Cyber Attack Resilient Control Systems

André Teixeira
Henrik Sandberg
Karl H. Johansson

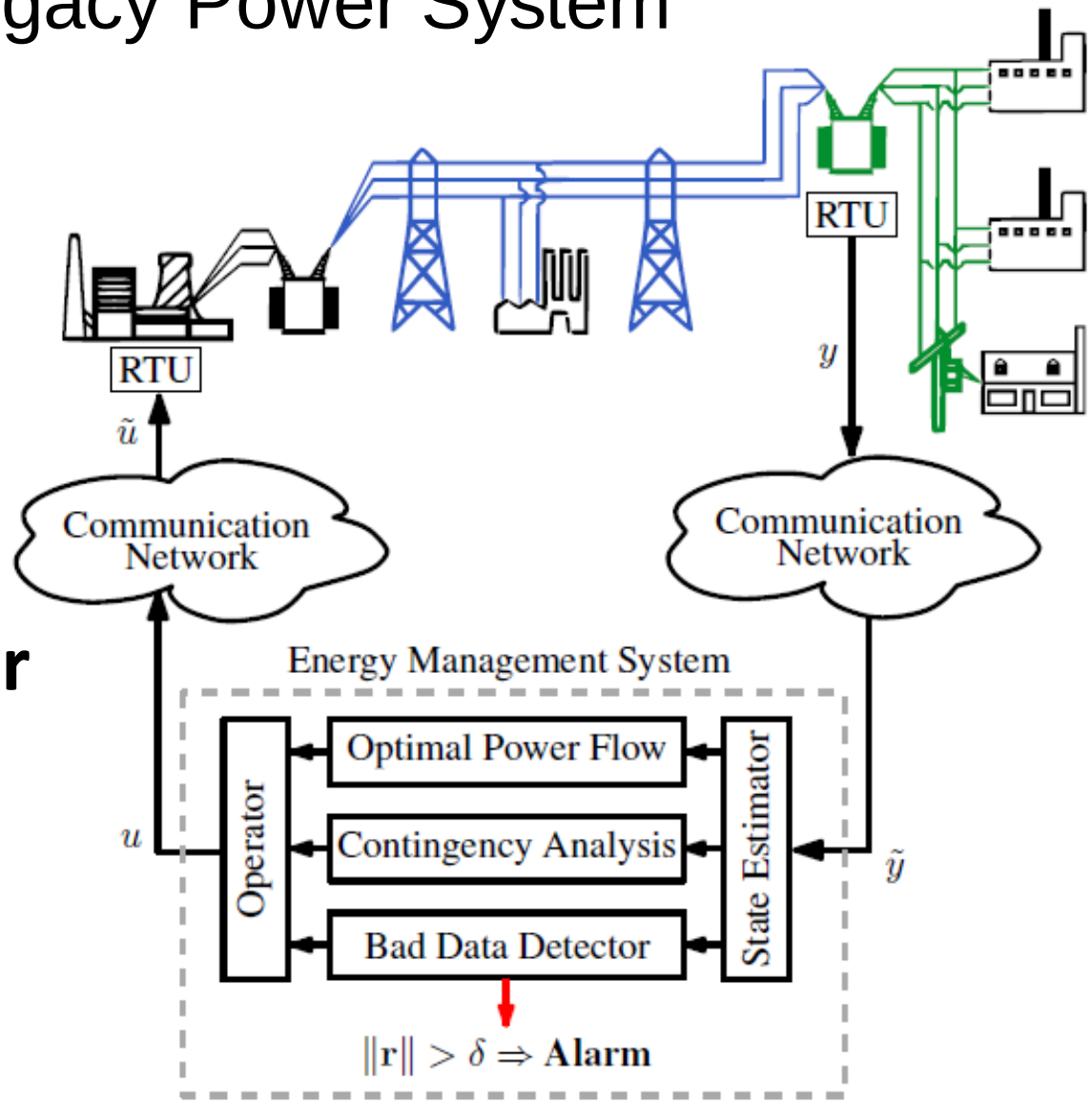
KTH Department of Automatic Control, Sweden

Graz, May 20th, 2014

© The SPARKS Consortium
EU FP7 Programme Contract No. 608224


Motivation: Legacy Power System

Power system control and monitoring over networks



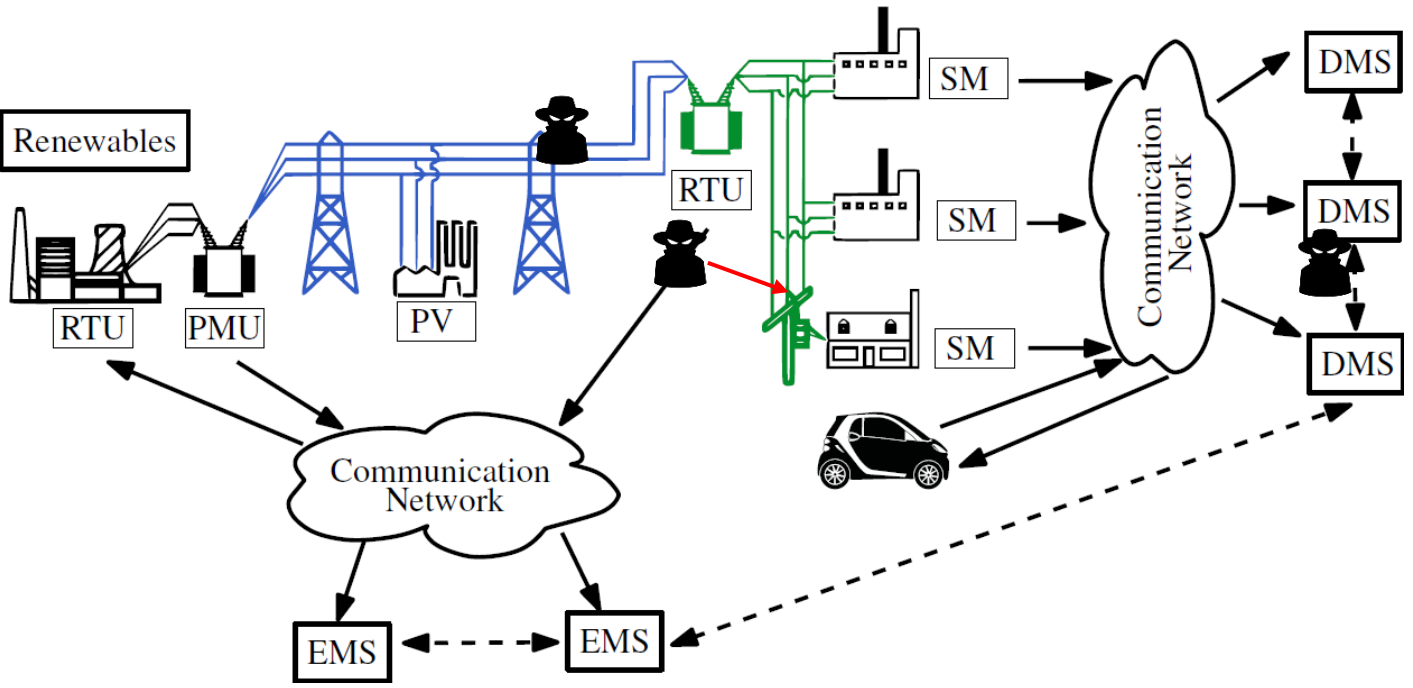
© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

Motivation: Smart Grid

SMART GRID PROTECTION AGAINST CYBER ATTACKS

Smart Grid

- More
  contro
- Large
  comm
- Leads
  vulner
  threat
  points of attacks



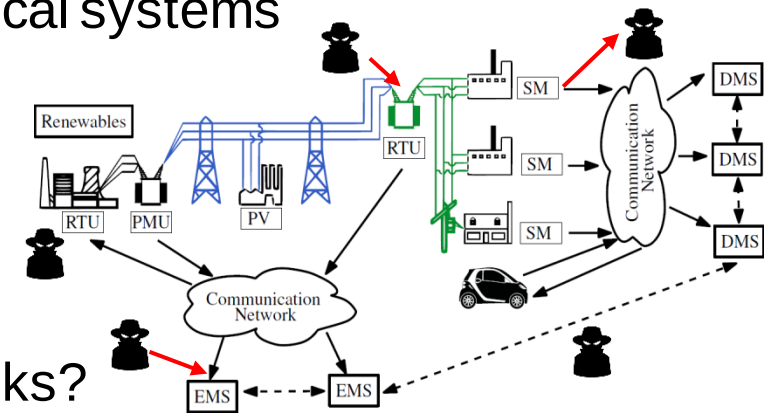
© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

Motivation

- The Smart Grid is a cyber-physical system
  - **Power system** and **IT infrastructure** tightly coupled through SCADA and control systems
  - integrated with data analytics environments etc.

- Traditional IT security provides necessary tools
  - but not sufficient to secure cyber-physical systems

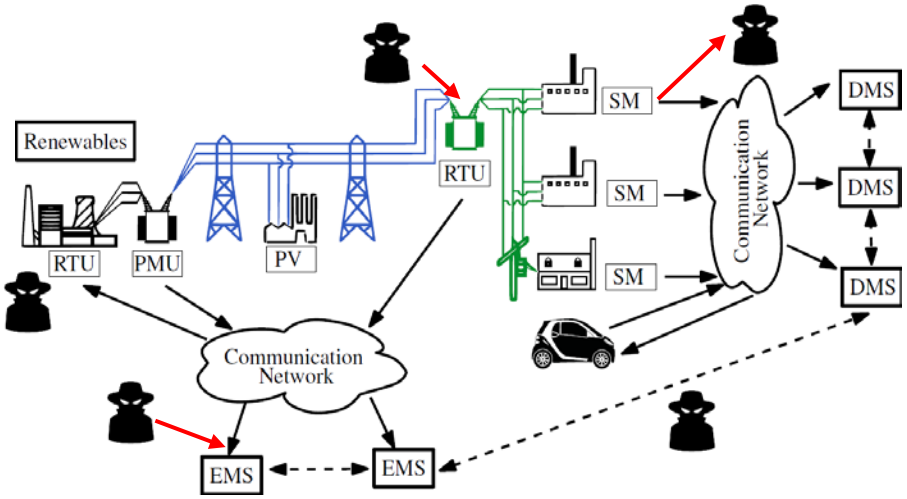
- Need for tools and strategies to understand and mitigate attacks:
  - Which threats should we care about?
  - What impact can we expect from attacks?
  - Which resources should we protect (more)?

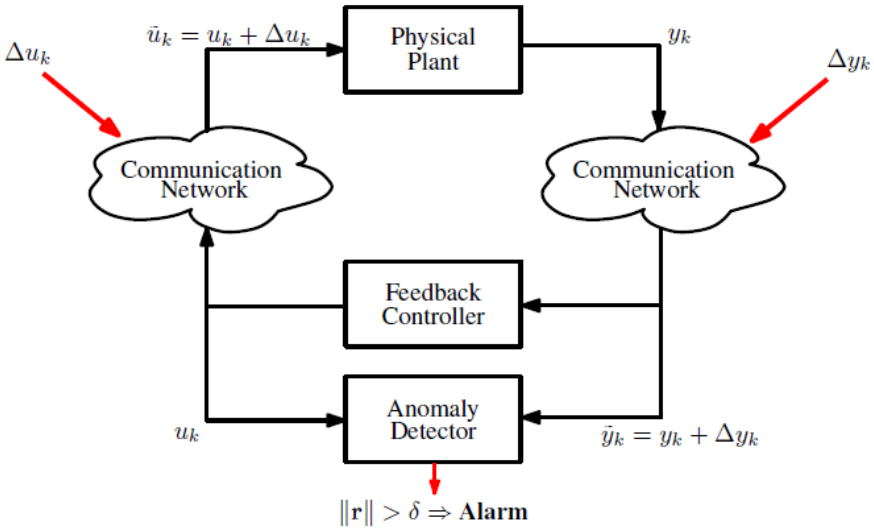


© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

Resilient Control Systems

- Resiliency to disturbances and malicious threats
  - Maintain state awareness
  - Accepted level of performance



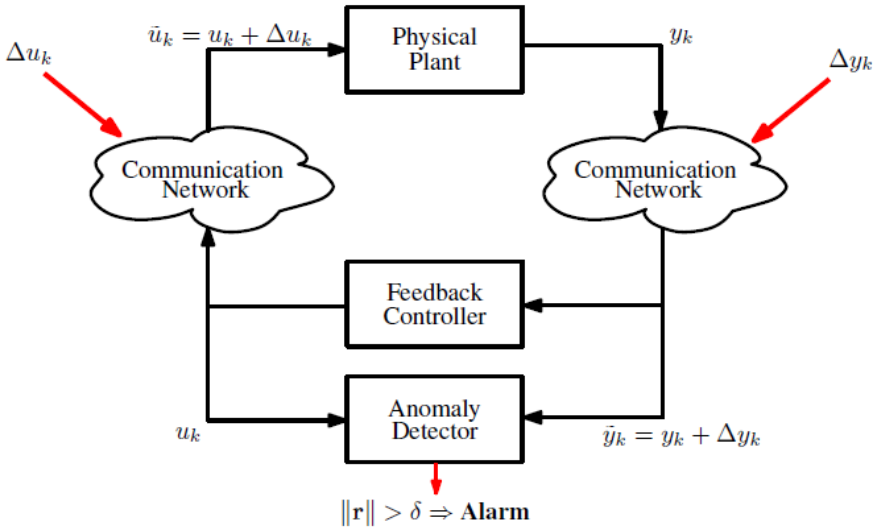


- Obtained through
  - automated fault detection
  - controller reconfiguration (islanding, for example)

© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

Objectives and Desired Outcomes

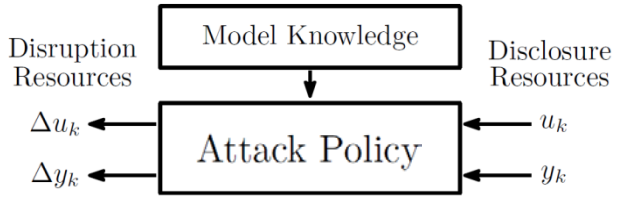
- New methods for cyber-secure networked control

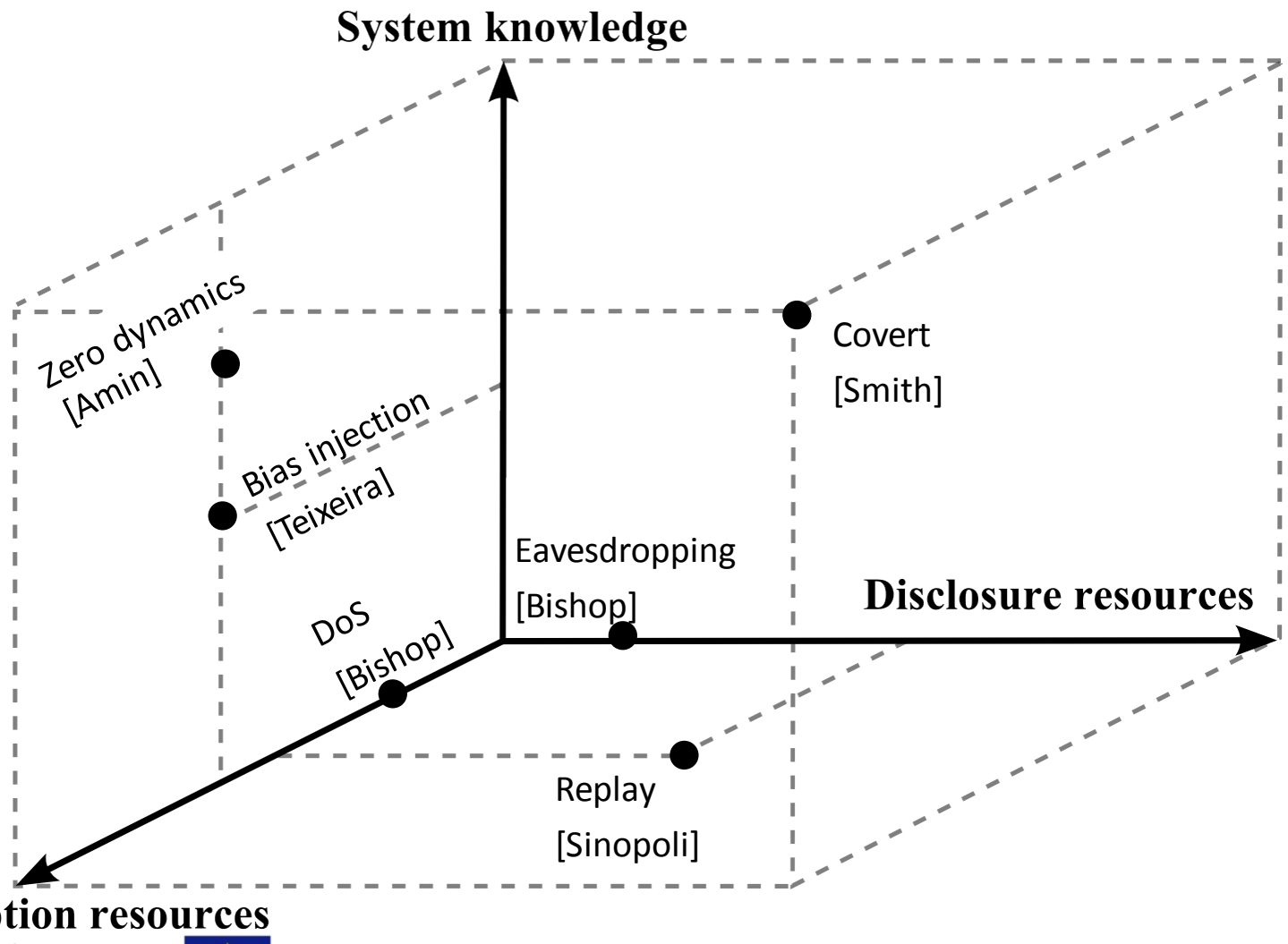


- Quantifying system performance under malicious attacks
- Rigorous theory and practice for resilient feedback controllers and anomaly detectors

© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

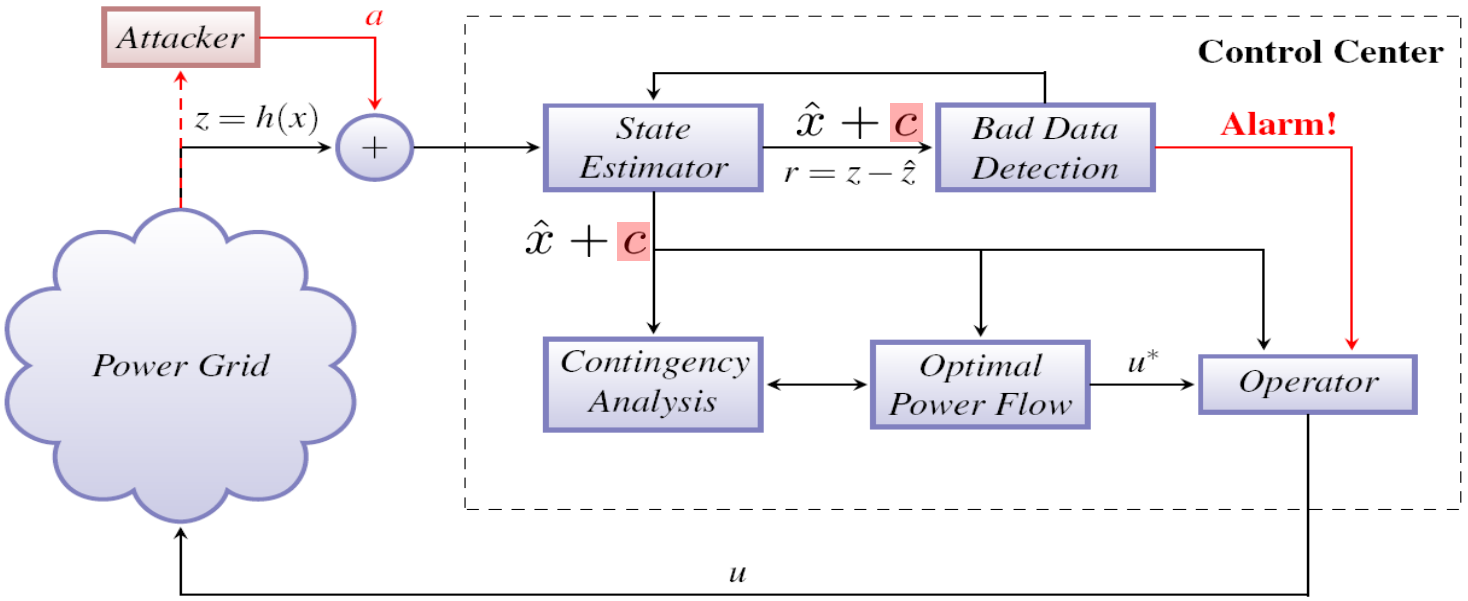
Quantifying the Attack Space





© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

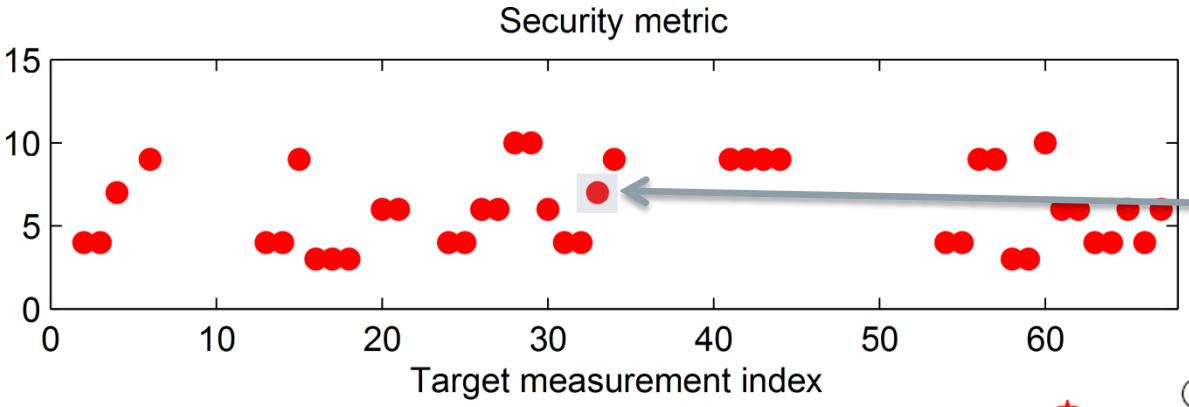
Example: False-data injection on EMS



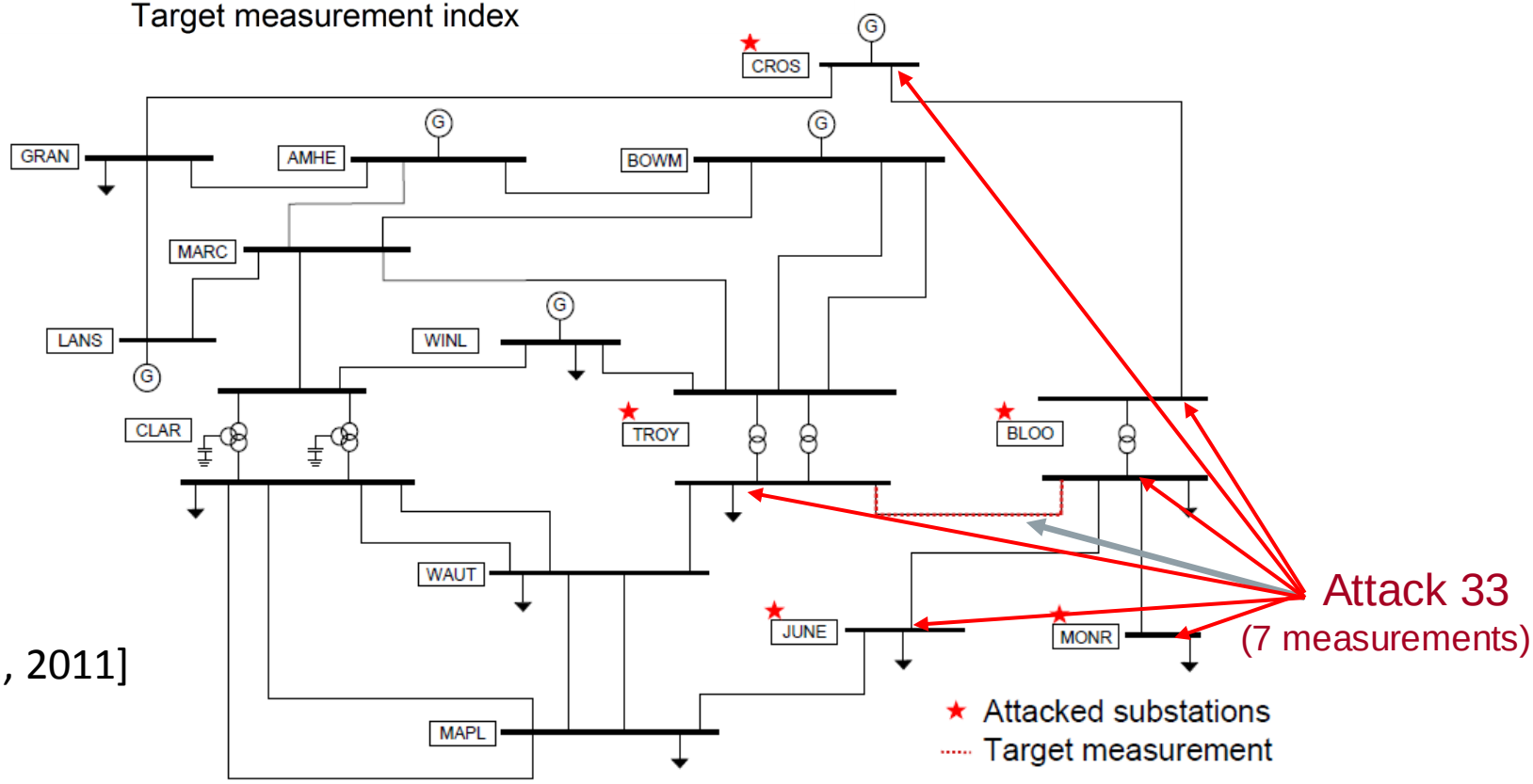
- **Scenario:** Attacker injects **undetectable malicious data** *a* to induce bias *c* in state estimate
  - Which threats should we care about?
  - Which resources should we protect (more)?

© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

Security Metric for VIKING Network



At least 7 measurement readings involved in an *undetectable* attack against measurement 33

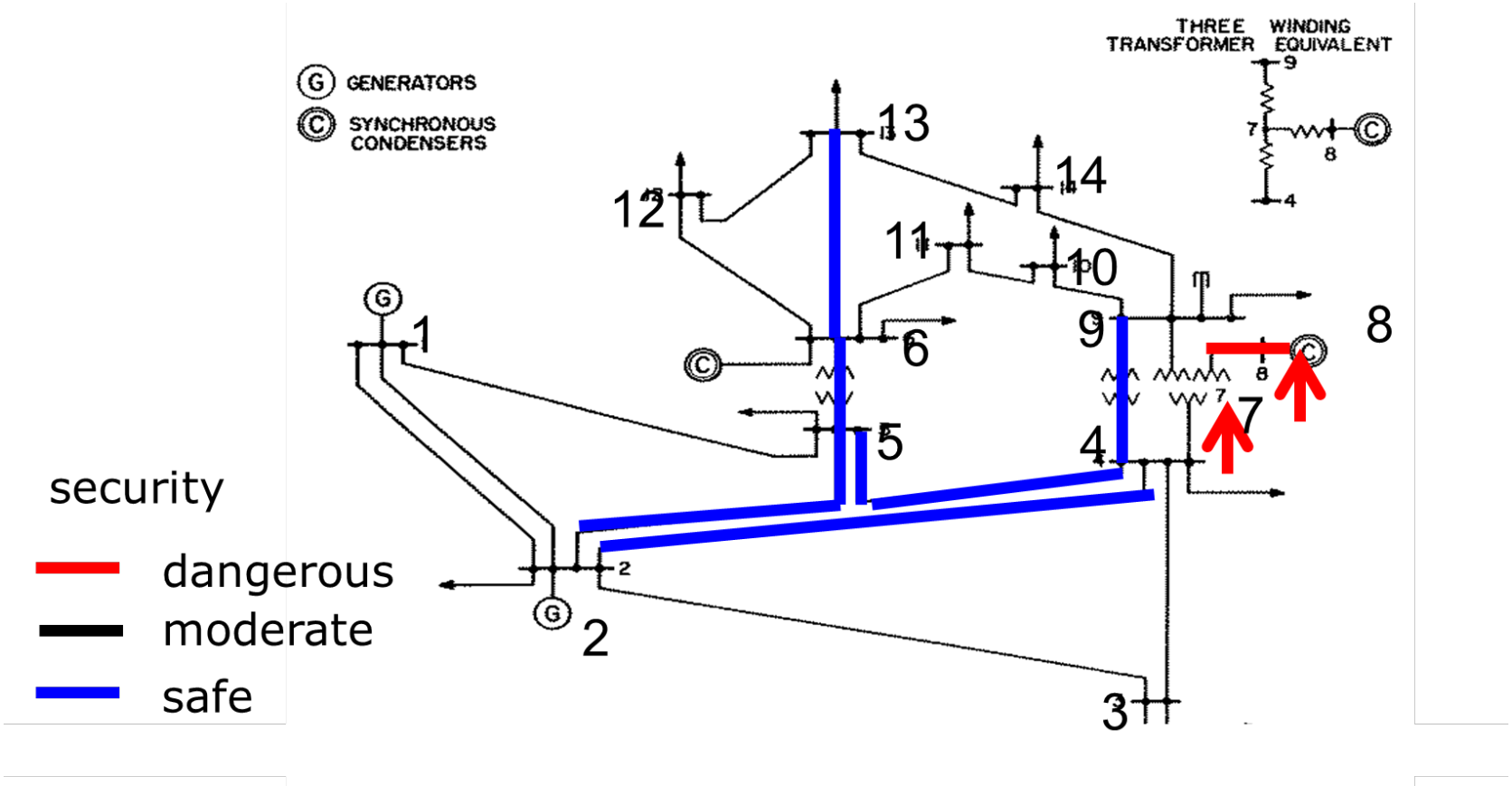


[Teixeira *et al.*, 2011]

© The SPARKS Cons
EU FP7 Programme

Example – Vulnerability Analysis

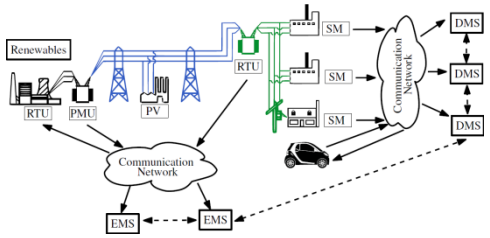
- A security metric from EU-project VIKING



- Used for allocation of new security measures

© The SPARKS Consortium
EU FP7 Programme Contract No. 608224

Discussion Session



SPARKS
SMART GRID PROTECTION AGAINST CYBER ATTACKS

- What are the **key** control loops?
  - Critical control loops to ensure performance / safety?
  - Most cyber-vulnerable control loops?
- Desired input / output of "vulnerability analysis" algorithms for control systems
  - What should the input / output mean in terms of Smart Grid?
  - How should the output be presented?
  - Keywords or system features to keep in mind?
- Meaningful validation scenarios
  - What could be considered a good "proof of concept"?

© The SPARKS Consortium
EU FP7 Programme Contract No. 608224