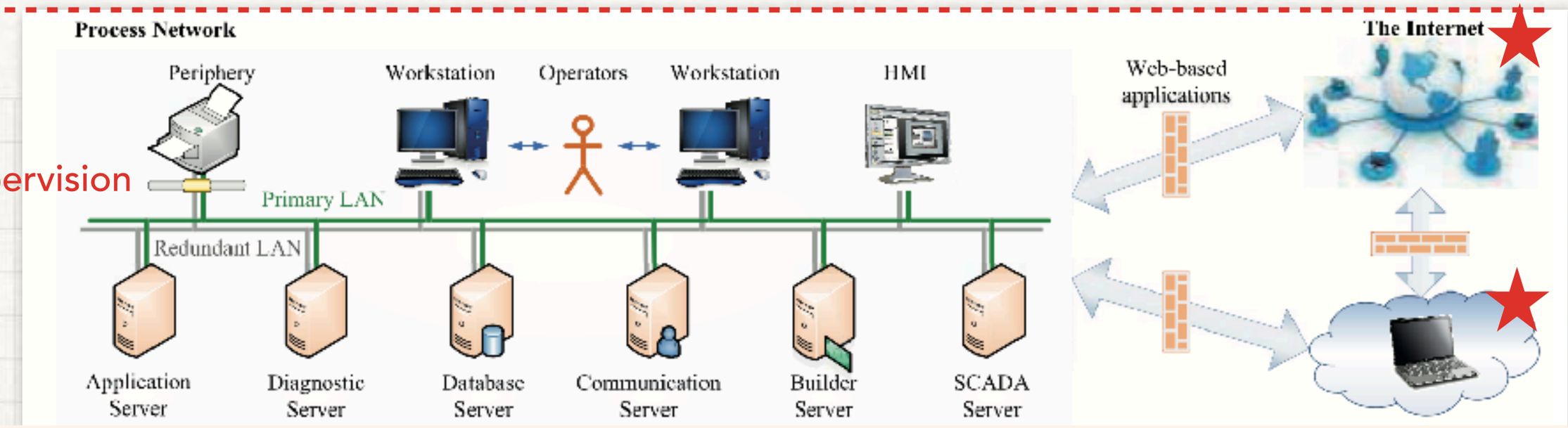
- Smart grid is faced with an increasing amount of cyber threats.
- Vulnerabilities exist throughout all the sub-systems of smart grid.



Ukraine Attack in the year 2015 (Whitehead et al., 2017)

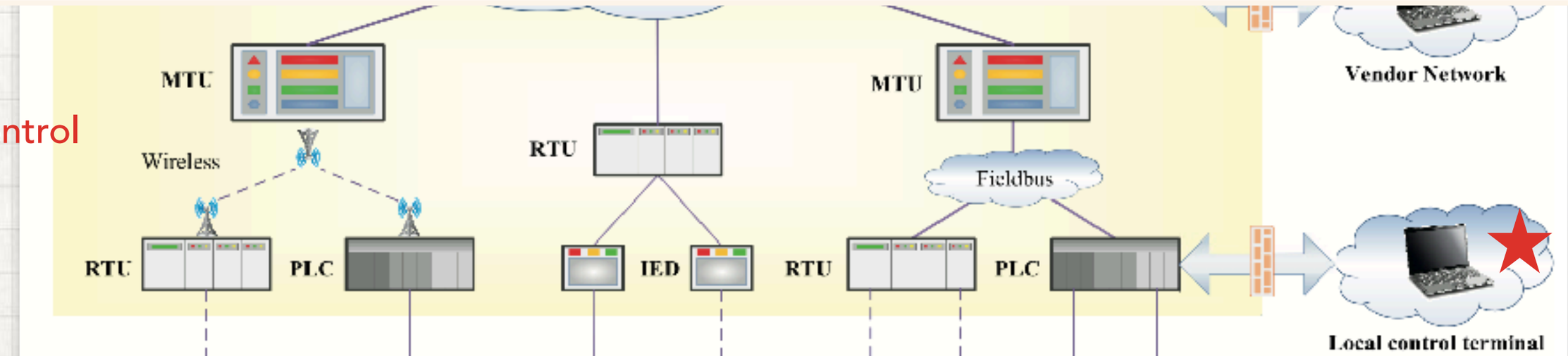
MOTIVATION

Supervision

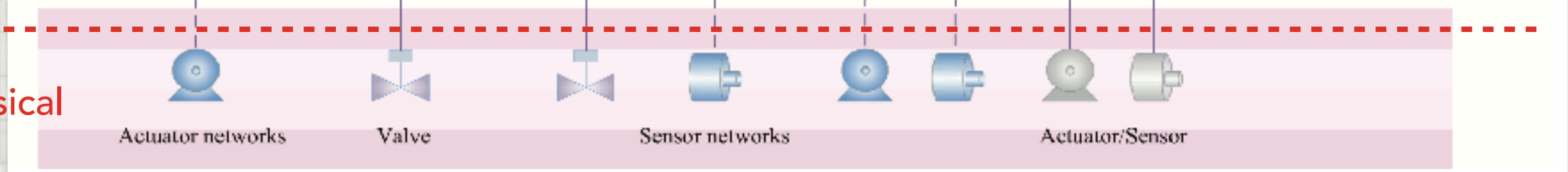


Heterogenous data from smart-grid layers could be used to analyse vulnerabilities against cyber threats.

Control



Physical



Smart Grid Structure (Fillatre et al., 2017)

B

Main Question:

How to model vulnerability assessment against cyber threats using data fusion in smart grid?

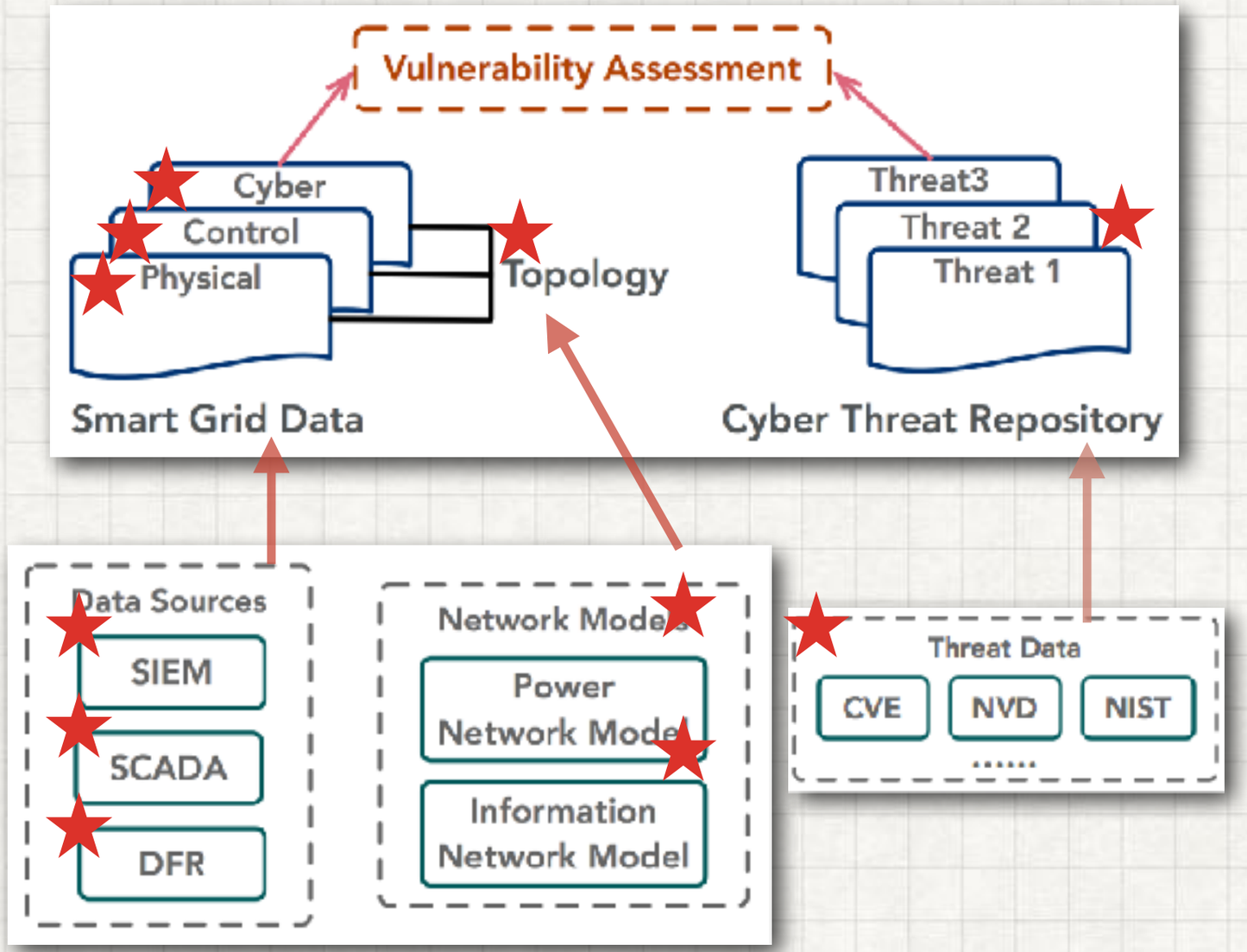
- Q1: How to integrate multiple sources of data?

- Q2: How to formulate cyber vulnerability assessment?

Q1: DATA FUSION

What are the data?

$$y = Mx + e$$



Data from smart grid:

- Physical data, e.g. power/ information networks, fault events (DFR);
- Control data, e.g. commands (SCADA);
- Cyber data, e.g. incidents events (SIEM);
- Topology data.

Data from cyber threat repository:

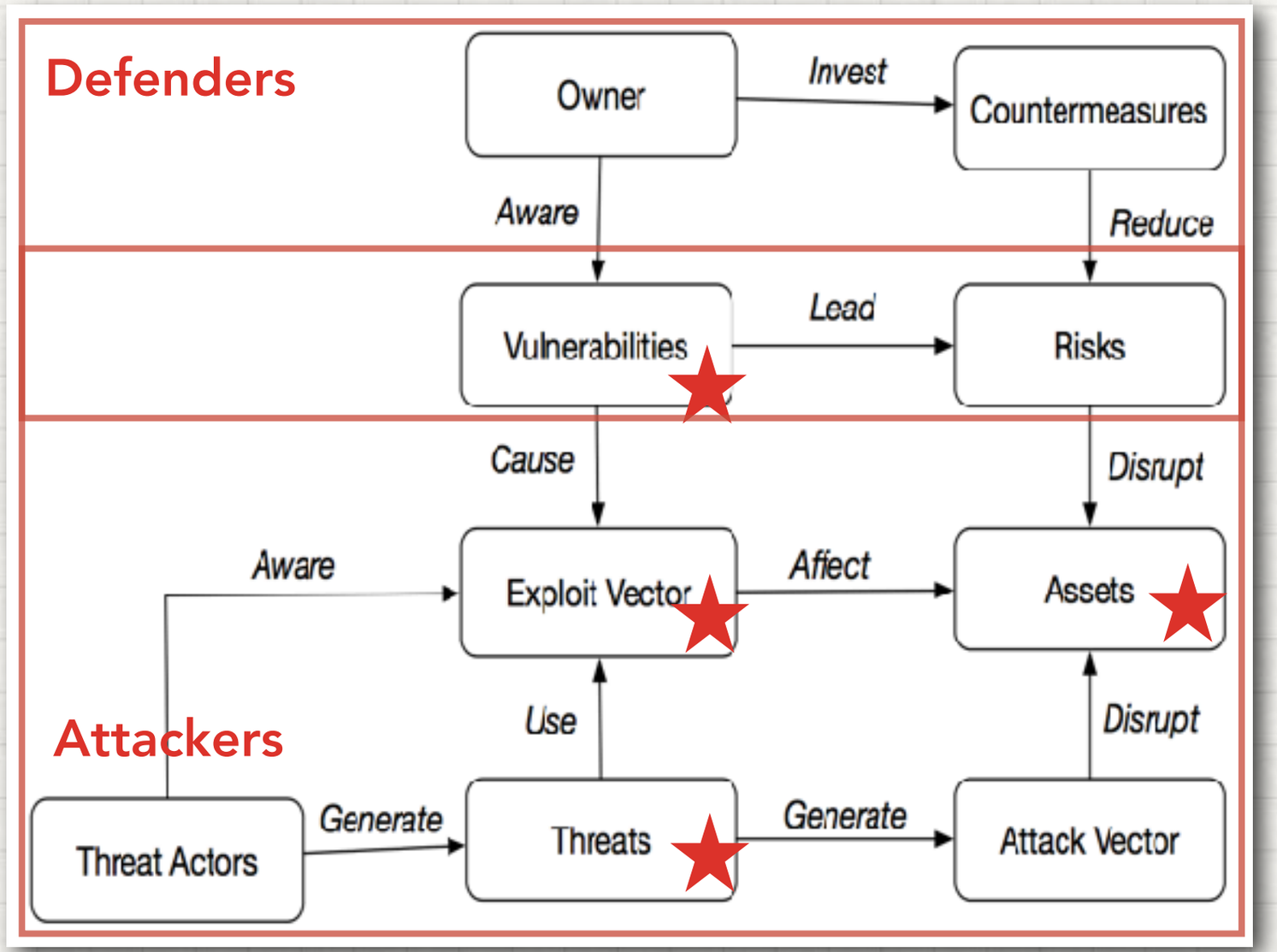
- Cyber threat patterns and attributes from existing standard databases.

SIEM: Security Incidents and Event Management; SCADA: Supervisory Control and Data Acquisition;
DFR: Digital Fault Recorder; CVE: Common Vulnerability and Exposure; National Vulnerability Database;
NIST: National Institute of Standard and Technology

Q2: VULNERABILITY ASSESSMENT FORMULATION

What is vulnerability?

Vulnerability is "weakness of an asset or control that can be exploited by a threat" according to ISO/IEC 27000:2009.



Concepts and Interactions

3 aspects of vulnerability:

- Type of cyber threats;
- Probability of acquiring related exploits;
- Victim assets that might be evolved.

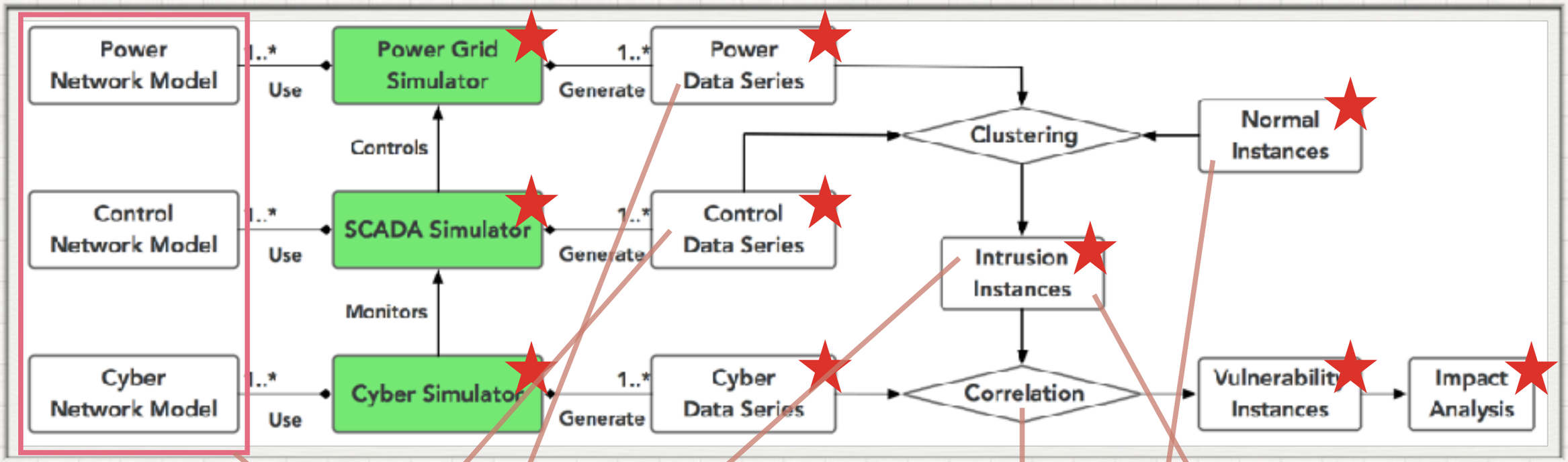
$$\bar{x} = x + a$$

x: power-state vector

a: attack vector

Q2: VULNERABILITY ASSESSMENT FORMULATION

How to use the data?



$$y = Mx + e$$

$$\bar{x} = x + a$$

Vulnerability Assessment Framework

CONCLUSION

- Smart grid cyber-physical structure induces cyber vulnerabilities;
- Data from multiple layers of smart grid architecture could be analysed to root out cyber vulnerabilities;
- Next work focuses on validation of data fusion vulnerability assessment models.

“Thanks. Questions?”

REFERENCES

- By Alan, RH, March, ST, Park, J. and Ram, S., 2004. Design science in information systems research. *MIS quarterly* , *28*(1), pp.75-105.
- Fillatre, L., Nikiforov, I. and Willett, P., 2017. security of SCADA systems against cyber–physical attacks. *IEEE Aerospace and Electronic Systems Magazine*, *32*(5), pp.28-45.
- Peffers, K., Tuunanen, T., Rothenberger, M.A. and Chatterjee, S., 2007. A design science research methodology for information systems research. *Journal of management information systems*, *24*(3), pp.45-77.
- Whitehead, D.E., Owens, K., Gammel, D. and Smith, J., 2017, April. Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. In *Protective Relay Engineers (CPRE), 2017 70th Annual Conference for* (pp. 1-8). IEEE.