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

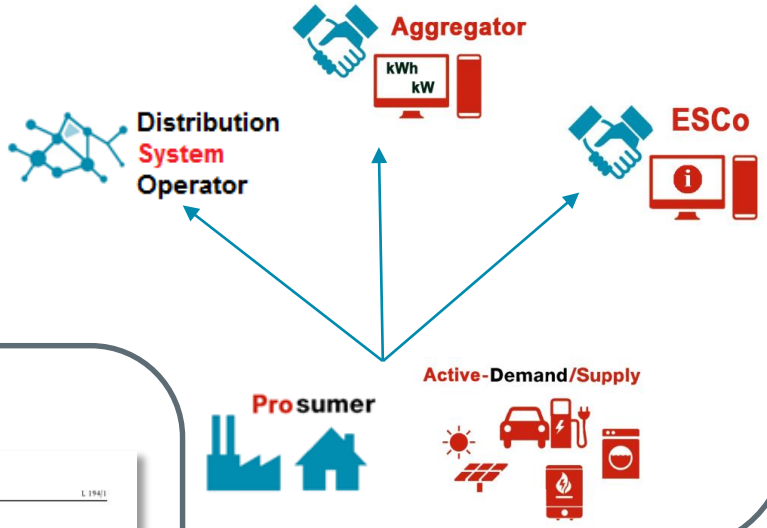
CRITICAL INFRASTRUCTURE COMPLEXITY INCREASES

Technology

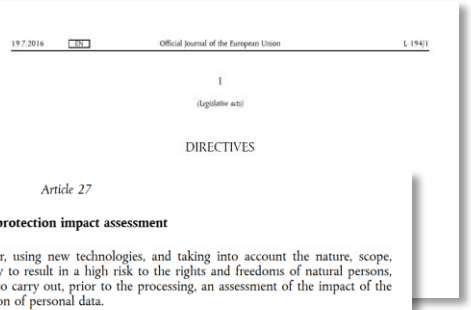
Cloud Computing

Internet of Things

Stakeholders



Legal and Regulatory



19.7.2016 EN Official Journal of the European Union L 194/1

I

(Legislative acts)

DIRECTIVES

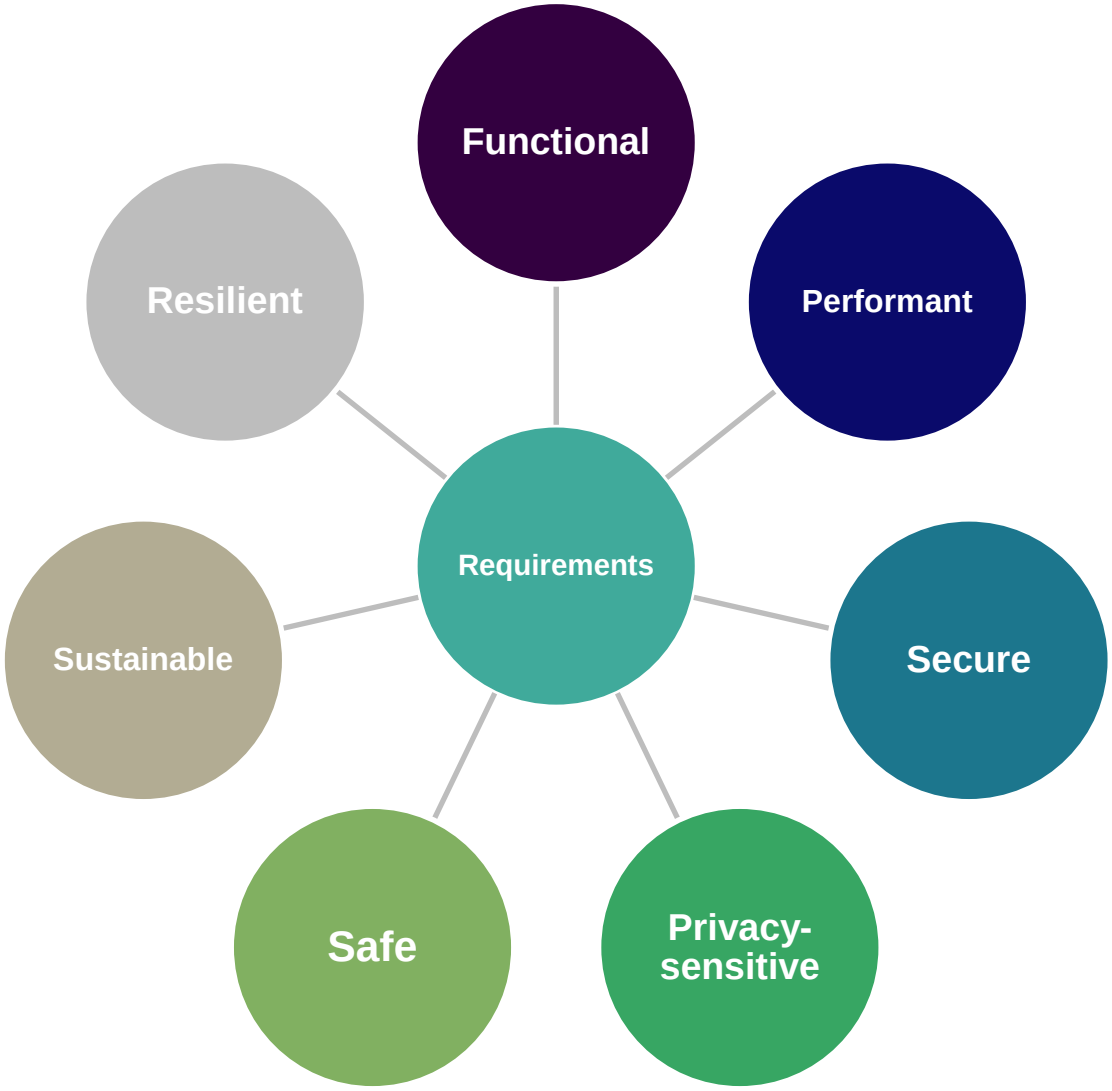
Article 27

Data protection impact assessment

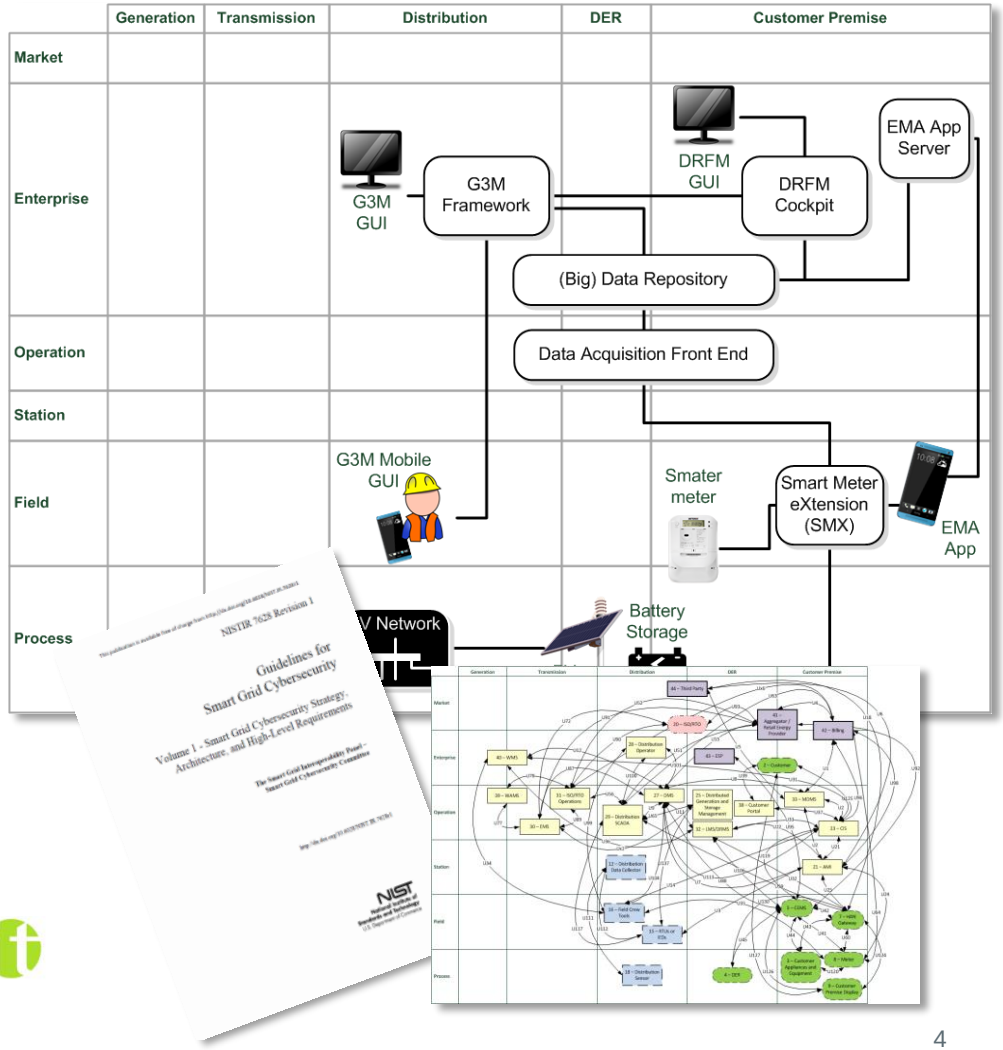
1. Where a type of processing, in particular, using new technologies, and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, Member States shall provide for the controller to carry out, prior to the processing, an assessment of the impact of the envisaged processing operations on the protection of personal data.

2. The assessment referred to in paragraph 1 shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Directive, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

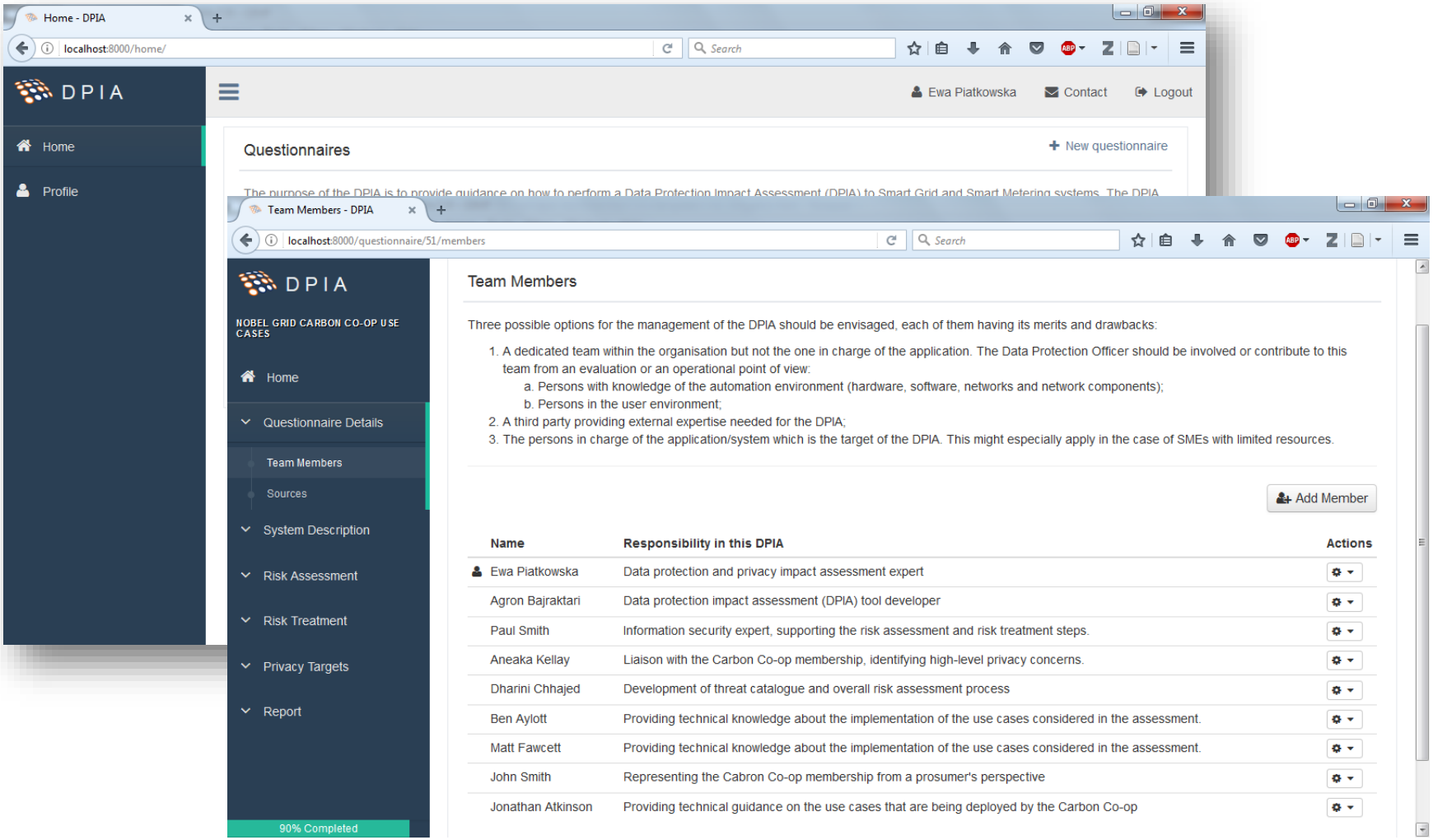
REQUIREMENTS AND TENSIONS



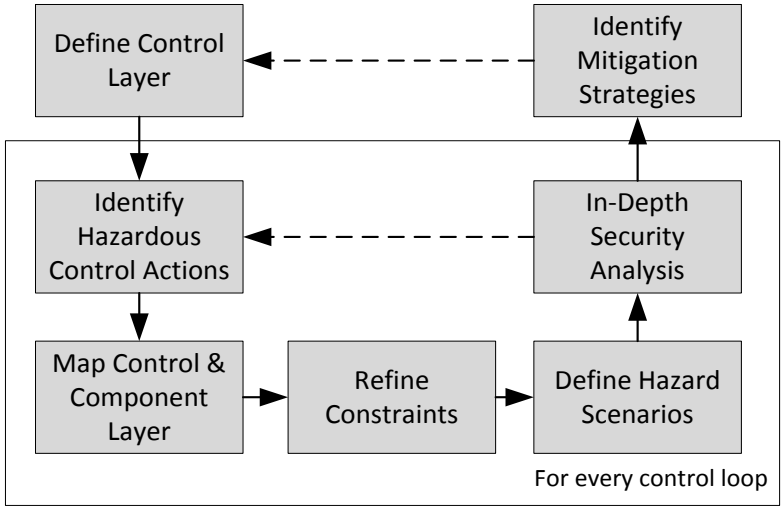
MODEL-DRIVEN SECURE ARCHITECTURE SPECIFICATION



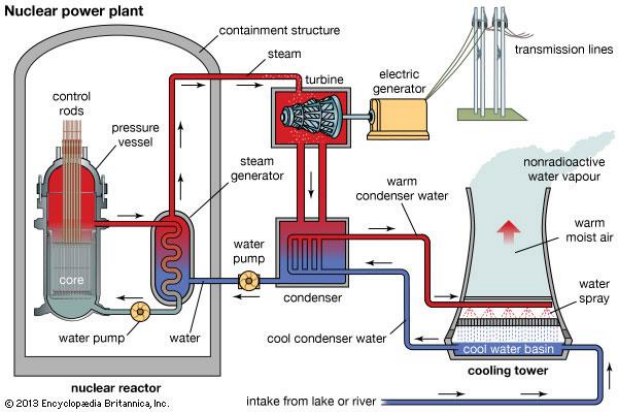
DATA PROTECTION IMPACT ASSESSMENT



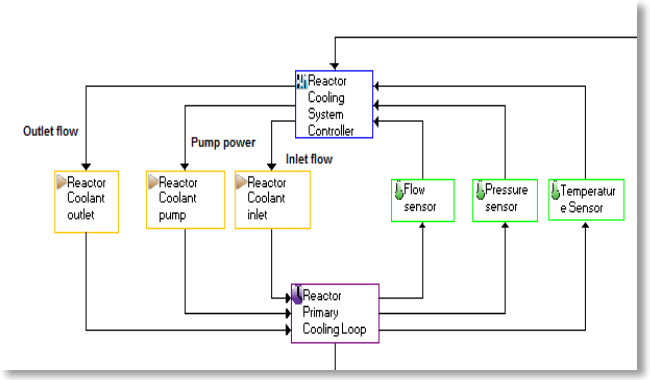
SAFETY AND SECURITY CO-ANALYSIS



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