

MODELLING AND VALIDATING SECURITY REQUIREMENTS

for Resilient Critical Infrastructures

Paul Smith

paul.smith@ait.ac.at

AIT Austrian Institute of Technology
Center for Digital Safety and Security



CRITICAL INFRASTRUCTURE COMPLEXITY INCREASES

Technology

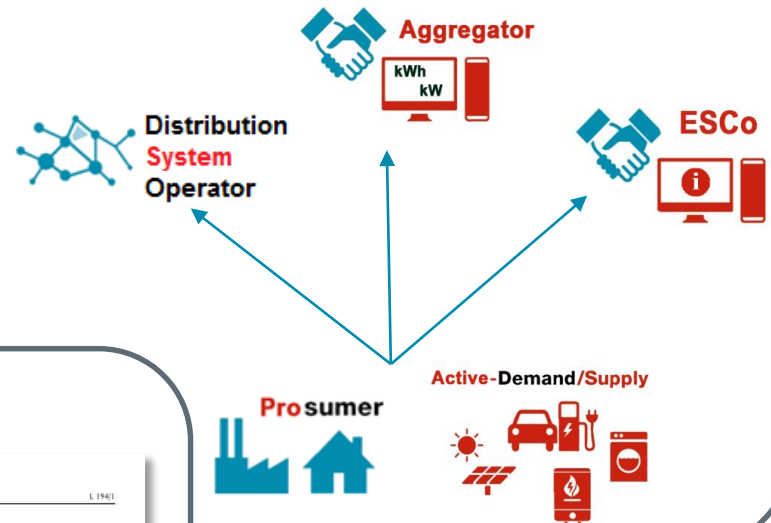


Cloud Computing

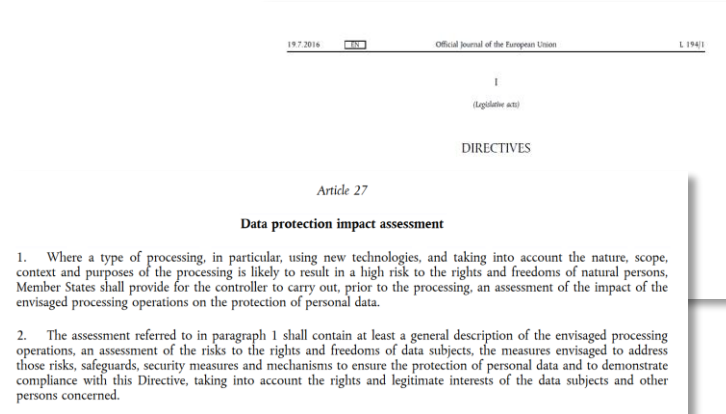


Internet of Things

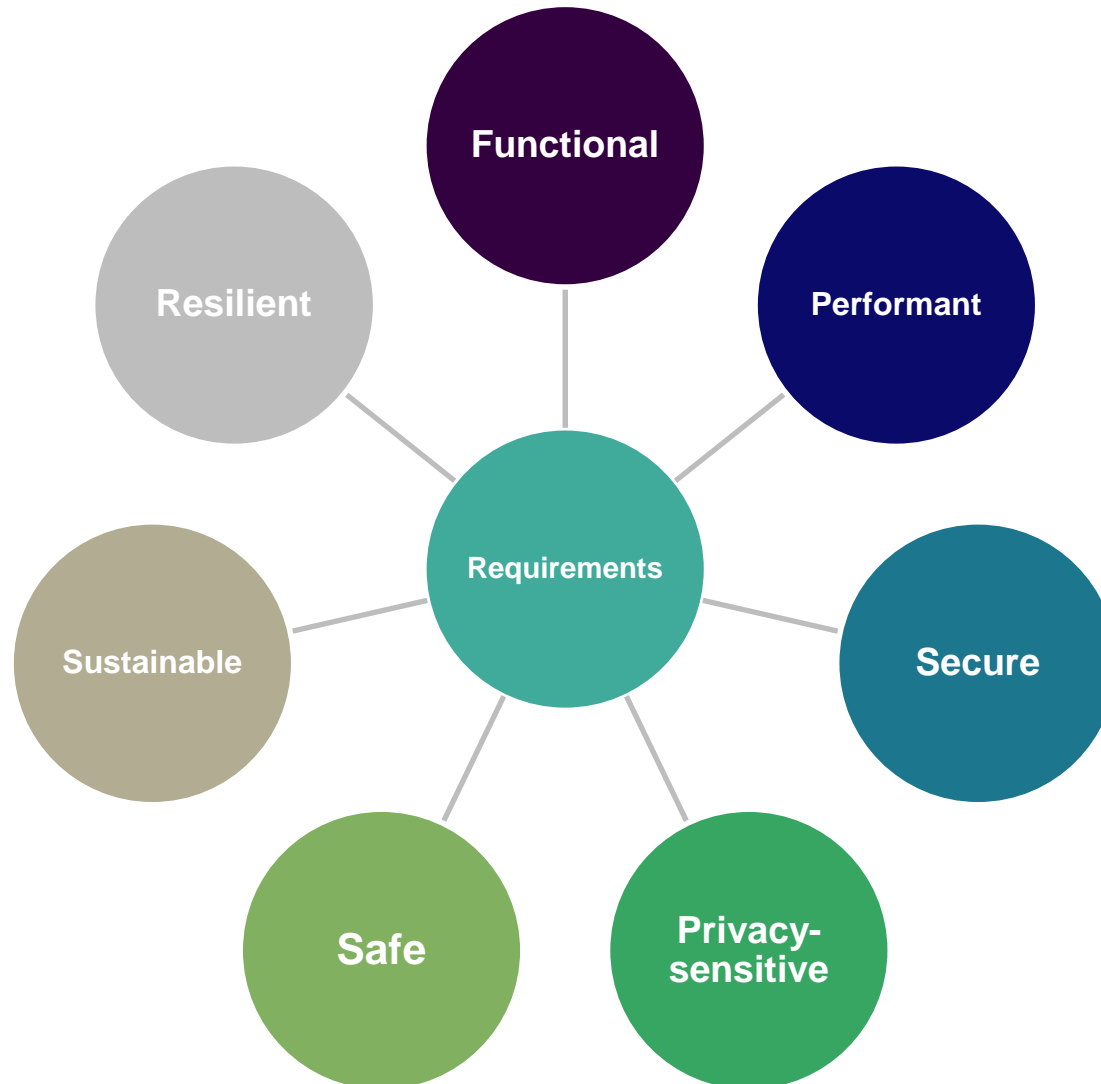
Stakeholders



Legal and Regulatory



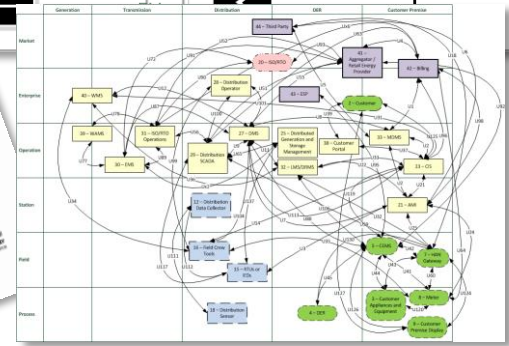
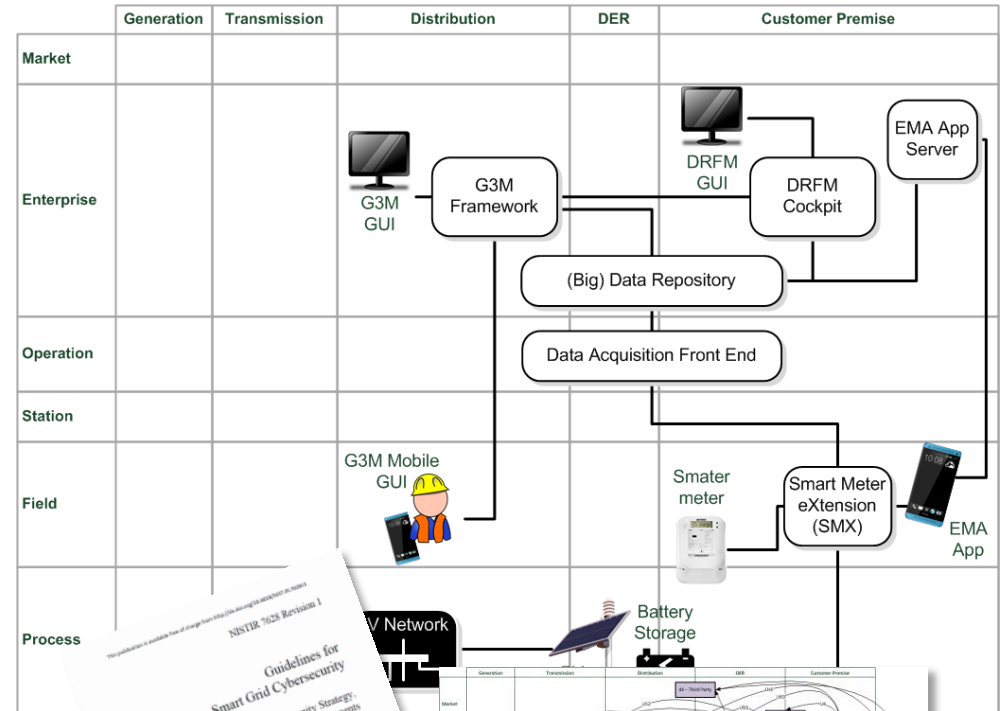
REQUIREMENTS AND TENSIONS



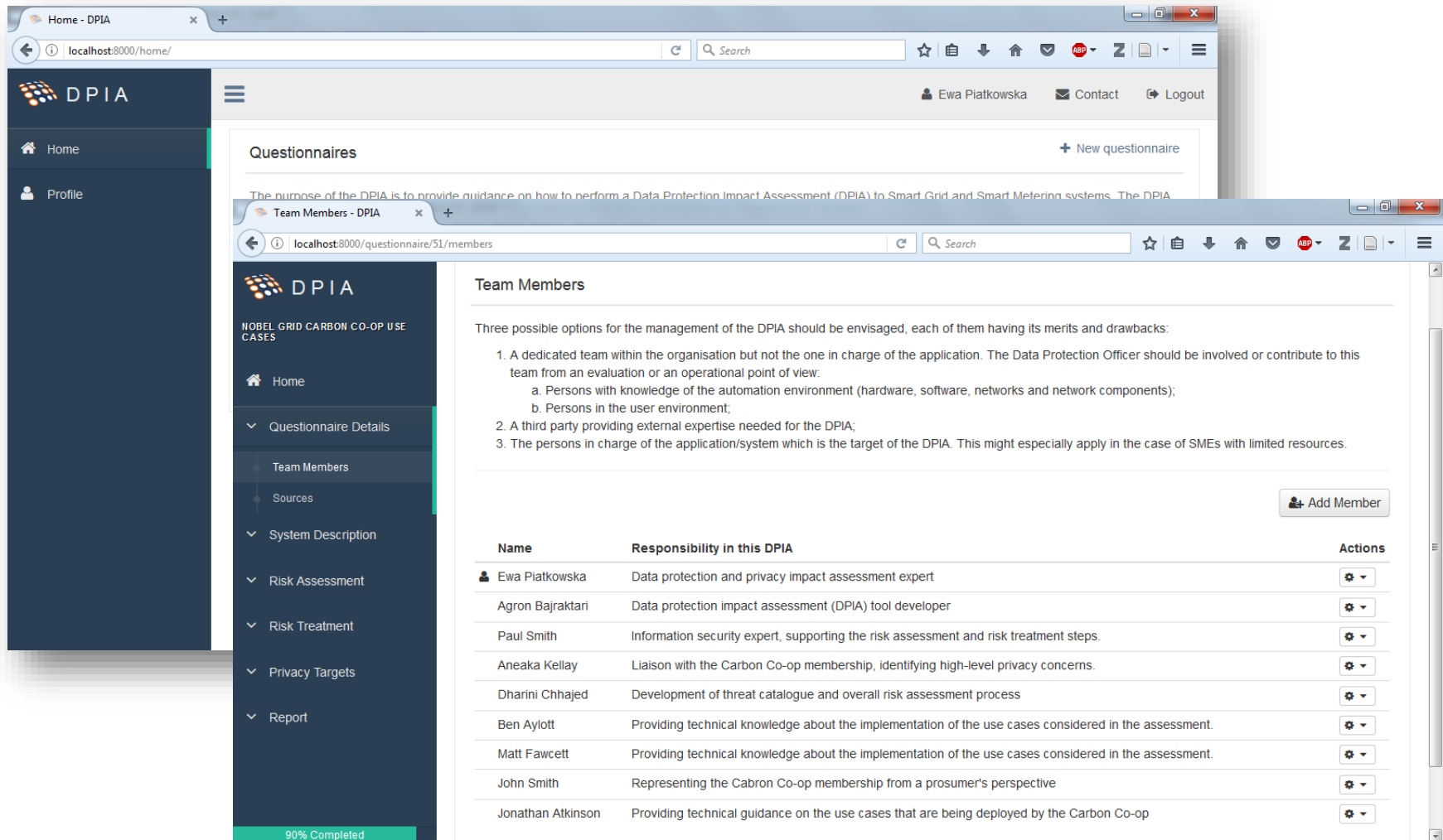
MODEL-DRIVEN SECURE ARCHITECTURE SPECIFICATION



Bundesministerium für Verkehr, Innovation und Technologie



DATA PROTECTION IMPACT ASSESSMENT



The screenshot shows a web application interface for a Data Protection Impact Assessment (DPIA). The top navigation bar includes the DPIA logo, a search bar, and user information for Ewa Piatkowska. The main content area is divided into two browser windows. The first window, titled 'Home - DPIA', shows a 'Questionnaires' section with a 'New questionnaire' button and a brief description of the DPIA's purpose. The second window, titled 'Team Members - DPIA', shows the 'Team Members' section for a specific questionnaire. It includes a list of three management options and an 'Add Member' button. Below this is a table listing team members and their responsibilities.

Questionnaires

The purpose of the DPIA is to provide guidance on how to perform a Data Protection Impact Assessment (DPIA) to Smart Grid and Smart Metering systems. The DPIA

Team Members

Three possible options for the management of the DPIA should be envisaged, each of them having its merits and drawbacks:

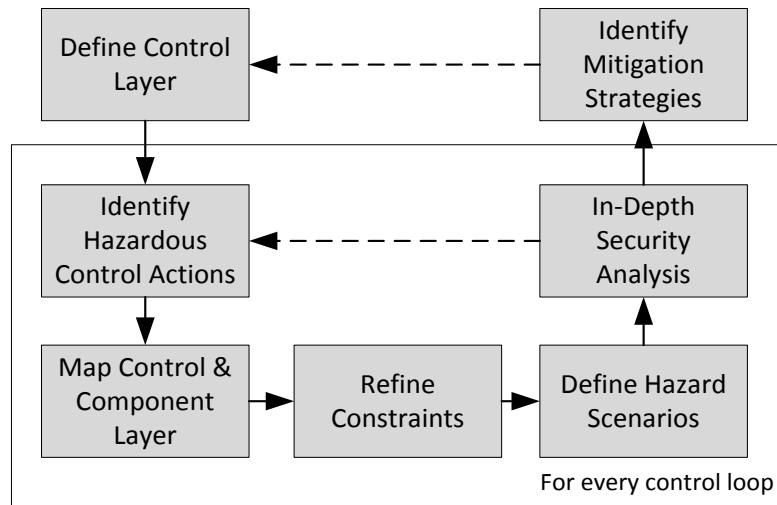
1. A dedicated team within the organisation but not the one in charge of the application. The Data Protection Officer should be involved or contribute to this team from an evaluation or an operational point of view:
 - a. Persons with knowledge of the automation environment (hardware, software, networks and network components);
 - b. Persons in the user environment;
2. A third party providing external expertise needed for the DPIA;
3. The persons in charge of the application/system which is the target of the DPIA. This might especially apply in the case of SMEs with limited resources.

[Add Member](#)

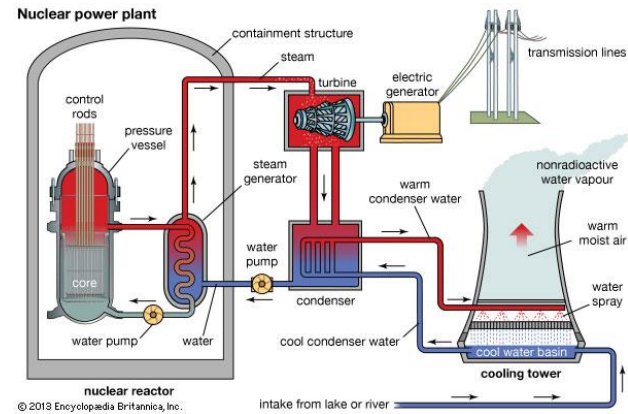
Name	Responsibility in this DPIA	Actions
Ewa Piatkowska	Data protection and privacy impact assessment expert	
Agron Bajraktari	Data protection impact assessment (DPIA) tool developer	
Paul Smith	Information security expert, supporting the risk assessment and risk treatment steps.	
Aneaka Kellay	Liaison with the Carbon Co-op membership, identifying high-level privacy concerns.	
Dharini Chhajed	Development of threat catalogue and overall risk assessment process	
Ben Aylott	Providing technical knowledge about the implementation of the use cases considered in the assessment.	
Matt Fawcett	Providing technical knowledge about the implementation of the use cases considered in the assessment.	
John Smith	Representing the Carbon Co-op membership from a prosumer's perspective	
Jonathan Atkinson	Providing technical guidance on the use cases that are being deployed by the Carbon Co-op	

90% Completed

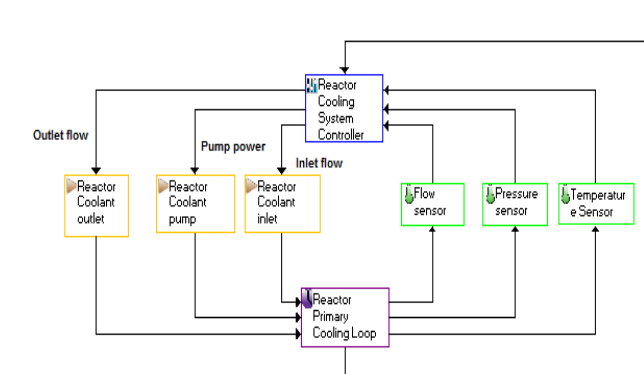
SAFETY AND SECURITY CO-ANALYSIS



STPA-SafeSec Process



Boiling water reactor



CONCLUSION

- Critical infrastructures are becoming increasingly complex and need to address a wide-range of potentially conflicting requirements
- Model-driven systems engineering can be used to support the design and validation of critical infrastructures in order to address these requirements
 - Up-front investment with long-term benefit
- AIT has extensive experience modelling systems to address requirements for
 - Security
 - Privacy and data protection
 - Safety and security
 - Risk management

THANK YOU!

Paul Smith

paul.smith@ait.ac.at

