SMART GRID PROTECTION AGAINST CYBER ATTACKS

Risk Assessment for Cyber-Physical Smart Grid Systems

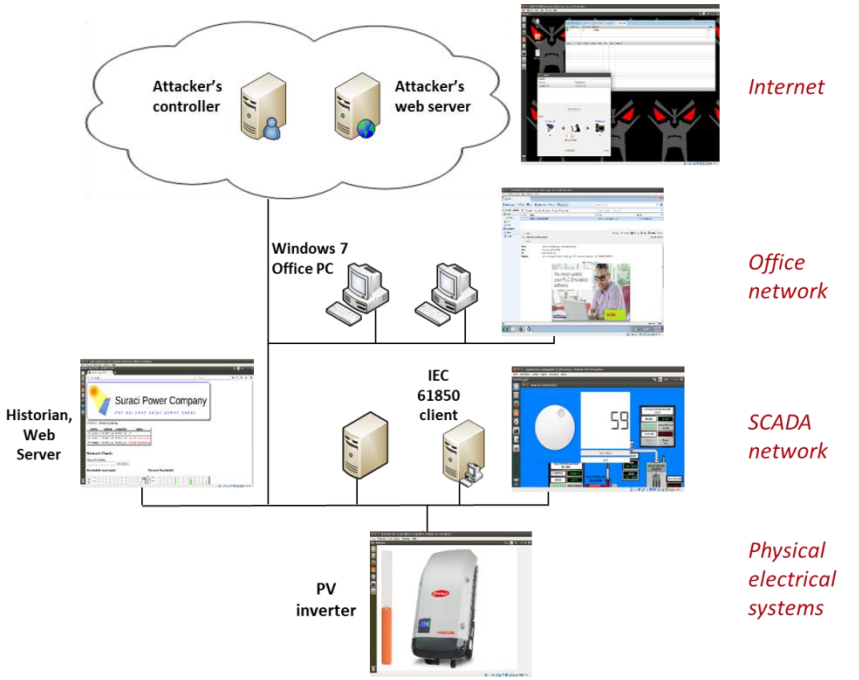
Paul Smith
paul.smith@ait.ac.at
AIT Austrian Institute of Technology

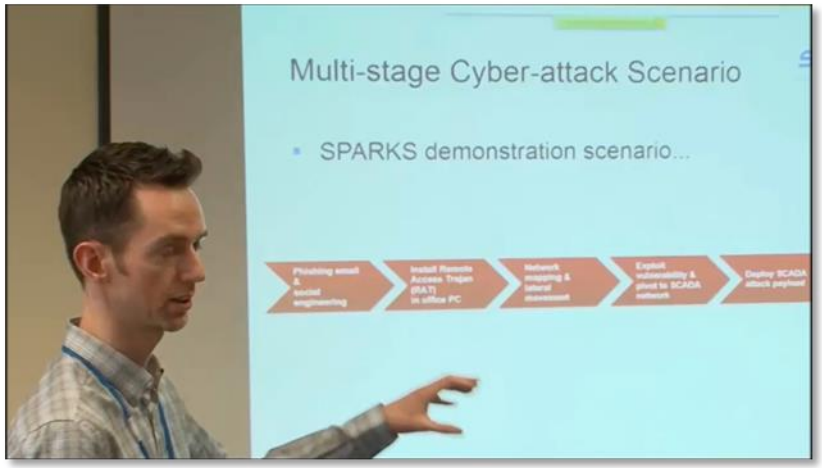
Novel Approaches in Risk and Security Management for Critical Infrastructures
Vienna, 19th September, 2017

EU FP7 Programme Contract No. 608224

Advanced Persistent **Cyber-Physical** Threat: SPARKS Demonstration

SMART GRID PROTECTION AGAINST CYBER ATTACKS



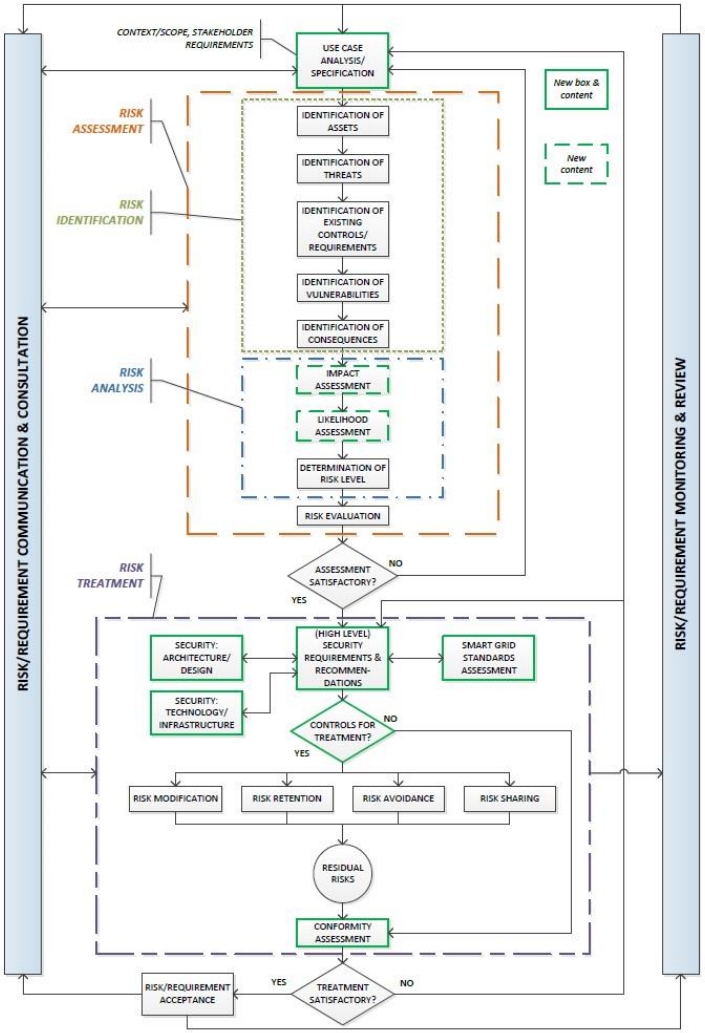


Phishing email & social engineering → Install Remote Access Trojan (RAT) in office PC → Network mapping & lateral movement → Exploit vulnerability & pivot to SCADA network → Deploy SCADA attack payload → Attack physical system functions

EU FP7 Programme Contract No. 608224

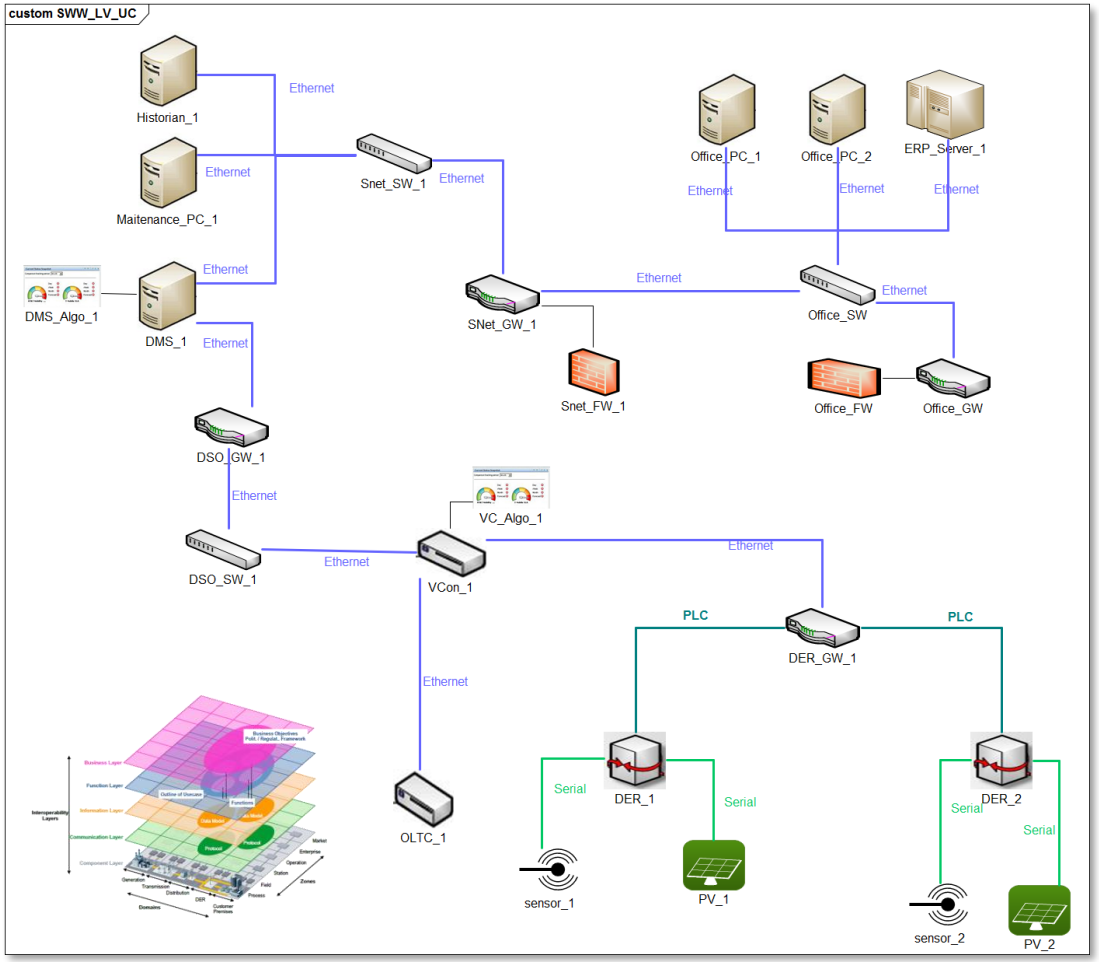
SPARKS Risk Assessment Framework

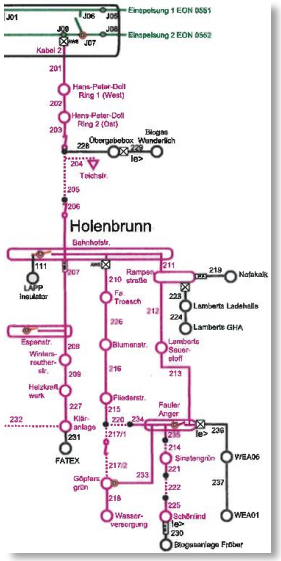
- Based on ISO/IEC 27005
- Familiar to the information security community
- Well-aligned with emerging cyber security requirements and compliance needs for critical infrastructure protection
- Guidance on how to implement the risk management process for a set of smart grid use cases

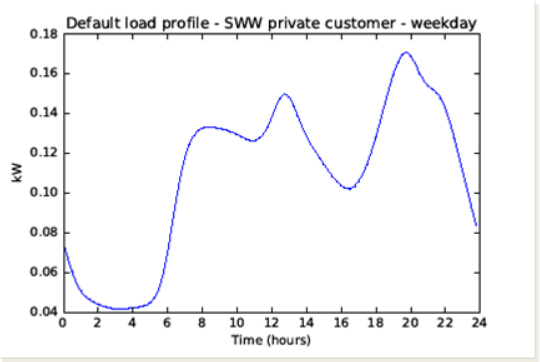


EU FP7 Programme Contract No. 608224

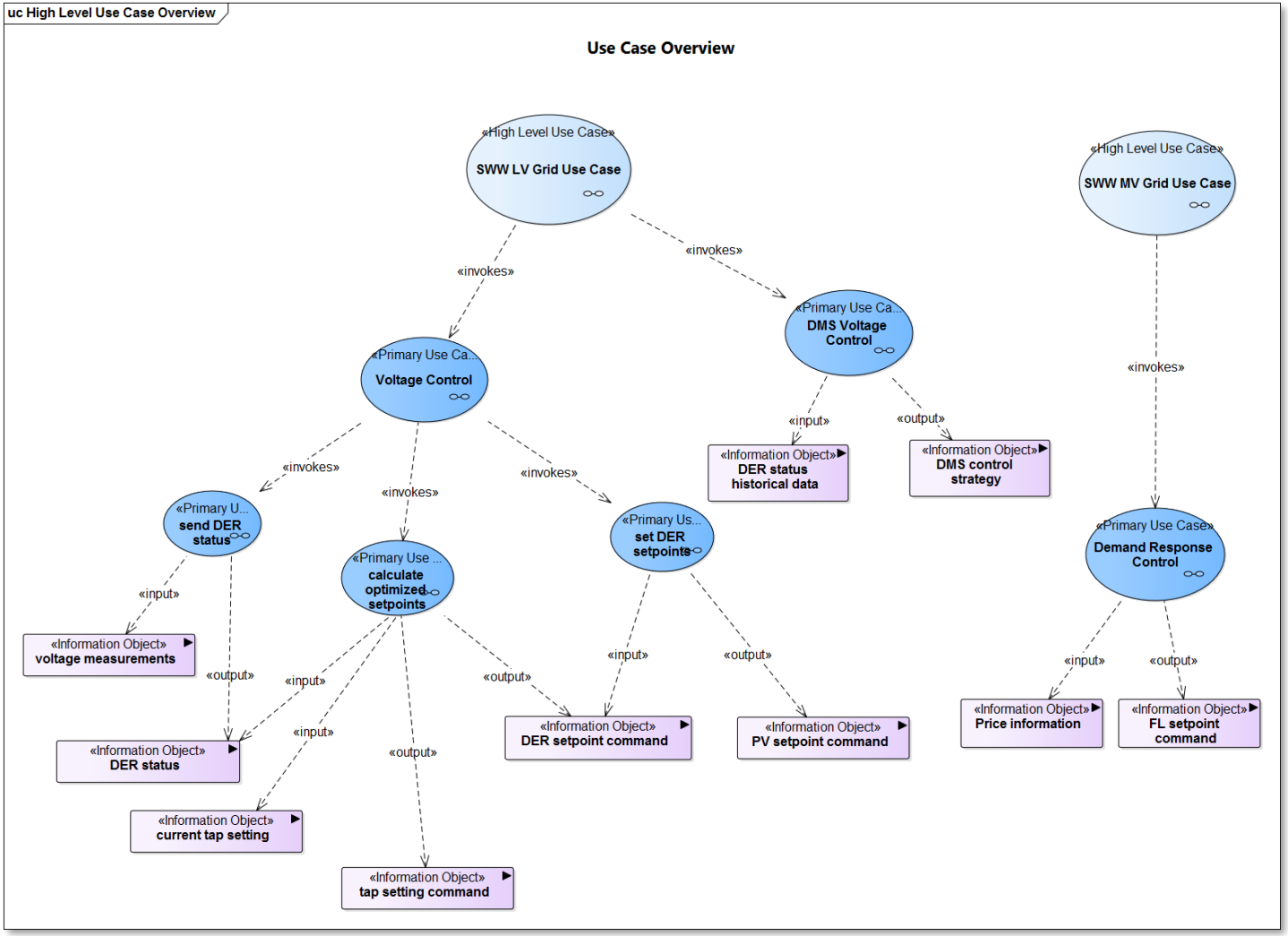
Context Establishment



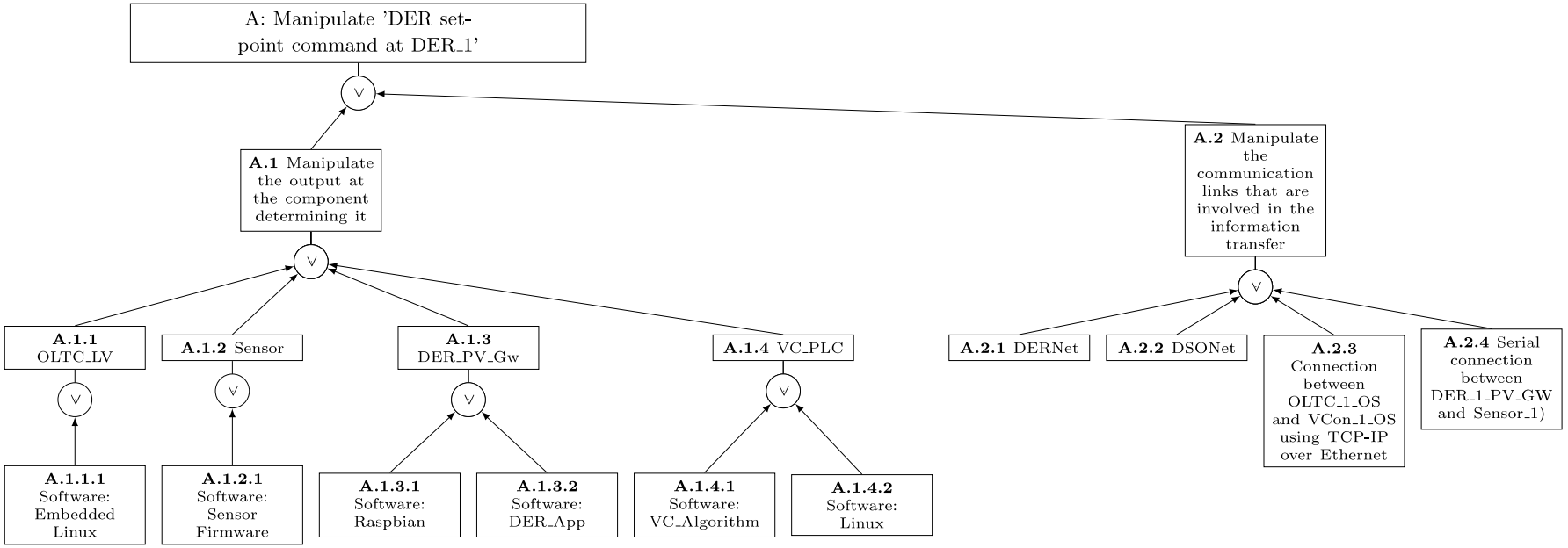




Identification of Assets



Identification of Threats: Attack Trees

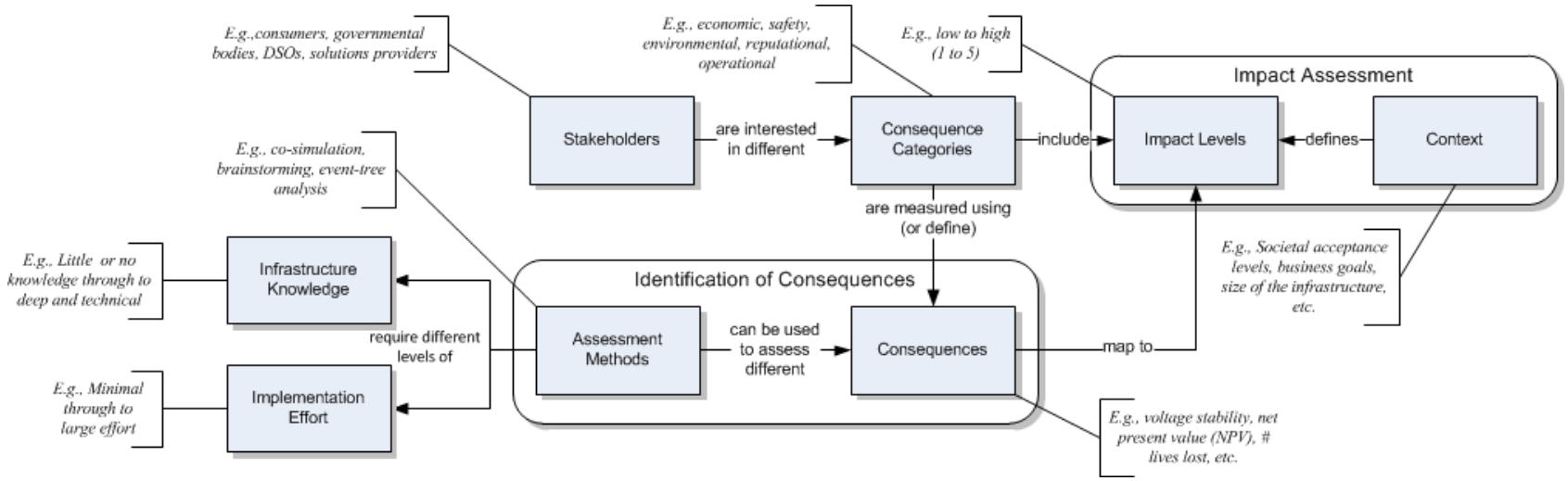


- Developed re-usable attack patterns to support the development of trees
- Tool support for tree generation, using an Ontology that is created from an SGAM-based architecture description

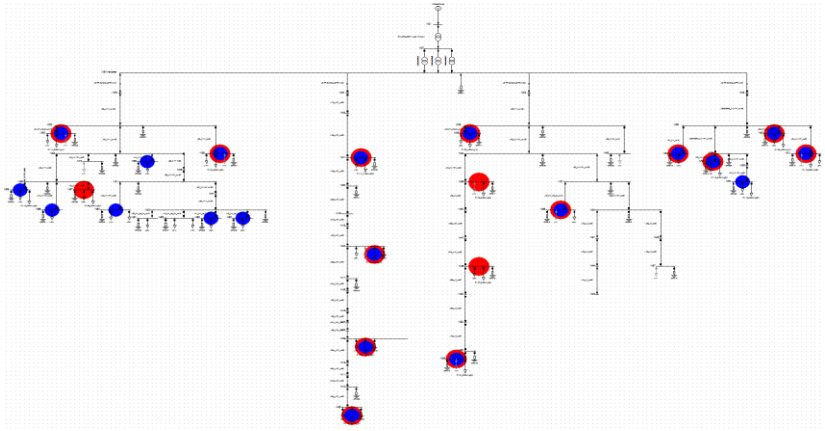
EU FP7 Programme Contract No. 608224

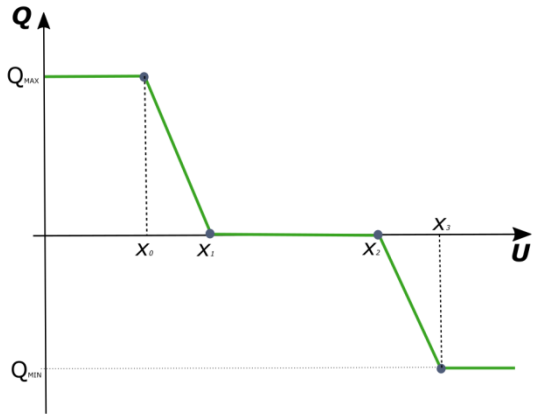
Consequence Identification

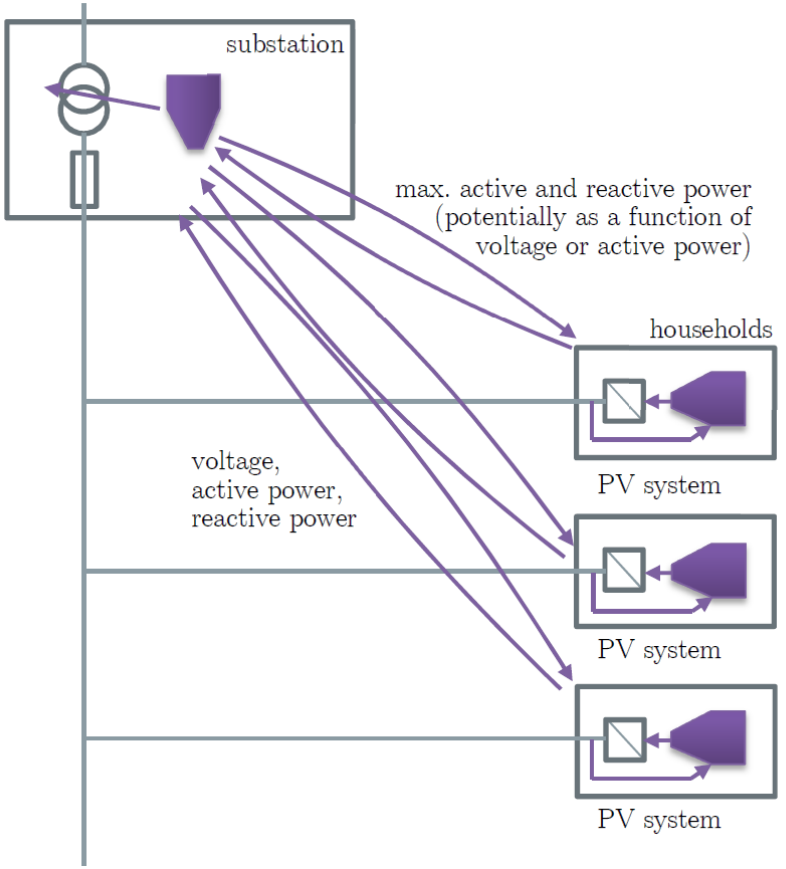
- Consequences identification for information security is largely concerned with data-related (CIA) losses
- In the smart grid, consequences can be wide-ranging, e.g., cyber-physical concerns, and challenging to identify
- Smart grid stakeholders have varied concerns and capacity to analyse consequences



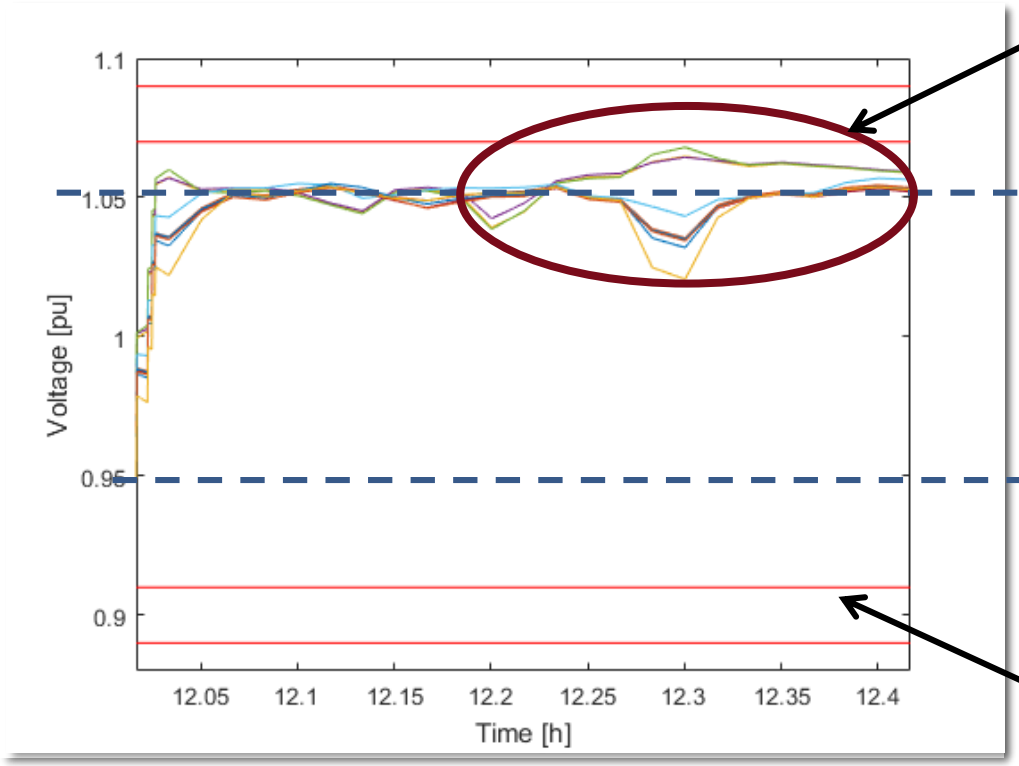
Co-Simulation of Cyber-attack Consequences







Co-Simulation of Power Systems Consequences



Overvoltage situation

±5% of the nominal voltage (230V)

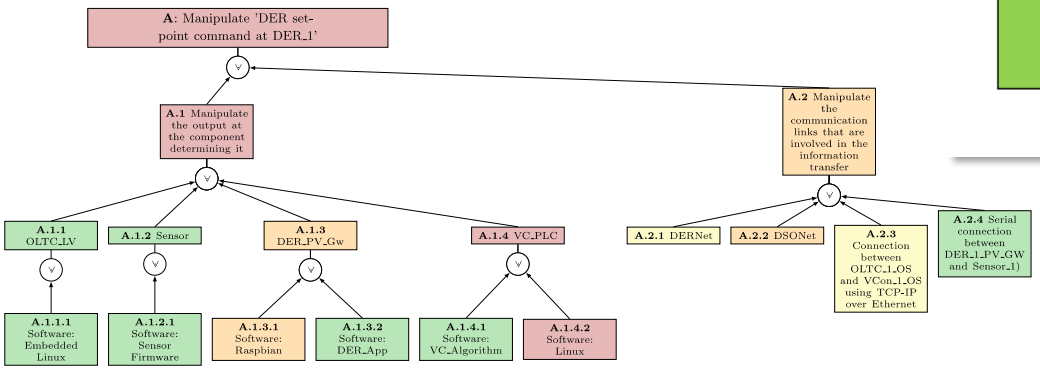
Manipulated Q(U) curve parameters

Likelihood and Impact Assessment

- Assign consequences to an organisation-specific impact level
- Analyse the threat likelihood using, for example, HMG IS1

		Energy supply (Watt)	Quality of supply / Voltage variation (over-/ under-voltage)		
HIGHLY CRITICAL	>5 MW	> 12% > 230 V | > 8% < 230V	more than 50% population of Wunsiedel supply area affected (>10.000 customers)	critical infrastructures beyond SWW supply area affected	
CRITICAL	500 kW - 5 MW	10% to 12% > 230 V | 6% to 8% < 230V	from 25% to 50% population of Wunsiedel	critical infrastructures in SWW	
HIGH	50 - 500 kW	5% to 10% > 230V | 4% to 6% < 230V			
MEDIUM	5 - 50 kW	2% to 5% > 230V | 2% to 4% < 230V			
LOW	<5 kW	< 2% +/- 230V			

Information object (Integrity Attacks)	Cardinality (Scale of Attack)	Voltage variation (over-/ under-voltage)	Populati
Setpoint command to DER (Figure 31)	One DER on bus 47 is effected	MEDIUM	n/a
Setpoint command to several DERs	Subset of DERs are effected	MEDIUM	n/a
Tap (Down) setting command to OLTC (Figure 34)	One substation is effected	HIGH	n/a
Tap (Up) setting command to OLTC (Figure 35)	One substation is effected	CRITICAL	LOW
Tap setting command to OLTC *and* DER setpoints commands (Figure 36)	One substation and all DERs are effected	HIGHLY CRITICAL	LOW



Conclusions

- The use of co-simulation can be used to examine in detail the effects of cyber-attacks to different information assets
  - However, there is a significant implementation overhead – will operators implement simulations in practical settings?
  - It may prove to define a set of well-established reference cases, which could be examined in detail and published for others to consider in the context of their local environment
- The ontology-based tool support for threat identification enables complex analyses that would not have been possible
- Advanced Persistent ***Cyber-Physical*** Threats are likely to become more prevalent and sophisticated
- Enabling **situational awareness** and **resilience** is critical

EU FP7 Programme Contract No. 608224

Questions

Website

https://project-sparks.eu

Follow Us

@eusparks

Email

paul.smith@ait.ac.at

Telephone

+43 (0) 664 883 90031

EU FP7 Programme Contract No. 608224