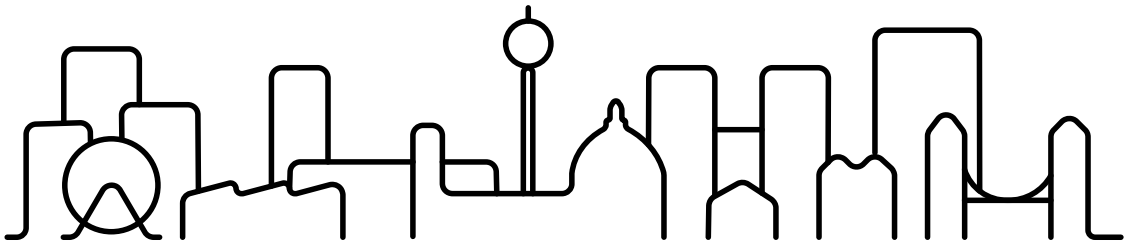
Improving the Robustness of Urban Electricity Networks

Andrea Ceccarelli

Department of Mathematics and Informatics
Università degli Studi di Firenze
Florence, Italy



irene : facts and figures

JPI- Urban Europe http://jpi-urbaneurope.eu/

duration: October 2014 – March 2017

volume: 160 PM

budget: 1.419 k€

No	Organisation	Country
1 Coordinator	Forschungszentrum Telekommunikation Wien - FTW	Austria
2	Ethos VO Ltd. (ETHOS)	U.K.
3	University of Twente (UT)	Netherlands
4	Università degli Studi di Firenze (UNIFI)	Italy
5	Queen Mary University of London (QMUL)	U.K.

Smart Grid and Smart Cities

The **Smart Grid** is an electricity network that can [...] ensure economically efficient, sustainable power system with [...] **security** of supply and **safety**.

M/490 EN - Smart Grid Mandate - Standardization Mandate to European Standardization Organizations (ESOs) to support European Smart Grid deployment

Smart Cities [...]. Enhancing [sustainability, economic development and a high quality of life] can be achieved through [...] **ICT infrastructure**.

https://ec.europa.eu/digital-agenda/en/content/defining-smart-cities

Overall goal and expected outcome

Overall goal

– Enable a highly robust and highly available power supply for future **smart city** scenarios

Expected outcome

Integrated **collaboration framework** *(and tool) that allows cities for different faults/attack scenarios to collaborate with their stakeholders and to evaluate the efficiency of attack countermeasures*

irene anticipated results - 1

Collaboration framework for city planners, stakeholders, DNOs to

- support secure development of the smart grid
- guide the planning/deployment of Smart Grid functions needed to optimize power availability for critical infrastructure.

It includes supporting tools to:

- understand minimum operational power requirements
- energy prediction
- propose mitigation measures as managed decentralization

irene anticipated results - 2

Identify security threats and their impacts on critical infrastructures, including

- **Dependencies** between infrastructures (cascading effect)
- **Root causes**, profiling of the potential attackers (motivations, funding, objectives, skills, etc.), **societal impact** of attacks
  - with the ultimate objective of building an attack threats databases

irene anticipated results - 3

Assessment of the mitigations based on modelling for different scenarios, including:

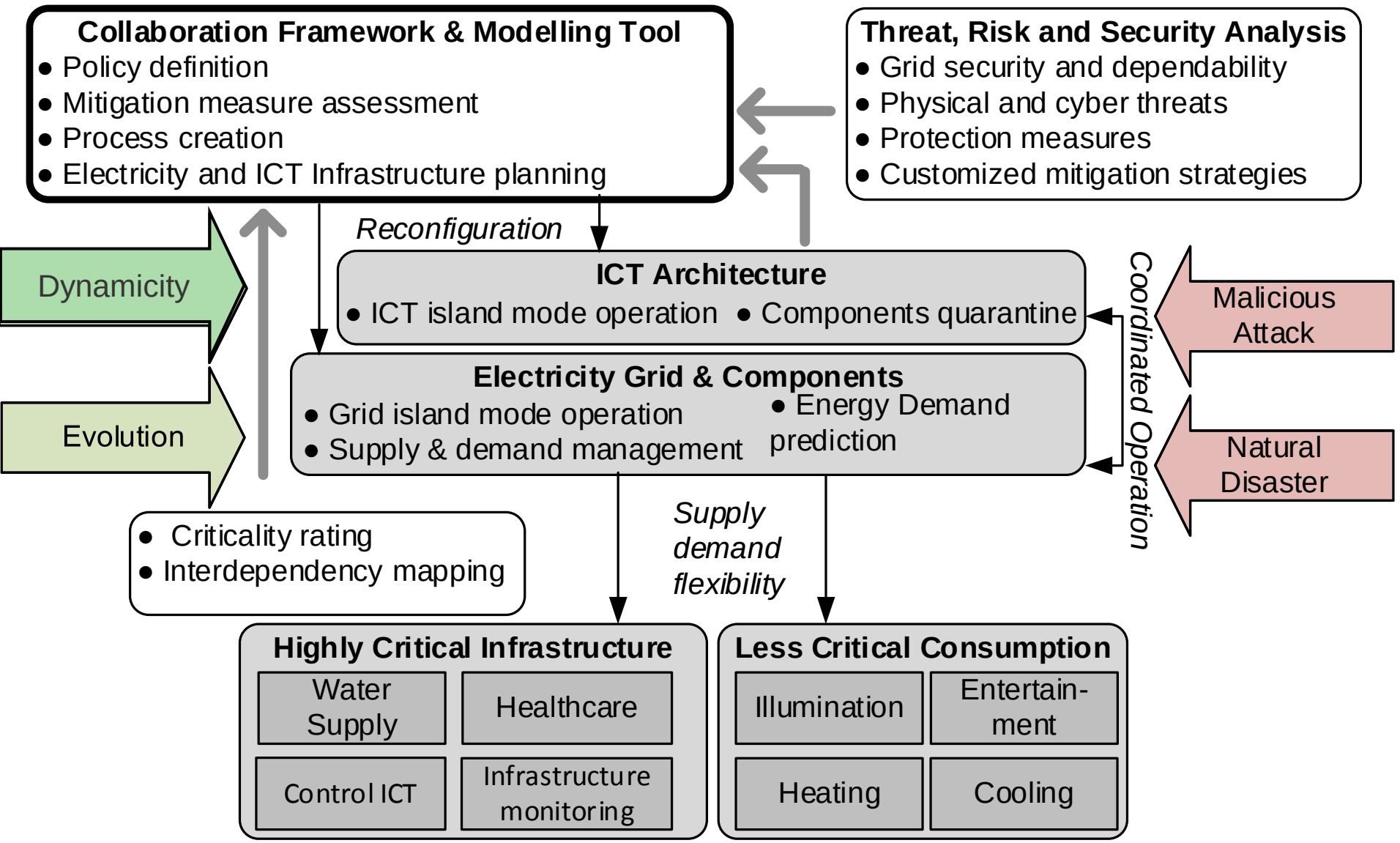
- different **grid architectures** and impact of **attacks**
- provisioning of **limited electricity** resources to most **critical infrastructures** and vulnerable citizens
- procedures and incentives to allow increased power availability for critical infrastructures

IRENE anticipated results - 4

Result evaluation methods based on (serious) gaming workshops

- walk with stakeholders through smart city evolution, disaster scenarios … using the methods and tools developed by IRENE

The irene approach



Some details on an ongoing activity – threats identification and classification

Investigate:

- threats as cyber-security vulnerabilities that result from the **interconnection of previously unconnected grid system parts**
- the inclusion of **new sensor and actuator devices** in the Smart Grids

- Input is the use cases (consumers, cities, Regulators, DNOs, IoT, ...) defined from **PEST** analysis of four possible "future" of Smart Cities

Just few words on the four "future"

	Low smart	High smart
Regulated	No change *(mostly) status quo* *It is the departure point*	Constrained response *Coordinated city lobbying; regulatory price controls; incentives for DNOs to innovate*
Free market	Best endeavours *Increasing pressure towards market liberalization; proliferation of independent DNOs and energy service companies;* *difficulties for city to create the necessary collaborative frameworks*	Freedom to act *Increase competition responding to the market as it evolves;* *cities can be relevant actors in both energy generation and supply*

Threat identification in evolutionary Smart Grids – the approach

IRENE should consider that a smart grid is the result of different evolution steps and support such evolution

Describe the security challenges that arise due to the *introduction of new sensors and the connection of new components*

- We propose to apply the threat analysis to a "story" of the Smart Grid
  - new assets are progressively introduced

(very brief) Methodology overview

For each step of the story, we conduct a risk assessment process (NIST SP800-30) aimed to detect

- new additional threats (structural and due to emergent behaviours)

> A phenomenon of a whole at the macro-level is **emergent** if and only if it is new with respect to the non-relational phenomena of any of its proper parts at the micro level.

This will provide the threats to assess the Collaborative Framework at later stages of the project

Conclusion: irene action plan

- Define scenario, requirements and a **collaborative framework**
- Map threats, attackers profiles and **societal impact of attacks**
- Design of **system architecture** to control supply and demand in an urban electricity grid
- **Security decision supports** based on models of the different settings and mitigation methods
- Evaluation via (serious) **gaming workshops**

THANK YOU for your attention