Karlsruhe Institute of Technology

Institute for Automation and Applied Informatics (IAI)
Research Area Advanced Automation Technologies (A2T)
Research Group Secure Energy Systems (SES)

Preliminary study for an alarm correlation framework based on risk assessment in IEC 61850 substations

Sine Canbolat*, Ghada Elbez, Prof. Dr. Veit Hagenmeyer

Cyber-physical security of future energy systems

- understand risk sources
- amplify risk awareness
- help engineers and/or operators for reducing the number of alerts
- mitigate risks in the further steps
- integrated by the SIEM (Security Information and Event Management) systems

- securing decision-making
- arising security concerns
- investigating which part of the **Smart Grid** is under **risk** and at which **level**
  - integrating recommendations from the **IEC 62351-7** standard

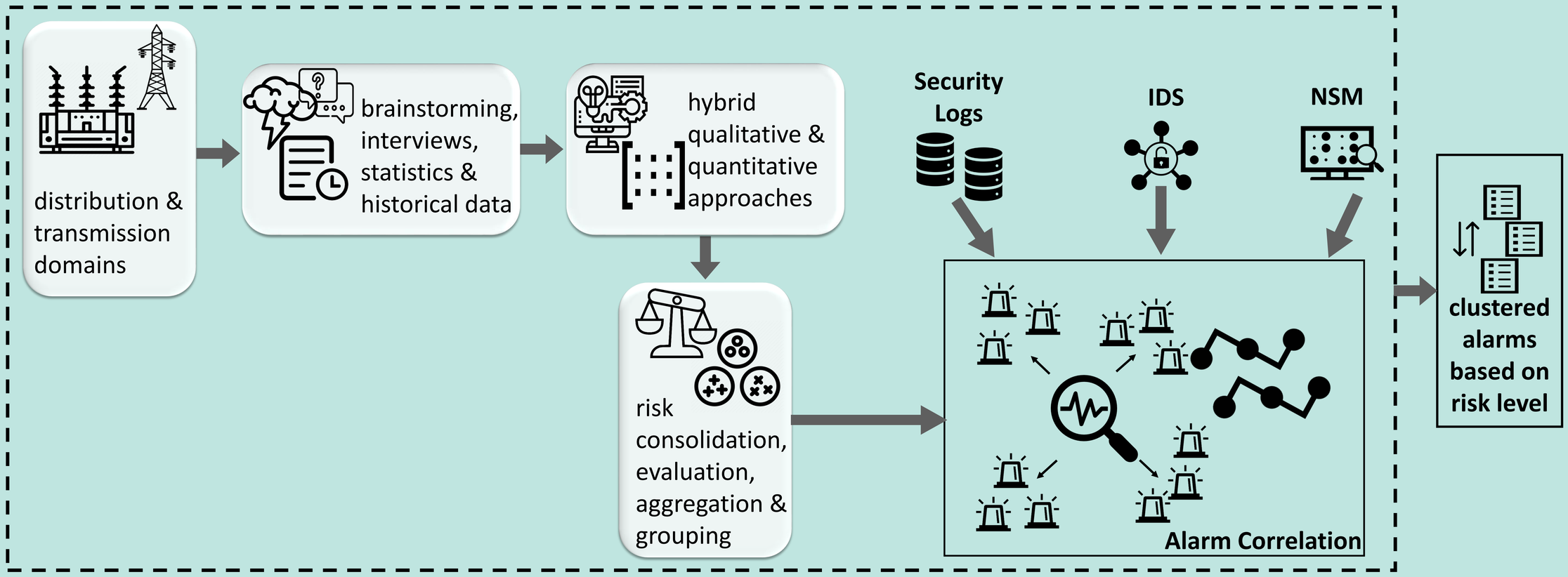
WHY

HOW

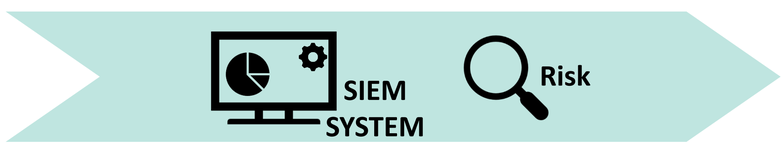
WHAT

- get logs and alarms from various levels and devices
- define the **risk level** corresponding to the **threat**

- implement **risk assessment** process [1]
- **analyze** and **correlate** various **alarms** according to **risk analysis**



How will we measure success?



- To which extend does the offered solution provide a comprehensive **risk assessment** process when compared to available SIEM systems?

- Are the **IEC 62351-7** recommendations adopted comprehensively?
  - based on collected DOs (Data Objects)

[1] Refsdal, A., Solhaug, B., & Stølen, K. (2015). Cyber-risk management. In Cyber-risk management (pp. 33-47). Springer, Cham.

* sine.canbolat@kit.edu