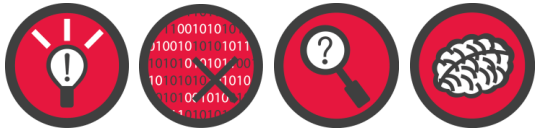
itrust consulting



Fonds National de la Recherche Luxembourg

This work was supported by the Fonds National de la Recherche, Luxembourg (project ref. 10239425).

Risk Monitoring in Industrial Control Systems

19/04/2016

ADaCoR 2016

Steve Muller

Risk Monitoring in Industrial Control Systems

Why risk monitoring?

Main objective:

Connect low-level view (intrusion detection) to high-level view (risk analysis)

intrusion detected

in real-time

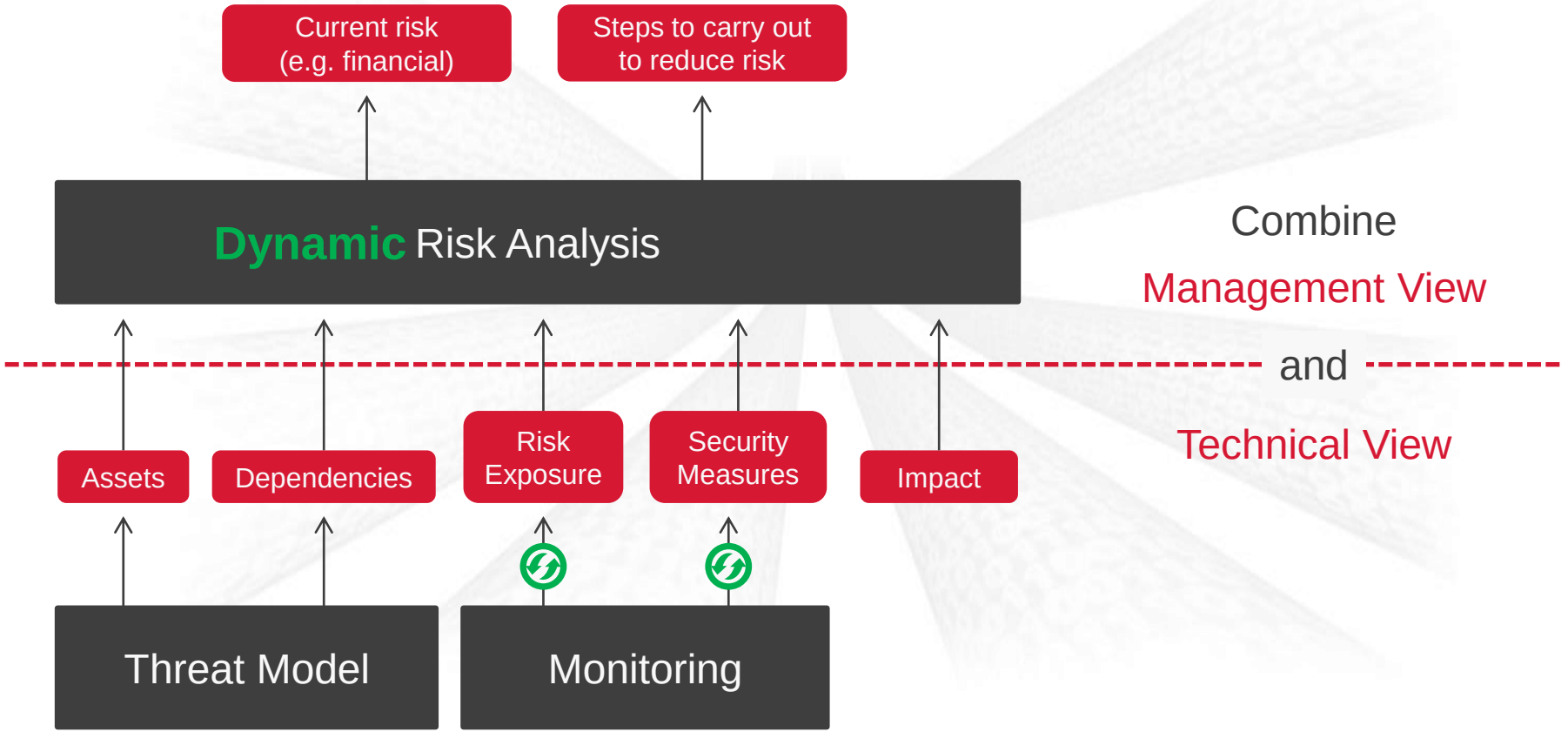
What is

- impact on other components?
- long-term damage?
- current risk exposure?
- priority to fix security issues?

in real-time

Risk Monitoring in Industrial Control Systems

How is it achieved?



Combine

Management View

and

Technical View

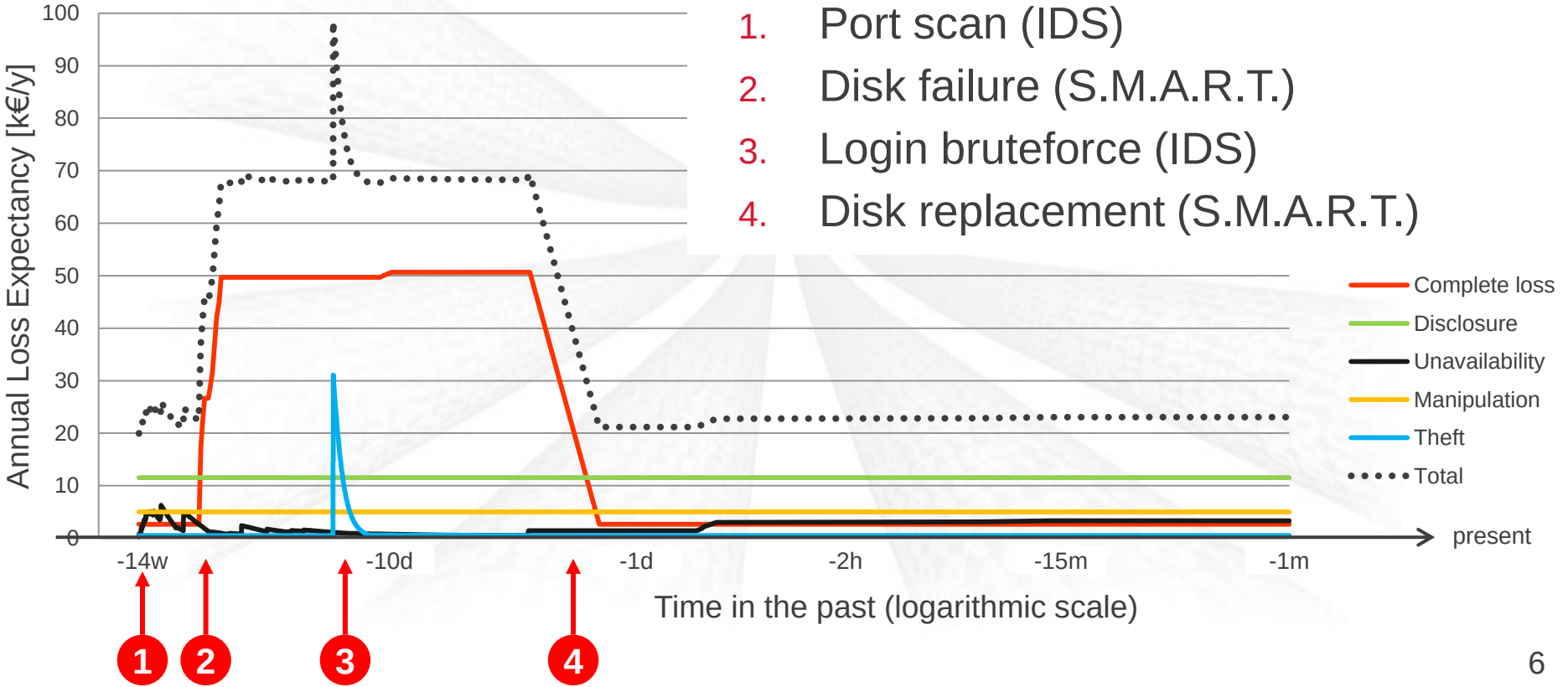
Risk Monitoring in Industrial Control Systems

Overview

I. Threat Model *supporting dependencies between assets*
II. Intrusion Detection Strategy *for Industrial Control Systems*
III. Formalisation of Interface Providing Risk Input Data *(e.g. from IDS)*
IV. Validation *in Smart Grid Luxembourg*

Risk Monitoring in Industrial Control Systems

Dashboard Proof-of-concept



1. Port scan (IDS)
2. Disk failure (S.M.A.R.T.)
3. Login bruteforce (IDS)
4. Disk replacement (S.M.A.R.T.)

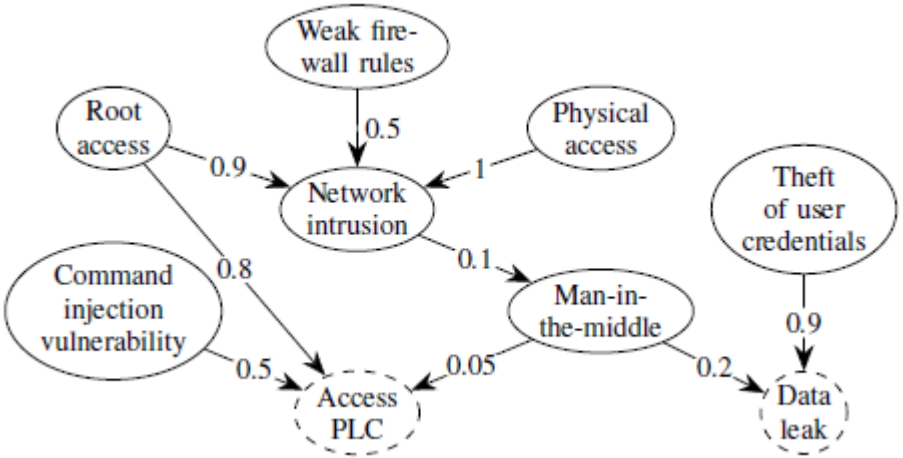
Risk Monitoring in Industrial Control Systems

Dependency model (under publication)

itrust consulting

- Idea: dependency = cause–consequence of incidents
  - encoded as directed graph
  - each Incident has impact, likelihood

- Deep analysis:
  - What-if simulation
  - Find ‘critical’ paths
  - Highlight causes of risk scenario



Risk Monitoring in Industrial Control Systems

IDS strategy for ICS (future work)

itrust consulting

	anomaly-based	signature-based	hybrid
 traffic rejected	*otherwise*	found attack A_1, or found attack A_2 ...	resembles attack A_1, or resembles attack A_2, or ... no pattern recognized
 traffic accepted	resembles benign training data	*otherwise*	resembles benign training data