Improving the robustness of urban electricity networks
IRENE

D5.2 – Evaluation method design, evaluation of IRENE methods, collaboration framework and modelling tool

Document version: 1.5
Document status: Draft
Project Document Date: 13/04/2017
Workpackage Contributing to the Project Document: WP5
Dissemination level: confidential/public

Author(s):
Eng Tseng Lau, Michael Chai, Yue Chen (Queen Mary University of London)
Alexandr Vasenev, Dan Ionita, Roel Wieringa, Lorena Montoya (University of Twente)
Andrea Ceccarelli, Tommaso Zoppi, Andrea Bondavalli, Paolo Lollini, Leonardo Montecchi (University of Florence)
Oliver Jung, Sandford Bessler (AIT Austrian Institute of Technology)
Tony Clarke, Edward Lambert (Ethos)

Table of Contents

LIST OF FIGURES

LIST OF TABLES

1 EXECUTIVE SUMMARY

The purpose of this WP5-D5.2 deliverable (Evaluation method design, evaluation of IRENE methods, collaboration frameworks and modelling tool) of the project IRENE is to test and assess the scalability of the methodologies, policies, frameworks and tools via gaming simulations with students and stakeholder workshops. The best practices related to evaluating systems and tools from WP5-D5.1 are put into practice into this deliverable. As a result, it forms basis for designing and studying outcomes of gaming simulations and stakeholder workshops that aim to improve infrastructures.

Stakeholders and students are exposed with disaster scenarios using the methods and tools developed by IRENE. The policies and methodologies developed in WP3 and the tool developed in WP4 will be integrated in the system architectures, together with feedback from the evaluation Work Package (WP5). Quantitative assessment of the dependability and security of the Smart Grids and the interacting infrastructure will be performed using model-based approaches. In addition an assessment of the solutions proposed within IRENE and the quantification of the gained improvements will be performed. The D5.2 will study feedbacks from students, assess scalability of the methods and tools to real-life situations, and report on quantitative assessment of the dependability of microgrids schemes improved during modelling sessions. This will further supports and complements the analysis including evaluations related to dependability and security assessment.

The tasks for this deliverables are:

Task 5.2 Design of IRENE evaluation method
This task involves the design of the method for evaluating the practicability, efficiency and the impact mitigation approaches and policies developed by IRENE.

Task 5.3 Evaluation of IRENE methods, frameworks and tools
This task involves the collection, processing and analysis of the data collected during the gaming and stakeholder workshop activities. The task will produce one deliverable. This deliverable will contain both a statistical analysis of the quantitative data collected during the evaluation as well as a narrative of the qualitative findings.

The organisation structure of this Deliverable is as follows:

Chapter 2 introduces and applies the design of the IRENE evaluation method through the surveyed state-of-the-art in gaming sessions and stakeholder workshops in the IRENE Deliverable D5.1 within WP5 [1]. The Chapter further applies the ‘Evaluation Continuum’ to evaluate the IRENE tools for collaborative grid planning purposes.

Chapter 3 presents the design of the gaming sessions and stakeholder workshops. The design includes several challenges in the grid that have to be addressed/mitigated.

Chapter 4 presents the questionnaire design for the gaming session and stakeholder workshop. The questionnaire design aims to examine the perceptions of IRENE approaches in terms of the degree of efficiency, practicability and impact mitigation.

Chapter 5 & 6 present the evaluation of the gaming simulation and stakeholder workshop respectively. A baseline grid configuration is developed and fellow students and stakeholders are required to undertake collaborative grid planning and further propose several solutions in order to improve the robustness of the ordinary grid structure. IRENE tools are used to simulate the outcome decision proposed by fellow students and stakeholders, along with results, discussions and evaluations of the gaming session and stakeholder workshop.

Chapter 7 describes an approach to evaluate the potential cascading failures and impact of failures across the grid. The approach is able to access the resilience of the grid topology and to identify the parts of the grid that are more vulnerable to cascading failures. The approach further confirms the analysis achieved in the application of the IRENE framework.

Finally, Chapter 8 concludes.

2 DESIGN OF IRENE EVALUATION METHOD

The introduction of renewables and decentralization of the grid structure is a promising approach to future smart grid technology. However, the implementation of smart grids may require more and more stakeholders to be involved in strategic grid management and planning. Stakeholders need to collaboratively improve the robustness and resilience of the grid but with complex consistent and comprehensive procedures. Accounting for robustness, resilience and cost are a complex task related to the management of the electricity grid.

The purpose of this deliverable is to test and assess the practicability, efficiency and impact mitigation approaches, methods and frameworks developed in IRENE to the real-life scenarios, and also the dependability and security assessment of the IRENE toolsets. In order to achieve these students' gaming simulation and stakeholder workshops are planned and organised. The following sections describe the deployment of the methodology as developed in IRENE WP5-D5.1 [1] to further test the IRENE's methods, frameworks and toolsets. This involves the characteristics of the experiments designed, the coordination and controlling of the experiments, as well as the collection, analysis and interpretation of experiment data during the gaming simulation and workshops.

2.1 RESILIENCE AND ROBUSTNESS

The increased interconnectivity and deployment of smarter grids where services are mostly consumed by citizens and critical facilities, as well as the limited amount of storage technology available to store excessive amount of generated energy make energy such a limited resource. The robustness and resilience of the grid can be formulated to evaluate the way to share a limited resource between multiple stakeholders. To find the optimal arrangements, stakeholders need to collaboratively plan an overall grid system. Additionally, for robustness and resilience management it is important for stakeholders to evaluate the improved grid system on possible undesirable events. This is because the enhancing the robustness and resilience may (or may not) incur additional monetary costs.

As provided in [1], four sequential steps are further used in the task of designing the gaming simulation and workshops. The established steps enhance the focusing of resilience analysis through the alteration of certain grid components and the evaluation of alterations by fellow stakeholders and students. The four steps are explained as follows:

- **Step 1:** Electrical grid description (roles of city-level stakeholders, grid topology, the addition/removal of grid components, grid component settings);
- **Step 2:** Identifying the impact of threats, the governed regulation and policies, and exploring alternatives to mitigate the impacts (islanding operation, reduce consumption load, preserve critical loads, mitigate lists of local threats);
- **Step 3:** The 'What-if' analysis (Resilience and monetary) of several scenarios (e.g., normal operation, economic-islanding, short-term outage, long-term-outage, complete grid outage) after Step 2. This step can be looped back to either Step 1 or Step 2, depending the degree of grid component alterations implemented.
- **Step 4:** The evaluation from students and stakeholders. This step can also lead to return to Step 1 (as if the updated evaluations do not produce satisfactory improvements) or the optimal outputs to policy and management actions.

2.2 ROLE OF STAKEHOLDERS

The collaboration of stakeholders is vital for improving the resilience of a complex system, such as an urban grid. As mentioned, the multi-stakeholder approach might account for input from different actors. The lists of stakeholders into the grid collaboration framework as listed in [2] include Municipal authority planner, Distribution Network Operator (DNO), Developers, Critical Infrastructure Operator, Business and Citizen Representative. Their expertise is complementary to account for strategic grid planning. As mentioned in [1], city planner might have significant expertise in daily administrative operations, but not necessarily in the topic of grid planning. In contrast, grid operators that are responsible for day-to-day functioning of the infrastructure, may overlook the importance of particular customers for the proper functioning of the city as a whole. All these stakeholders might account for multiple factors and consider how the introduction of new components can improve the grid functioning in times of outages. Therefore, the multiple collaboration of stakeholder is important.

In designing the stakeholders' collaboration framework in gaming simulations with students, students will be represented as city-level stakeholders (City planner, DNO, and Citizen & Business Representative), to improve the resilience and robustness of the overall grid. Meanwhile, stakeholders with different expertise will be invited to the stakeholder workshop that require them to sit together and collaboratively plan a grid structure that will improve the robustness and resilience of the electricity networks.

2.3 THE EVALUATION CONTINUUM

An 'evaluation continuum' is outlined in the earlier [1] that reflects real-world factors in which the evaluation of a tool for collaborative grid modeling might take place. The evaluation continuum is presented in Figure 2-1:

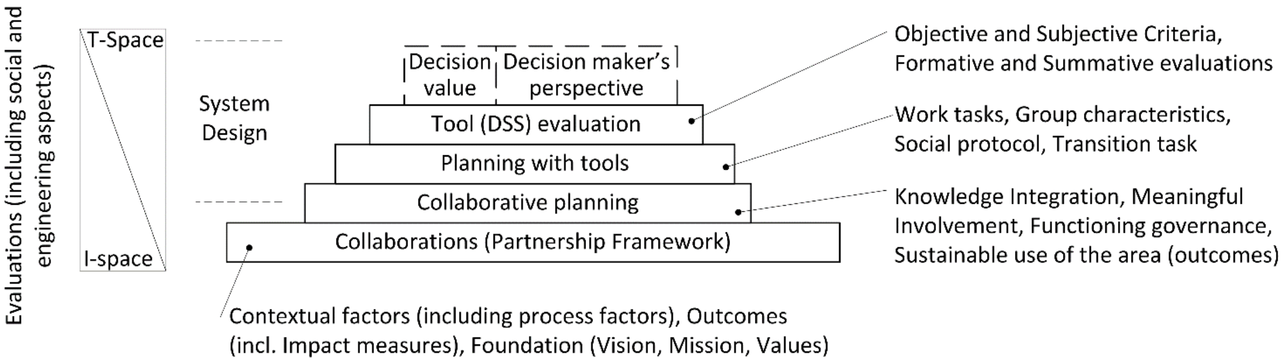


Figure 2-1. Evaluation continuum: evaluation aspects and system design [1].

The evaluation can focus on different aspects: collaborations, collaborative planning as a process, planning with tools as a part of it, and the tool evaluation. The tool evaluation is the decision support system (DSS) evaluation, as the IRENE toolsets support specific decision-making processes. The evaluation of DSS is related to: 1. decision value and 2. Decision maker(s), where the perceptions of decision values are evaluated by decision makers in order to form the desired output of the formulation and process in grid planning strategy.

The evaluation continuum of Figure 2-1 is applied into the IRENE evaluation framework, where the first instance the community partnership framework (students and stakeholders) is applied to enhance the community planning in grid infrastructure problems that could not be solved by single person alone. After that, IRENE toolset is used by fellow students and stakeholders to evaluate the functional requirements of grid improvements. Then, the IRENE toolset is further used to evaluate the performance (resilience, threat mitigation and monetary cost) of different grid component alterations. In other words, the IRENE toolset provides several decisive values that allow the decision makers to summarize the formative presentation of results through the grid analysis using IRENE's methodology, policy and toolset. The important features of several solutions and the anticipated grid planning impacts must introduced during in gaming and workshop sessions. This concerns with which factors that affect the overall grid planning strategy. The continuum aims to provide a reference knowledge base for such a decision. The key performance indicators – resilience, threat mitigation and monetary costs, will account for evaluating decision values that evaluate improvements in urban grid planning.

As mentioned in [1], the system design and system engineering methods are used to complement the validation of evaluation continuum. This is the "comprehensive, iterative and recursive" step where the students and stakeholders provide the grid planning strategy requirements as the initial step. Through the use of IRENE methods, policies and toolsets for grid planning purposes, students' and stakeholders' requirements are linked with IRENE's functional analysis and further validation process are performed to determine the level of acceptance on IRENE's methods, policies and toolsets by students and stakeholders. Use case scenarios are used not only to bridge the validation and evaluation efforts, but also enhance the level of confidences among students and stakeholders of the practicability of IRENE methods, policies and toolsets in real-life scenarios.

Overall, the system design and engineering methods enable students and stakeholders to examine whether the IRENE is applicable for their needs. Additionally, different level of expertise during the gaming sessions and stakeholder workshops are expected. Henceforth, different types of questionnaires to be asked are delegated at the end of the gaming simulation and workshops. For instance, less experienced participants of such sessions can provide their view on how a system operates as a whole ('system test' characteristic). Questions related to the scalability of solutions and the limits of applications of artifacts can be asked to more experienced practitioners. The feedback collected during the gaming and stakeholder workshop sessions will be used for validating the IRENE methods, policies and toolsets. This will consider the evaluation from the perspective of decision makers.

3 GAMING AND WORKSHOP DESIGN

3.1 GAMING SIMULATION – AN INTRODUCTION

Total of three gaming sessions will be conducted with fellow students throughout the IRENE project lifetime. Two sessions will be held at CuriousU summer school at University of Twente (UT) and University of Florence (UNIFI), and one session will be held at Queen Mary University of London (QMUL) on 1st December 2016. The goal of the gaming is to validate the applicability of the IRENE tools, methodologies and policies for improving the robustness of the urban electrical grids.

3.1.1 CuriousU summer school gaming simulation

The three experiments within the two gaming sessions are interrelated as shown in Figure 3-1. The combination of three experiments covers different combinations of possible usage of the iconic modelling language. The focus of the second and the third experiments concerns modelling a system and identifying threats to a system accordingly. Together, the system of experiments deals with both modelling and threat identification steps. With respect to evaluation criteria, the perception of users are studied and amounts of threats identified by different groups are compared. The participants will be provided with both iconic or textual grid elements for *Experiments 1* and *2*. Constructed grid models (either iconic or textual ones) together with a generic threat list forms the input to *Experiment 3*. The configuration of experiments forms a structure that assessed the utility of iconic models, influence of iconicity to model the grid, and its role in identifying threats. Samples of BSc, MSc and PhD students are used. *Experiments 1* and *2* will be conducted at UT during the CuriousU summer school. Later, *Experiment* 3 will take place at UNIFI.

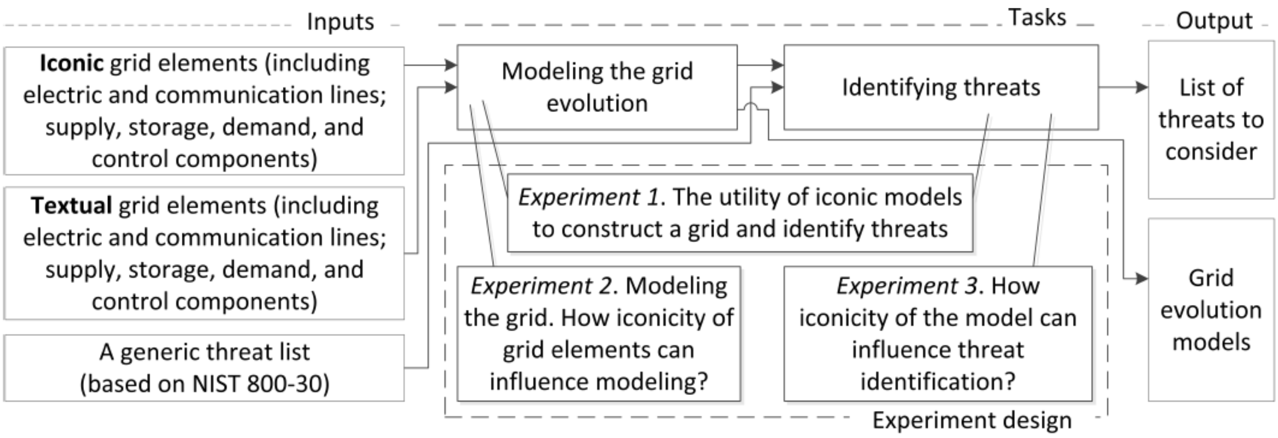


Figure 3-1 Outline and relations between the three experiments [3]

For the CuriousU gaming session, an urban electricity grid will be taken as an example of an adaptive cyber-physical system. The grid model represents city-level grid components (e.g., a power substation, hospital) and connections between them. Such a model consists of: i) nodes as modelling elements that represent the system components and ii) links among the nodes. While students are not representative city planners (and we acknowledge that it somewhat weakens evaluation efforts), the outcomes of the experiments are produced by general cognitive mechanisms which are shared by both groups. Furthermore, students are unlikely to possess knowledge or experience with regard to critical infrastructure modelling tools or threat identification techniques. Therefore, students will be firstly introduced to typical infrastructure components of grids simulating the basic knowledge that city planner stakeholders may have by IRENE researchers.

3.1.2 QMUL gaming simulation

For the gaming session at QMUL, IRENE researchers will be expected to deliver lectures on smart grids to introduce students to major ideas of smart grids, as well as the current issues and challenges. The IRENE toolset will be demonstrated to students to clarify the idea how modelling tools can used to improve the resilience of the overall grid. Student will then further required to discuss what grid updates might be introduced to ensure that a city can withstand a blackout with less negative impact. The aim of this exercise is to investigate how the tool (in the context of collaborative decision making in the situation of uncertainty) can be used to improve the robustness/resilience of a complex urban grid.

3.2 STAKEHOLDER WORKSHOP SESSION - AN INTRODUCTION

The goal of the gaming workshop is to assess scalability of the IRENE methods, policies and tools to real-life situations, using the expertise of the stakeholders. The stakeholder workshop will be held at the Power Networks Demonstration Centre (PNDC) in Glasgow, 24-25th January 2017. IRENE researchers will be expected to deliver lectures on smart grids to introduce stakeholders to major ideas of smart grids, as well as the current issues and challenges. The IRENE software toolset will be demonstrated to stakeholder to clarify the idea of how modelling tools can used to improve the resilience of the overall grid. Stakeholders will be briefed on the changes that the grid might undertake, and they are required to use the IRENE toolset (in the context of collaborative decision making in the situation of uncertainty) to improve the robustness/resilience of a complex urban grid.

3.3 DESIGN METHODOLOGY

3.3.1 CuriousU gaming session

Using the experimental design methodology as outlined in [3]. Here the experiments for the CuriousU gaming simulation and the workshops consider modelling challenges (*MC*):

- *MC1*. To support the reduction of the cognitive complexity required to understand and model a system;
- *MC2*. Top facilitate the threat identification activity using a system model.

The experiments tackle challenges *MC1* and *MC2* as shown in Table 3-1. Also, the table describes the sample populations, modelling targets, and treatments of the three experiments.

	Experiment		
	1	2	3
Challenges tackled	*MC1, MC2*	*MC1*	*MC2*
Sample Population	2 groups of 6-8 participants		2 group of 3 participants
Modelling Target	Infrastructure of the grid on UT campus		Model of UNIFI area
Treatment	Design a prototype using provided software tools		List of threat occurrences in the given scenario

Table 3-1 Characteristic of the experiment for CuriousU summer school [3].

Experiment 1 focused on whether modelling a grid (MC1) and identifying threats (MC2) can be performed within a comparable time interval by using iconic or symbolic modelling constructs. For this, the students will be required to construct a model how they imagine the campus grid (e.g. University of Twente) in 5-10 years. The potential threats to the validity of this experiment is that the pre-existing security or safety knowledge and experimenter expectancy (as the exercise will be supervised) cannot be controlled. However, the treatment and measurement validity will be verified by running the two sessions in parallel provided by each group of students with the same tools (MS Visio) and instructions (handouts). Two supervisors involved in the experiment will be allowed only to answer questions strictly related to the threat lists.

Experiment 2 concerns only with the modelling task and will not cover the threat identification step. It investigates whether iconicity of the modelling language influences the modelling changes in the system and understand-ability (MC1). After performing the task, the participants (students) are required to fill in a questionnaire (subsection 4.1). *Experiment 2* will be conducted under stricter conditions: supervisors are not allowed to assist the modellers. Participants will answer printed questionnaires immediately after the task. However, group dynamics may influence the measurement validity. For instance, one can assume that some participants may have reported lower agreement or perceived the task as more difficult due to intra-group personality or skill mismatches. The experiments do not investigate either of these aspects. Nevertheless, as the groups will be formed from a pool of participants with similar education experiences, it is expect that influences of these aspects are limited. Another threat to validity to the second experiment is that both groups may have worked in a single, although in a very large room. To counter it two supervisors will try to limit cross-group interaction.

Experiment 3 explicitly deals with identifying threats to a grid. It concentrates on how participants relate an iconic or symbolic grid model to a generic threat list. It is designed to understand how the iconicity feature of a model influences the ability of non-experts to perform an effective - complete, precise, and accurate - threat identification task (MC2). After defining two groups of 3 students at UNIFI, the participants will be asked to identify all the possible threat occurrences of a given modelled scenario considering a reference threat list [4]. All participants with the same scenario, described either in iconic or symbolic signs. The independent variable (iconicity of constructs), thus, was thus similar as in Experiment 1 and Experiment 2. See Table 3-1 for details. The obtained threat lists will be compared with a list provided by an expert from UNIFI to assess the completeness of students' lists. Also, the participants are required to fill in a questionnaire (subsection 4.1) after the gaming session.

3.3.2 QMUL gaming and PNDC stakeholder workshop

Due to the similarities of the design methodology for both QMUL gaming and PNDC stakeholder workshop, such design methodologies are explained under the same subsection.

Similarly, using the experimental design methodology as outlined in [3]. Here the experiments for the QMUL gaming simulation and the PNDC workshop consider challenges (*C*):

- *C1*. To support the increased population by adding/removing grid components within the grid model;
- *C2*. To support the failure/outage occurs within the grid elements where:
  - *C2a*. To support single failure within single point/node of grid architecture;
  - *C2b*. To support the complete grid outage in the entire grid architecture;
- *C3*. Towards decarbonisation.

For the purpose of evaluation, an example of urban city is taken as the central theme of the gaming simulation and workshop. The urban grid represents city-level grid components (e.g. mid-scale power stations, small-scale local generations, critical infrastructures such as hospitals) with electrical connection line connecting generation and consuming side. Then, assuming the future case the city grows with increased populations. This accounts the need to modify the existing urban grid architecture configurations to adapt to the future grid scenario. The overall characteristics of experiments designed for the gaming and workshop to tackle *C1* and *C2* is presented in Table 3-2 Characteristic of the gaming and stakeholder workshop experiment.

	Experiments	
	QMUL gaming (G)	**Stakeholder workshop (S)**
Challenges	*C1,C2*	*C1, C2, C3*
Sample population	2 groups of 3 participants (students)	3 participants (stakeholders)
Initial grid scenario	Urban city grid	Urban city grid
Treatment	-Change network architecture when city population grows -Change network architecture to improve the overall resilience	-Change network architecture when city population grows -Change network architecture to improve the overall resilience

Table 3-2 Characteristic of the gaming and stakeholder workshop experiment.

Overall, the aim of the experiments are to encourage the collaboration purposes within students and stakeholders to tackle the challenges (*C1*, *C2*) from the initial grid scenario so that the improved grid will deliver desired services in the future. The tool calculates two indicators – resilience coefficients and monetary costs (with or without savings). The resilience coefficient in this paper is computed based on the extents in which the amount of energy demand within consumers are met when there is an outage in the grid [5]. The resilient coefficient is determined as the mean fraction of the demand served for the outage node divided by the overall demand. A grid is robust and resilient when the computed resilient coefficient is high, or is maintained throughout the outage period. The cost savings are determined based on the difference in between the business-as-usual operation of the traditional grid (without capability of islanding, and also without implementation of DGs, energy system storages and renewables), and the alternative operation mode, when DGs, energy storage systems and renewables are activated.

Experiments are carried out for students and stakeholders with and without specific experience on smart grid backgrounds. Additionally, students participating in the gaming simulation are the representative of the stakeholders. Overall some of participants (e.g. students, business and citizen representative) invited were relatively new in smart grid backgrounds. In order to enhance the concept of smart grids within participants and also, to allow validity of the evaluation continuum, participants were firstly introduced to smart grids, as well as the basic grid architecture and components.

After the completion of experiments, participants are required to complete questionnaires individually. Different versions of questionnaires are delegated due to different nature of knowledge and background possessed by students and stakeholders. The questionnaires will typically evaluate the efficiency, practicability and impact mitigation, approaches, policies and toolset developed by IRENE.

3.4 IRENE WORKFLOW IN GAMING AND STAKEHOLDER WORKSHOP

The IRENE open modelling framework which was introduced in IRENE D4.2 of WP4 [6] includes an IRENE toolset that is supported by a workflow, as depicted in [7]. Overall, the IRENE toolset includes the Evolutionary Threat Analysis (ETA), BayesianFAIR, Microgrid Evaluation (MGE), Single Failure Simulation Tool (SILFAST), and Overall Grid Modelling (OGM).

The ETA will be used to evaluate threats from the grid evolutions (e.g. grid infrastructural upgrades) as proposed by students and stakeholders. This will lead to the changes in the number of threats impacting the grids as described by the evolutions. The BayesianFAIR will further allow the numerical threat ranking assessments that will help the students and stakeholders to focus on effective mitigation plans.

The MGE is an event based simulation of interacting the load prediction and its flexibility, along with the optimization models to produce new local control actions that reduces the demand. It is the demand management control mechanism. The SILFAST applies the mid-level topology to identify the overloaded lines due to single line failures. Both MGE and SILFAST will be demonstrated towards fellow students and stakeholders using video presentations of tool simulations.

The OGM is a Graphical User Interface (GUI) based engineering tool for fellow users to manipulate, evaluate and update the existing grid infrastructure, demand prediction and revised policies. The OGM will be used in the gaming and stakeholder workshops to allow the resilience assessment of grid changes in real-time.

In addition to the IRENE workflow, a model-based-evaluation technique that was introduced in [1] will be further applied in this deliverable in order to evaluate the potential cascading failures and impact of failures across the grid. The approach is able to access the resilience of the grid topology and to identify the parts of the grid that are more vulnerable to cascading failures. The approach will validate the analysis achieved in the application of the IRENE framework.

4 QUESTIONNAIRE DESIGN

4.1 QUESTIONNAIRE DESIGNS FOR CURIOUSU GAMING SIMULATION

There will be no questionnaire session in the *Experiment 1* of the CuriousU gaming simulation. For *Experiment 2,* questionnaire session will be conducted where the questionnaire forms by 4 questions to document students' perception of difficulty and success of the modelling task. Questionnaire design asks for a score from 1 to 5 to each question following a psychometric semantic differential scale to reduce acquiescence bias [7].

E2Q1. *"How would you describe the difficulty of the task you just completed?"*
Rate from 1 (Very easy) to 5 (Very Difficult);
E2Q2. *"How satisfied are you with the tools provided to complete the task?"*
Rate from 1 (Not Satisfied) to 5 (Very Satisfied);
E2Q3. *"How would you rate the amount of time it took to complete the task?"*
Rate from 1 (Very little time) to 5 (Too long);
E2Q4. *"How much do you agree with the final version of the model?"*
Rate from 1 (Don't agree) to 5 (Fully agree).

The questions for *Experiment 3* are as follows:

E3Q1. *"How would you describe the diffculty of building the list of threats?"*
Rate from 1 (Very easy) to 5 (Very Diffcult);
E3Q2. *"Was the graphical/symbolic description enough to complete the task?"*
Rate from: 1 (Unnecessary) to 5 (Very Useful);
E3Q3. *"Did you feel that additional software supports were needed?"*
Rate from: 1 (No) to 5 (Yes, I was lost);
E3Q4. *"How would you rate the amount of time it took to complete the task?"*
Rate from: 1 (Very little time) to 5 (Too long);
E3Q5. *"Do you feel that the list you provided is complete?"*
Rate from 1 (Very poor list) to 5 (Very complete list).

4.2 QUESTIONNAIRE DESIGN FOR QMUL GAMING SIMULATION

The gaming simulation (as presented Table 3-2) focused on addressing the challenges *C1* and *C2* using the IRENE's approaches from the initial grid scenario so that the improved grid will deliver desired services in the future. After the gaming sessions, students were asked to fill in a questionnaire formed of 12 questions to document their perception of using the IRENE approaches, the degree of efficiency, practicability and impact mitigation approaches in collaboratively proposing an improved grid solution. Questionnaire design contained the score from 1 to 5 and 1 to 7 through a psychometric sematic differential scale to reduce acquiescence bias [8] and the anonymous-based questionnaire to reduce response bias [7]. The questions were as follows:

G1Q1. *"The main stakeholder role in the workshop?"*
Roles: Municipal authority planner, Distribution Network Operator, Critical infrastructure owner/operator, Business and Citizen Representative groups, other;
G1Q2. *"Please rate your current knowledge on smart grids";*
Rate from 1 (Very low) to 7 (Very high);
G1Q3. *"Please rate the practicability of:*

	Rate from 1 (Very incorrect) to 7 (Very correct);
G1Q3a.	*consumer profile with DSM capability?*
G1Q3b.	*assumption on controlled generations required to balance the demand?*
G1Q3c.	*assumption that the islanded operation is possible during an outage/contingency event?*
G1Q3d.	*assumption on plausible points of disconnected load during the outage/contingency simulation?*
G1Q3e.	*assumptions that IEEE-14 bus can be used in the toolset?*
G1Q3f.	*assumption that some loads are critical?*
G1Q3g.	*assumption that some loads are uninterruptible"*
G1Q4.	*"Please rate the effectiveness of:*
	Rate from 1 (Very ineffective) to 7 (Very effective);
G1Q4a.	*the toolset in addressing the outage?*
G1Q4b.	*the threat assessment within grid components?*
G1Q4c.	*the demand forecast?"*
G1Q5.	*"Please rate the efficiency (speed) of:*
	Rate from 1 (Very inefficient) to 7 (Very efficient);
G1Q5a.	*time needed to run/re-run a simulation?*
G1Q5b.	*time needed to construct/re-construct the grid components?*
G1Q5c.	*time needed to run/re-run a demand forecast?"*
G1Q6.	*"How would you rate the level of:*
	Rate from 1 (Very low) to 7 (Very high);
G1Q6a.	*knowledge required in using the toolset?*
G1Q6b.	*easiness in using the toolset?"*
G1Q7.	*"If you rate the level of G1Q6. As 5 or above, please explain why?"*
	Open-ended-questions;
G1Q8.	*"How understandable is the toolset simulation in:*
	Rate from 1 (Very easy) to 7 (Very hard);
G1Q8a.	*Resilience coefficient;*
G1Q8b.	*Threat assessment;"*
G1Q9.	*"How practicable (realistic) is the toolset simulation in:*
	Rate from 1 (Very unrealistic) to 7 (Very realistic);
G1Q9a.	*Resilience coefficient;*
G1Q9b.	*Threat assessment;"*
G1Q10.	*"How strongly do you agree that the toolset is:*
	Rate from 1 (Completely disagree) to 7 (Completely agree);
G1Q10a.	*practicable for evaluation of urban electricity network?*
G1Q10b.	*fast in providing simulation analysis of urban electricity network?*
G1Q10c.	*useful in addressing the outage in urban electricity network?"*
G1Q11.	*"How strongly do you agree that the grid modelling toolset is useful:*
	Rate from 1 (Completely disagree) to 5 (Completely agree);
G1Q11a.	*as a collaborative decision support system?*
G1Q11b.	*in establishing a collaborative planning framework among stakeholders?"*
G1Q12.	*"What would you suggest to improve the toolset?"*
	(Please provide at least two suggestions).

4.3 Questionnaire design for PNDC stakeholder workshop

The stakeholder workshop (as presented Table 3-2) focused on addressing the challenges *C1*, *C2 and C3* using the IRENE's approaches from the initial grid scenario so that the improved grid will sustain against the increased populations (due to city grows) and decarbonisation in the future. Similar with the gaming simulation design, after the workshop sessions, stakeholders were asked to fill in a questionnaire formed of 11 questions to document their perception of using the IRENE approaches, the degree of efficiency, practicability and impact mitigation approaches in collaboratively proposing an improved grid solution. However, some questions were altered to suit the level of expertise within the stakeholders participated in the workshop. The questions were as follows:

G1Q1. *"What is your main role in your company?"*
Roles: Municipal authority planner, Distribution Network Operator, Critical infrastructure owner/operator, Business and Citizen Representative groups, other;
G1Q2. *"Please rate your current knowledge on smart grids";*
Rate from 1 (Very low) to 7 (Very high);
G1Q3. *"Please rate the practicability of:*
Rate from 1 (Very incorrect) to 7 (Very correct);
G1Q3a. *consumer profile with DSM capability?*
G1Q3b. *assumption on controlled generations required to balance the demand?*
G1Q3c. *assumption that the islanded operation is possible during an outage/contingency event?*
G1Q3d. *assumption on plausible points of disconnected load during the outage/contingency simulation?*
G1Q3e. *assumption that some loads are critical?*
G1Q3f. *assumption that some loads are uninterruptible?"*
G1Q4. *"Please rate the effectiveness of:*
Rate from 1 (Very ineffective) to 7 (Very effective);
G1Q4a. *the tool in addressing the outage?*
G1Q4b. *the demand forecast?"*
G1Q5. *"Please rate the efficiency (speed) of:*
Rate from 1 (Very inefficient) to 7 (Very efficient);
G1Q5a. *time needed to run/re-run a simulation?*
G1Q5b. *time needed to construct/re-construct the grid components?*
G1Q5c. *time needed to run/re-run a demand forecast?"*
G1Q6. *"How would you rate the level of:*
Rate from 1 (Very low) to 7 (Very high);
G1Q6a. *knowledge required in using the tool?*
G1Q6b. *easiness in using the tool?"*
G1Q7. *"If you rate the level of G1Q6. As 5 or above, please explain why?"*
Open-ended-questions;
G1Q8. *"How understandable is the tool simulation in:*
Rate from 1 (Very easy) to 7 (Very hard);
G1Q8a. *Resilience coefficient";*
G1Q9. *"How practicable (realistic) is the tool simulation in:*
Rate from 1 (Very unrealistic) to 7 (Very realistic);
G1Q9a. *Resilience coefficient";*
G1Q10. *"How strongly do you agree that the tool is:*

	Rate from 1 (Completely disagree) to 7 (Completely agree);
G1Q10a.	*practicable for evaluation of urban electricity network?*
G1Q10b.	*fast in providing simulation analysis of urban electricity network?*
G1Q10c.	*useful in addressing the outage in urban electricity network?"*
G1Q11.	*"How strongly do you agree that the grid modelling tool is useful:*
	Rate from 1 (Completely disagree) to 5 (Completely agree);
G1Q11a.	*as a collaborative decision support system?*
G1Q11b.	*in establishing a collaborative planning framework among stakeholders?"*
G1Q12.	*"What would you suggest to improve the tool?"*
	(Please provide at least two suggestions).

5 CuriousU gaming simulation results

The nput to the *Experiments 1* and *2* included lists of i) generic threats to grid components and ii) either an iconic or a symbolic list of grid components to build an urban grid. The latter input was organized as a template in a MS Visio file. In the third experiment, the students were supplied with a list of generic threats and with either an iconic or symbolic model. The provided model was similar in complexity to those obtained during the first two exercises. Iconic modelling constructs are described in [4] and form pairs (icon-name). Some icons are included in Figure 5-1. In the symbolic template, the modelling constructs were presented only by their names (e.g., 'power substation', 'wind farm', and 'hospital'), without icons.

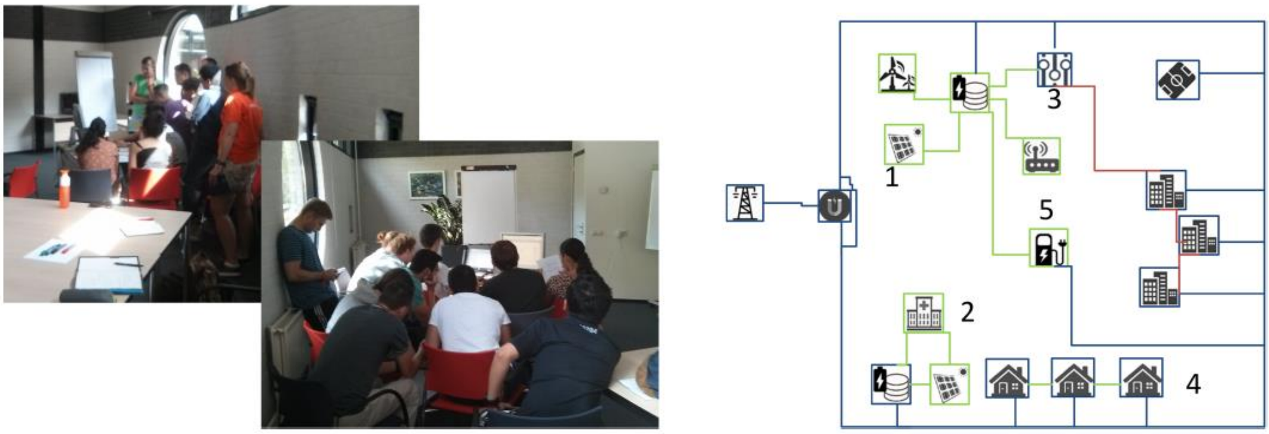


Figure 5-1 Experiment 1 running and the grid structure constructed by one of the groups (numbers in the figure indicate steps when new components are introduced).

5.1 Experiment 1

This experiment aimed to consider the utility of the provided language to model the grid and identify threats to it. The main task was to create grid models (see, e.g., Figure 5-1). Also, participants were asked to identify threats relevant to particular steps of the grid development (using a generic list of possible threats, as described in [4]) and to relate evolution to threat sources (in terms of their capability, intent, and targeting characteristics. This secondary task investigated whether participants can meaningfully relate the grid structure they constructed with the idea of threat modelling. By doing so, it was intended to position the task of threat identification in the context of security engineering. Altogether, this aimed at investigating whether constructing a grid model and identifying threats to it can be feasible for both iconic and symbolic groups.

5.1.1 Experiment 1 – main findings

An interesting finding of this experiment was that the iconic group decided to proceed with modelling the grid in MS Visio directly, while another group started to draft their plans on a whiteboard and paper sheets. It was not anticipated that groups would utilize alternative media when confronted with non-iconic notations. An explanation could be that in this case a lack of iconicity eliminated perceived benefits of using a software-modelling tool, while the flexibility afforded by free-hand drawing led to the use of whiteboard. This potentially points out that the notation of a modelling language can directly impact the modelling process. Both groups were capable to construct grid models and identify a comparable number of relevant threats, despite their previous lack of experience with this task. It suggests that the both representations, as well as the language, can be used for relating components to threat sources.

5.2 EXPERIMENT 2

This experiment concentrated on obtaining initial quantitative data whether modelling using software tools with iconic signs is perceived by non-experts as more understandable compared to modelling with non-iconic signs. Similar to *Experiment 1*, two groups of ten students each were asked to construct models of a smart future university campus. Afterwards, four questionnaires from the group that used iconic signs (Group 1) and seven questionnaires from the other group (Group 2) were collected.

5.2.1 Experiment 2 - main findings

Table 5-1 describes the collected data. The members of Group 2 found the task more difficult (by 64%) and were less satisfied with the tool to model the infrastructure (24%). The *E2Q1* answers from the two groups differ significantly and their confidence intervals do not overlap. It highlights difficulties that the students from Group 2 encountered during modelling the future grid. The replies to *E2Q3* and *E2Q4* are less illustrative: while being comparable, they deviate largely.

Questions	Iconic signs (Group 1)	Symbolic (Group 2)
E2Q1	Avg 2,0 (Std 0,7)	3,3 (0,5)
E2Q2	3,8 (0,4)	2,8 (0,8)
E2Q3	2,5 (1,1)	2,9 (0,5)
E2Q4	3,0 (0,7)	3,0 (1,0)

Table 5-1 Experiment 2: average and standard deviations

5.3 EXPERIMENT 3

The last experiment focused on investigating how an iconic/non-iconic model influences the outcomes of the threat identification task. Two groups each of 3 students participated in the experiment: Group 1 worked with an iconic description of the grid of the scientific complex of UNIFI, while Group 2 worked with a non-iconic (symbolic) version. Provided with a list of generic threats (a subset of threats 7, 10, 17, 18, 19, 21, 24, 29, 31, 37 of the threat list in Appendix B of [4]), all students built a threat list to the system model.

5.3.1 Experiment 3 - main findings

Table 5-2 shows that the amount of valid identified threats is significantly higher for participants who were supplied with the iconic model. In Table 5-2 ‘A’ and ‘B’ letters in the questions distinguish between questionnaires for *Experiment 3a* and *3b*. Group 1 members identified 17, 10, and 19 threats. Members from Group 2 identified 8, 8, and 9 valid threats.

The expert evaluated most of the threats identified by the students as being valid. Some threats, e.g., “conduct physical attacks on organizational facilities”, were commonly identified. Some others threats were identified less often ((for instance, only two out of six students identified “conduct attacks using unauthorised ports, protocols and services”). An explanation can be that some threats that are difficult to understand (and identify), because they require specific technical knowledge.

The Iconic group reported less difficulty (*E3AQ1*) and more satisfaction of the results (*E3AQ5*). Also, they were indicated (*E3AQ3*) that additional software support is needed less, if compared to the symbolic group. Interestingly, the participants didn't anticipate that employing another representation format can result in a more complete list of threats. *E3AQ5* and *E3BQ5* answers of Group 1 both score 3.0. More specifically, there is only a relatively small increase (0.3) in the difference between *E3BQ5* and *E3AQ5* for Group 2.

In summary, all subjects in possession of the iconic model constructed more complete lists of plausible threats compared to their counterparts. It suggests that the threat identification task can benefit from employing an iconic model of a system.

Questions	Iconic signs (Group 1)	Symbolic (Group 2)
Experiment 3a (answers 1 to 5)		
E3AQ1	Avg 3.0 (Std 0)	3.7 (0.6)
E3AQ2	5.0 (0.0)	4.0 (1.0)
E3AQ3	1.3 (0.6)	2.7 (0.6)
E3AQ4	2.7 (0.6)	3.3 (0.6)
E3AQ5	3.0 (1.0)	2.0 (0.0)
Experiment 3b (answers 1 to 5)		
E3BQ1	4.0 (0.0)	3.0 (0.0)
E3BQ2	4.0 (1.0)	4.0 (1.0)
E3BQ3	3.0 (1.0)	3.0 (1.0)
E3BQ4	3.3 (0.6)	2.7 (0.6)
E3BQ5	3.0 (1.0)	2.3 (0.6)
Threat (Amount)		
Identified Threats	15.3 (4.7)	8.3 (0.6)

Table 5-2 Experiment 3: average and standard deviations

5.4 Evaluation of CuriousU gaming simulation

5.4.1 Modelling challenges (MC)

MC1: Reduction of cognitive complexity. While *Experiment 1* showed that both notations can be potentially used to identify threats to a system, *E2Q1* from *Experiment 2* and to a smaller extent *E2Q3* showed that the perceived difficulty of the modelling task slightly decrease when iconic signs are used. Notably, the Iconic group was less satisfied with the tools provided (*E2Q2*). Nevertheless, based on the outcome of the experiments it can be argued that the use of iconic signs instead of symbolic ones lowered the cognitive complexity of the task.

MC2: Facilitating threat identification. In general, non-expert users can identify threats to a system regardless of the model's representation (*Experiment 1*). However, if supplied with a readily made iconic models - in contrast to a symbolic one - they performed better (*Experiment 3*) and considered that such the iconic description was completely enough to perform the task.

5.4.2 Practical implications

As noted in [9], enumerating threats helps system architects to develop realistic and meaningful security requirements. Thus, this paper contributes to the process of working on security requirements at large.

The findings hint at high-level suggestions how to approach eliciting security requirements from stakeholders who are less experienced in modelling. In particular: i) using icons for modelling compared to pure text representation of modelling constructs facilitates comprehension of non-experts; ii) iconic models can assist in identifying potential threats by non-experts. It can be envisioned that an informal iconic model of a system, such as the one shown in Figure 5-1, can facilitate collaboration between stakeholders.

5.4.3 Limitations

Notes on experiments. Some aspects related to the configuration of experiments should be noted. First, it can be possible that outcomes of the experiments were obtained by pure chance. However, it is the consistency of outcomes of several experiments that points out that using icon-based informal modelling language can be useful to identify threats to a complex system. Second, the experiments were focused on assets-threats connections. We did not account for compliance obligations, raw requirements, security requirements, as well as security measures at large. All these aspects are important for security requirements engineering. Investigating the effect of iconicity in connection to other security requirement engineering processes might be a direction for future research. Third, the impact of iconicity may be different if the users only identify threats or model and identify threats as two consequent steps. This aspect, as well as the question how qualitative results can be related to quantitative ones in case of threat identification, deserves further studies.

Model Quality. In this study the semantics (i.e., correctness and completeness) of the models was not investigated in detail. Also, although a RA expert examined the threats identified by students within *Experiment 3*, any claims with regard to the effects of iconicity cannot be mode on the absolute quality of the results. Besides, the "quality" of the identified threats was not part of the evaluation. It is the next steps of the security development process that should account for such a merit. Besides, the study on how iconicity can explicate tacit knowledge (as experts are needed for this task) and creativity (students were provided with a list of possible threats) are not implemented. Still, it can be anticipated that iconic models, due the reduction of cognitive load, can also contribute to these aspects.

Adherence to syntax. Groups with symbolic signs started to freely draw schemes on the whiteboard, thereby reducing possibilities to enforce syntax of the modelling language. Another way used to represent information suited the task (and the audiences) better. However, benefits and limitations of using a specific media were not investigated. Possibly, dual encoding (illustrating the text corresponding to the components next to their graphical representation) can support efficiently employing different media for modelling.

Choice of signs. Symbolic signs were kept as simple as possible, by using only boxes, arrows and colours. However, the complexity and suitability of iconic signs were not evaluated. It is possible that these icons can be simplified, employ more discriminable symbols, and possess more semantic transparency. Also, this research did not concern the modelling constructs themselves, as well as portability of the modelling approach to a large-scale scenario. It does not investigate how having a very large number of iconic representations can negatively impact human comprehension because of, for instance, similarity across potentially similar elements. We can expect that in such cases modelling languages might benefit from grouping elements. Also, the way that the cost of icon design can influence modelling process, was not considered in this paper.

6 QMUL GAMING SIMULATION RESULTS

6.1 THE QMUL GAMING SIMULATION

This section presents the evaluation of gaming simulations conducted at Queen Mary University of London (QMUL) with QMUL students. The goal of the gaming workshop is to validate the applicability of the IRENE tools, methodologies and policies for improving the robustness of the urban electrical grids.

Total of six PhD students were participated in the gaming workshops. In the beginning of the workshop, IRENE researchers delivered mini-lectures on smart grids to introduce students to major ideas of smart grids, as well as the current issues and challenges. Software tools based on WP3 and WP4 were demonstrated to students to clarify the idea how modelling tools can used to improve the resilience of the overall grid.

6.2 THE GAMING EXERCISE

During the gaming session, exercise handouts were given to students (Appendix A). Students formed two groups (Group A & B). Within each group students (running in parallel) represented city-level stakeholders (City planner, DNO, and Citizen & Business Representative), as was suggested by the handouts. These stakeholder roles correspond to professionals who might benefit from using the tool. These professionals need to collaborative decide how to introduce new components or modifying the existing components to improve robustness of the grid. The base configuration of the system architecture used in the exercise is shown in Figure 6-1. The given system architecture was modelled within the IRENE's overall grid modelling tool [10].

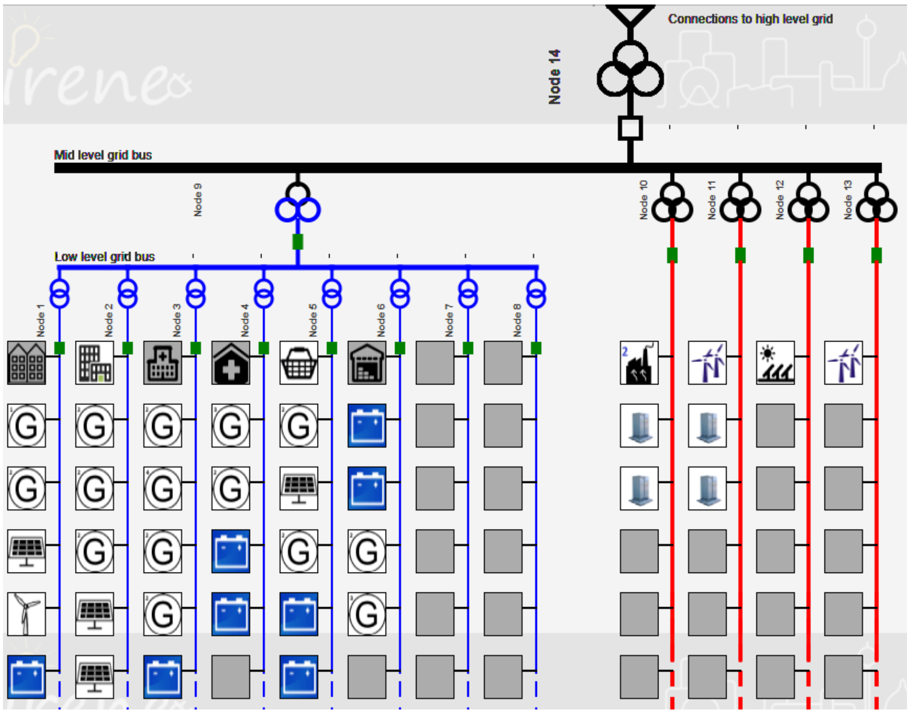


Figure 6-1: The system architecture.

The architecture included a number of city grid components, as shown in Figure 6-1 and listed in Table 6-1:

Node No.	Number of distributed generators		Number of energy stor-age	Profiles included	Populations
	Non-renewa-ble	Renewable			
1	2	2	1	Households	15000
2	3	2	0	Offices	2
3	4	0	1	Hospitals	2
4	2	0	2	Outpatient clinics	5
5	2	1	2	Supermarkets	5
6	2	0	2	Warehouses	5
7	0	0	0	0	-
8	0	0	0	0	-
9	0	0	0	0	-
10	1	0	2	0	-
11	0	1	2	0	-
12	0	1	0	0	-
13	0	1	0	0	-
14	0	0	0	0	-

Table 6-1 Number of distributed generators, energy storages, types of consumer profiles and their populations included

In addition to the description of the grid architecture, student were briefed on the changes that the grid might undertake. It was suggested that the city grows and hence the populations within the city are increased (compared to the data in Table 6-1). Specifically, amount of city components would be as follows: Households = 25000; Offices = 3; Hospitals = 3; Outpatient clinics = 5; Supermarket = 5; Warehouses = 6.

After providing the information, we asked the students to discuss what grid updates might be introduced to ensure that a city can withstand a blackout with less negative impact. The aim of this exercise is to investigate how the tool (in the context of collaborative decision making in the situation of uncertainty) can be used to improve the robustness/resilience of a complex urban grid.

6.3 Solution Suggested by Group A

The collaborative decisions as proposed by Group A, using the base configuration of Figure 6-1 were:

i. Move solar PV from Node 2 to Node 7;

ii. Remove one non-renewable generation in Node 2;

iii. Remove one non-renewable generation and add one energy storage in Node 3;

iv. Add one non-renewable generation in Node 6;

v. Remove solar PV and add one non-renewable generation in Node 1;

vi. Add one non-renewable generator and one energy storage in Node 7.

The new system architecture and the component distributions as proposed by Group A are shown in Figure 6-2 and Table 6-2.

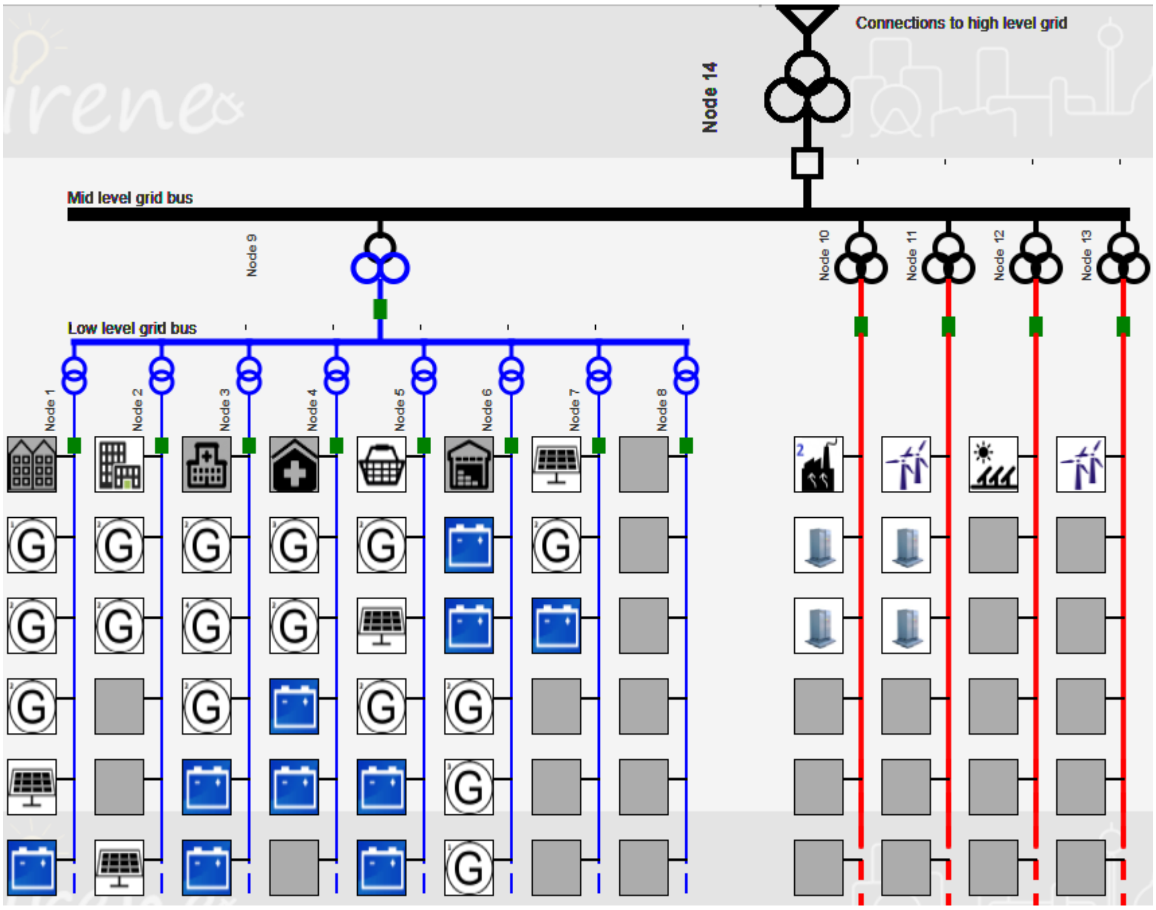


Figure 6-2: The new system architecture as proposed by Group A.

	Baseline			**Group A**		
Node No.	Number of distributed generators		Number of energy storage	Number of distributed generators		Number of energy storage
	Non-renewable	Renewable		Non-renewable	Renewable	
1	2	2	1	3	1	1
2	3	2	0	2	1	0
3	4	0	1	3	0	2
4	2	0	2	2	0	2
5	2	1	2	2	1	2
6	2	0	2	3	0	2
7	0	0	0	1	1	1
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	1	0	2	1	0	2
11	0	1	2	0	1	2

12	0	1	0	0	1	0
13	0	1	0	0	1	0
14	0	0	0	0	0	0

Table 6-2 Number of distributed generators, energy storages, types of consumer profiles and their populations included proposed by Group A

6.4 Solution Suggested by Group B

The collaborative decisions proposed by Group B, using the base configuration of Figure 6-1 were:

i. Add two non-renewable generations in Nodes 7 & 8;

ii. Add one solar PV in Nodes 7 & 8;

iii. Add one small-scale wind turbine in Nodes 7 & 8;

iv. Add one energy storage in Nodes 7 & 8.

The new system architecture and the component distributions as proposed by Group A are shown in Figure 6-3 and Table 6-3.

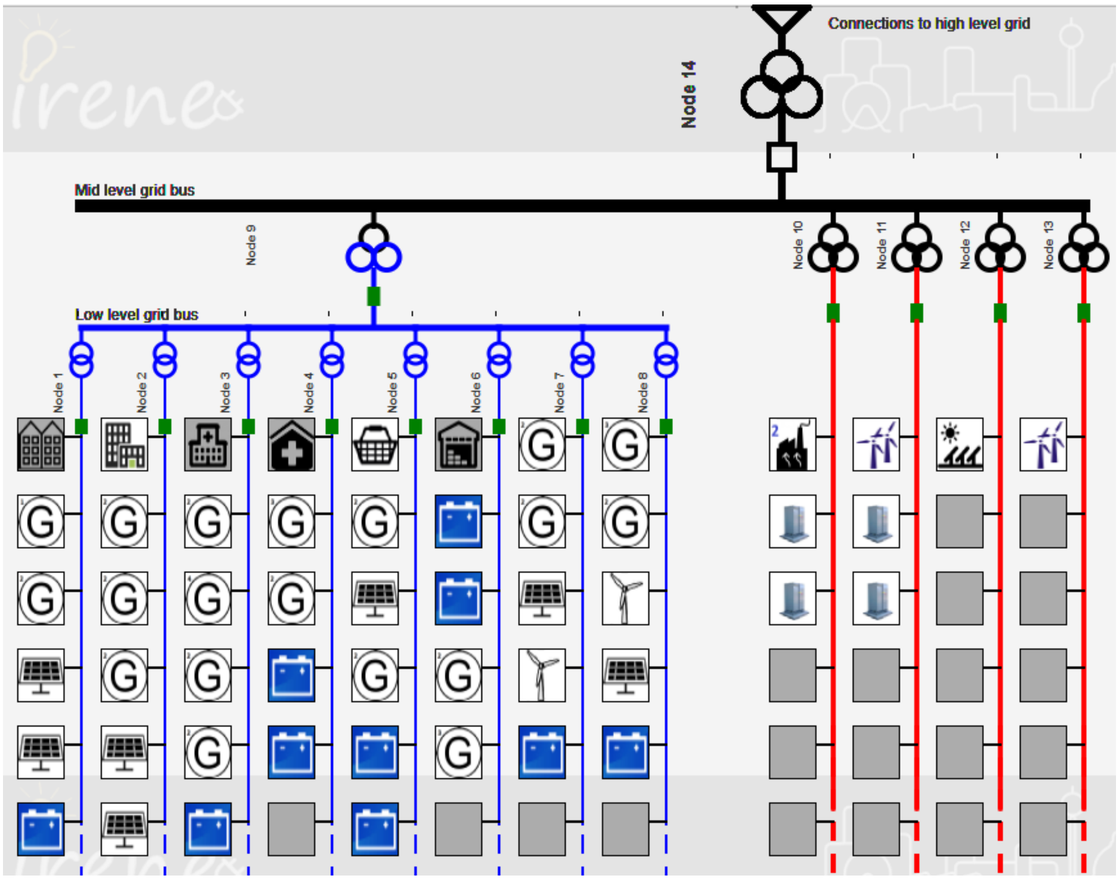


Figure 6-3: The new system architecture as proposed by Group B.

	Baseline			Group B		
Node No.	Number of distributed generators		Number of energy storage	Number of distributed generators		Number of energy storage
	Non-renewable	Renewable		Non-renewable	Renewable	
1	2	2	1	2	2	1
2	3	2	0	3	2	0
3	4	0	1	4	0	1
4	2	0	2	2	0	2
5	2	1	2	2	1	2
6	2	0	2	2	0	2
7	0	0	0	2	2	1
8	0	0	0	2	2	1
9	0	0	0	0	0	0
10	1	0	2	1	0	2
11	0	1	2	0	1	2
12	0	1	0	0	1	0
13	0	1	0	0	1	0
14	0	0	0	0	0	0

Table 6-3 Number of distributed generators, energy storages, types of consumer profiles and their populations included proposed by Group B

Additionally, Group B clarified that all generations should not be fully utilized as more spaces for city development are required.

6.5 Overall Grid Modelling (OGM) tool simulation results

In order to access the effectiveness of the collaborative decisions as made by Groups A & B, normal and failure of grid operations are simulated for each node, and also the entire microgrid level. Failures occur when there is a line-disconnection between the microgrid and main grid level, and also the line disconnection within the microgrid nodes. When there is a line disconnection due to a failure event, the islanding capability is activated to ensure uninterrupted operation during a utility system outage with N-1 compliance [11]. Decisions placed and the performance of the implemented decisions by each groups are compared with the baseline case in terms of resilience coefficients and cost savings [11].

We used the following indicators – resilience coefficients and costs savings in the OGM tool. The resilience coefficient in this case is computed based on the extents in which the amount of energy demand within consumers are met when there is an outage in the grid [11]. The resilient coefficient is determined as the mean fraction of the demand served for the outage node divided by the overall demand.

The cost savings are determined based on the difference in between the business-as-usual operation of the traditional grid (without capability of islanding, and also without implementation of distributed generations, energy system storages and renewables), and the improve operation with the employment of distributed generations, energy storage systems and renewables.

The decisions are simulated using the IRENE's OGM tool and the timeline for the simulation is allowed for 24 hours. The grid with various operating conditions are simulated for the initial grid, Group A & B, as shown in Table 6-4.

Grid operation	Economic islanding capability	Indicators	
		Resilience Coefficient	Cost saving
Normal	✓		✓
Outage 4 hours for single node		✓	✓
Outage 8 hours for single node		✓	✓
Outage 4 hours for grid outage		✓	✓
Outage 8 hours for grid outage		✓	✓

Table 6-4 The grid operation and the indicators applied.

Based on Table 6-4, the "economic-islanding" capability during the normal grid operation is enabled that employs distributed generations, renewable sources and energy storage systems to provide power at times of high electricity price, rather than drawing the electricity from the main grid [11]. Additionally, the different outage configurations (4 and 8 hours) are chosen as it is the main intention to examine the overall robustness of the city in sustaining both the short or longer term of outages.

We also examined the outage in every single node, because we are interested to examine such outage effects on the changes of the supply and demand, as well as the changes in the indicators in the grid level city.

The baseline scenario is also simulated alongside with the modification of the grid components as suggested by Groups A & B, using the new consumer populations: Households = 25000; Offices = 3; Hospitals = 3; Outpatient clinics = 5; Supermarket = 5; Warehouses = 6.

6.5.1 Case 1 – normal operation

In this case, assuming no failure occurs, the normal mode of operation is applied and therefore the "economic-islanding" capability of microgrid is enabled. The cost savings and resilience coefficient achieved for baseline, Group A and B are shown in Table 6-5.

	Baseline	Group A	Group B
Cost savings (£)	1865.39	2112.27	2136.36
Resilience coefficient	0	0	0

Table 6-5 Cost savings and resilience coefficient for normal operations

Based on Table 6-5, the collaborative decisions proposed by Group B achieve higher amount of cost savings than Group A, and also higher than the Baseline scenario. Hence the decision by Group B achieves higher amount of cost savings, particularly for "economic-islanding" normal mode of grid operations. The resilience coefficients are all zeros. This is because the grid is not resilient as normal mode of operation without any outage events are applied in this case. The simulation excludes the addition of installation and maintenance of individual generators.

6.5.2 Case 2 – four hours of outage duration

In the second case, it is assumed that an outage within the microgrid or the entire grid occur at 0900 for the duration of four hours. The "economic-islanding" capability is disabled in the case of outage events. Table 6-6 shows the result of the simulation using the baseline scenario, Group A and B. Overall Group A's collaborative decision promotes highest amount of cost savings than Group B, and also the baseline case. In all cases critical loads were served during the outage events. The computed resilience coefficients are identical.

Outage Node	**Cost savings (£)**			**Resilient coefficient**		
	Baseline	Group A	Group B	Baseline	Group A	Group B
Node 1	208.47	138.98	208.47	0.21	0.21	0.21
Node 2	-94.79	-29.06	-94.79	0.218	0.218	0.218
Node 3	198.33	368.82	198.33	0.242	0.242	0.242
Node 4	211.16	259.30	211.16	0.131	0.131	0.131
Node 5	206.19	125.25	206.19	0.109	0.109	0.109
Node 6	321.80	205.25	321.80	0.007	0.007	0.007
Grid outage	1286.65	1559.54	1558.27	1	1	1
Total savings (£)	2337.81	2628.08	2609.43	-	-	-

Table 6-6 Case 2 - cost savings and resilience coefficient for outage operations. Negative sign indicates additional costs are introduced (no cost savings are achieved).

6.5.3 Case 3 – eight hours of outage duration

In the final case, it is assumed that an outage within the microgrid or the entire grid occur at 0900 with prolonged outage duration of eight hours compared to Case 2. The "economic-islanding" capability is also disabled. Each outage node disconnections is evaluated. Table 6-7 shows the result of the simulation using the baseline scenario, Group A and B. Overall Group B's collaborative decision promotes highest amount of cost savings. The installation of a new energy storage system and also the removal of one of the non-renewable generator in Node 3 as proposed by Group A results in insufficiency of energy supply to match the fraction of demand to be served during the outage in Node 3. The low resilient coefficient as computed in Node 3 by Group A suggests the failed portion of demand (0.252 – 0.15 = 0.105) served in Node 3 during the outage.

Outage Node	Cost savings (£)			Resilient coefficient		
	Baseline	Group A	Group B	Baseline	Group A	Group B
Node 1	310.83	136.55	310.83	0.219	0.219	0.219
Node 2	-189.66	-159.42	-189.66	0.208	0.208	0.208
Node 3	272.31	Invalid	272.31	0.252	0.12	0.252
Node 4	225.49	116.06	225.49	0.132	0.132	0.132
Node 5	234.59	-12.35	234.59	0.106	0.106	0.106
Node 6	546.84	267.97	546.84	0.064	0.064	0.064
Grid outage	1817.43	1850.01	2118.89	1	1	1
Total savings (£)	3217.83	-	3519.29	-	-	-

Table 6-7 Case 3 - cost savings and resilience coefficient for outage operations. Negative sign indicates additional costs are introduced (no cost savings are achieved). Invalid indicates that cost savings are not calculated as the proportions of the demand at the particular node during the outage is not met.

6.6 Evolutionary Threat Analysis (ETA) tool simulation results

Here we list the results of application of the ETA tool on the scenarios that are listed in Section 6.

The first step is to analyse the baseline scenario in Figure 6-1. Looking at the last column of Table 6-9 we can observe how each of the 38 threats occurs on average in 58.18 different parts of the grid (e.g., on average 58 components of the grid are exposed to MiM attacks), with a standard deviation of 62.89. Moreover, on each of the 2211 identified threats in the baseline scenario, 3.14 ± 1.65 high-level mitigation strategies (see [4]) can be implemented to reduce its impact or avoid its happening. Furthermore, in the baseline scenario all the 38 IRENE threats [4] can occur, while 15 of these 38 types of threat can also emerge from the interconnection of previously disconnected components. In particular, we can observe how the IRENE threat 15 “Conduct communications interception attacks.” and the IRENE threat 31 “Incorrect Privilege Settings” emerge in the higher number of cases in this scenario. For example, communications can be intercepted by monitoring the traffic on a given channel.

	Structural	Emerging	Total
Threat Types	36	15	38
Most Frequent Threat	(IRENE 19) Conduct physical attacks on organizational facilities.	(IRENE 31) Incorrect privilege settings	(IRENE 19) Conduct physical attacks on organizational facilities.
	(IRENE 6) Install sniffers or scanning devices on organizational information systems and networks.	(IRENE 15) Conduct communications interception attacks.	(IRENE 15) Conduct communications interception attacks.
Occurrences	(Avg) 42.08 (Std) 39.77	(Avg) 46.40 (Std) 51.01	(Avg) 58.18 (Std) 62.89
Mitigations	(Avg) 2.99 (Std) 1.62	(Avg) 3.09 (Std) 1.14	(Avg) 3.14 (Std) 1.65

Table 6-8: ETA detail for the baseline.

Moreover, the ETA tool is able to perform an evolutionary threat analysis, meaning that it builds a threat list starting from the results obtained at the previous steps. Here, the baseline scenario represents the basic setup of the targeted scenario, while two parallel evolutions of that baseline are proposed by students of Group A and Group B (see Figure 6-2 and Figure 6-3). Therefore, our analysis was split into two parts by considering i) the baseline scenario and the evolution suggested by Group A, and ii) the baseline and the Group B suggestions.

6.6.1 Group A Evolution

Starting from the baseline, all the components (57 buildings and 56 connections) are considered as newly added. The ETA tool identifies 2211 threats from the IRENE threat list that can impact the grid. As highlighted in the first row of Table 6-9, 68.52% of them are structural threats, while the remaining 31.48% emerge due to interconnections among different components of the grid. Considering the evolution of the "*Baseline*" suggested from the students i.e., "*Group A Step*", we can see that 98 structural and 83 emerging threats are removed (-), while 158 and 70 are respectively added (+) to that scenario due to the inclusion of the buildings. Overall, we obtain that the grid at its last evolution stage can be targeted by 2258 threats, 1575 structural and 683 emerging. Compared to the overall number of threats of the baseline, we can assert that this evolution is increasing the total number of threats that are affecting the targeted grid scenario.

Grid Scenario	Components			Structural Threats			Emerging Threats			Threat Stats (%)			
	Buildings	Connections	Tot	Tot	+	-	Tot	+	-	Structural	Emerging	+	-
Baseline	57	56	113	1515	1515	0	696	696	0	68.52	31.48	100.00	0.00
Group A Step	59	57	116	1575	158	98	683	70	83	69.75	30.25	10.10	8.02

Table 6-9: ETA summary for Group A evolution.

With respect to the in-depth results obtained for the "*Baseline*", in the suggested evolution step each threat of the IRENE threat list can occur on average in 59.42 ± 58.11 different places. Moreover, the most frequent threats are the same of the baseline scenario i.e., IRENE threats 19 and 15, which occur respectively in 121 and 119 separate parts of the grid.

6.6.2 Group B Evolution

Considering the same baseline as starting point, that the grid at its last evolution stage as suggested by students of Group B can be targeted by 2595 threats (see Table 6-10). Compared to the overall number of threats of the baseline, we can assert that this evolution is increasing the total number of threats that are affecting the targeted grid scenario.

Grid Scenario	Components			Structural Threats			Emerging Threats			Threat Stats (%)			
	Buildings	Connections	Tot	Tot	+	-	Tot	+	-	Structural	Emerging	+	-
Baseline	57	56	113	1515	1515	0	696	696	0	68.52	31.48	100.00	0.00
Group B Step	67	66	133	1789	274	0	806	110	0	68.94	31.06	14.80	0.00

Table 6-10: ETA summary for Group B evolution.

Looking in detail at the identified threats of the final stage of the grid after implementing the Group B step (see Table 6-11), we point out that all the 38 IRENE threats [4] can occur, while 15 of these 38 types of threat can also emerge from the interconnection of previously disconnected components.

In particular, we can observe how the IRENE threat 15 "Conduct communications interception attacks." and the IRENE threat 31 "Incorrect Privilege Settings" emerge in the higher number of cases in this scenario. For example, communications can be intercepted by monitoring the traffic on a given channel. Looking at the last column of Table 6-11, we can observe how each of the 38 threats occurs on average in 68.28 different parts of the grid (e.g., on average 68 components or group of components of the grid are exposed to MiM attacks), with a standard deviation of 69.76. Moreover, on each of the 2595 identified threats, 2.97 ± 1.53 high-level mitigation strategies (see [4]) can be implemented to reduce its impact or avoid its happening.

	Structural	Emerging	Total
Threat Types	36	15	38
Most Frequent Threat	(IRENE 19) Conduct physical attacks on organizational facilities.	(IRENE 31) Incorrect privilege settings	(IRENE 19) Conduct physical attacks on organizational facilities.
	(IRENE 6) Install sniffers or scanning devices on organizational information systems and networks.	(IRENE 15) Conduct communications interception attacks.	(IRENE 15) Conduct communications interception attacks.
Occurrences	(Avg) 39.55 (Std) 28.31	(Avg) 44.00 (Std) 36.31	(Avg) 68.28 (Std) 69.76
Mitigations	(Avg) 2.94 (Std) 1.41	(Avg) 3.20 (Std) 1.01	(Avg) 2.97 (Std) 1.53

Table 6-11: ETA detail for the Group B evolution.

6.6.3 ETA evaluations

Overall, the two groups depicted evolutions by increasing the number of components with respect to the amount that was defined in the baseline scenario. This leaded to an increase in the number of threats impacting the grids described by the evolutions. Anyway, the statistics related to the average occurrences and the most frequent threats are not slightly changing: the IRENE threats 15, 19 and 31 are still the most common in these topologies. Also, the spread of threats is around 69% structural and 31% emerging for both evolutions.

6.7 EVALUATIONS OF QMUL GAMING SIMULATION

Overall, the gaming exercise was successfully conducted with pros and cons of the grid component alterations within the collaborative decisions made by two groups, in comparison with the baseline case. Additionally, the gaming workshop also noted the extensive collaboration within stakeholders (fellow students) in successfully increasing the robustness of the electricity network that is prone to outage events.

The questionnaire feedback session was administered to fellow students at the end of the workshop (refer Appendix B for the Questionnaire). Outcomes of the gaming session showed that the tasks related to grid update (including the introduction of renewables and changes in the consumption) could be effectively performed in an understandable manner. Results can be compared and a better alternative (w.r.t. some criteria) can be selected. Participants indicated (Q6) that the toolset can be used even without having advanced domain-specific knowledge. Also, one of the participants agreed upon the convenience and the ease of use of the OGM tool where rapid simulation results can be observed.

However, one of the participant outlined the difficulty in understanding the given scenario and demanded more relevant data in order to provide better decisions, rather than the overall grid outlook. Several students also pointed out the data given in order to provide a clearer indication of remodifying the grid components. Still, some additional explanations are needed before using the tool. For instance, the participant indicated that the resilience coefficient was not completely understandable (Q8), as well as some advanced functionalities (namely, threat assessment) of the OGM tool were not clear (Q8). This was due to the insufficient amount of time required to present all the important criteria to fellow students in the workshop.

In summary, the obtained feedbacks and comments are indeed useful not only to improve the usability of the OGM tool, but also to improve the overall understanding of fellow users by providing more descriptions of the grid scenario, data information such as the capacity of generations and demands, and a clearer description of the OGM tool. The improvements will be implemented and such implementations will be further evaluated in the stakeholder workshop.

7 THE STAKEHOLDER WORKSHOP RESULTS

This report presents the evaluation of gaming simulations with stakeholders conducted at Power Networks Demonstration Centre (PNDC), Glasgow. The goal of the gaming workshop is to assess scalability of the IRENE methods, policies and tools to real-life situations, using the expertise of the stakeholders.

Total of three stakeholders were participated in the workshops. In the beginning of the workshop, IRENE researchers delivered mini-lectures on IRENE overall project structures to introduce stakeholders to major ideas of the current issues and challenges, as well as the IRENE aims and objectives. Software tools based on WP3 and WP4 were demonstrated to stakeholder to clarify the idea how modelling tools can used to improve the resilience of the overall grid.

7.1 THE WORKSHOP EXERCISE

During the workshop session, exercise handouts were given to stakeholders (Appendix B). They are represented as one of their stakeholder roles (City planner, DNO, and Citizen & Business Representative). The stakeholders need to collaborative decide how to introduce new components or modifying the existing components to improve robustness of the grid. The base configuration of the system architecture used in the exercise is shown in Figure 7-1. The given system architecture was modelled within the IRENE's overall grid modelling tool [10].

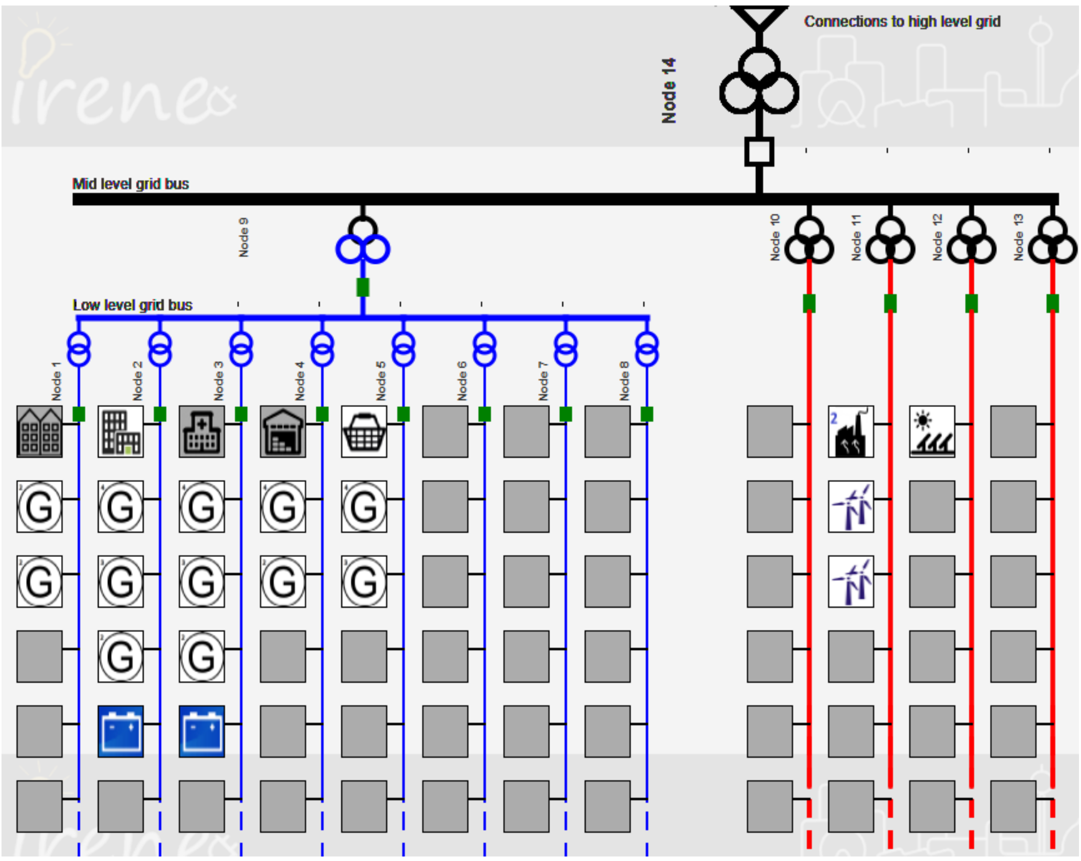


Figure 7-1: The system architecture.

The distribution of the grid components in Figure 7-1 are presented in Table 7-1:

Node No.	Number of distributed generators		Number of energy storage	Profiles included	Populations
	Non-renewable	Renewable			
1	2	0	0	Households	2500
2	3	0	1	Offices	2
3	3	0	1	Hospitals	2
4	2	0	0	Supermarkets	3
5	2	0	0	Warehouses	8
6	0	0	0	0	-
7	0	0	0	0	-
8	0	0	0	0	-
9	1	0	0	0	-
10	0	0	0	0	-
11	1	2	0	0	-
12	0	1	0	0	-
13	0	0	0	0	-
14	0	0	0	0	-

Table 7-1 Number of distributed generators, energy storages, types of consumer profiles and their populations included

In addition to the description of the grid architecture, stakeholders were briefed on the changes that the grid might undertake. It was suggested that the city grows and hence the populations within the city are increased (compared to the data in Table 6-1). Specifically, amount of city components would be as follows: Households = 4500; Offices = 3; Hospitals = 3; Supermarket = 5; Warehouses = 12.

After providing the information, we asked the stakeholders to discuss what grid updates might be introduced to ensure that a city can withstand a blackout with less negative impact. The aim of this exercise is to investigate how the tool (in the context of collaborative decision making in the situation of uncertainty) can be used to improve the robustness/resilience of a complex urban grid.

7.2 First scenario

The collaborative decisions as proposed using the base configuration of Figure 7-1 were:

i. Remove a generator from Node 2;

ii. Remove a generator from Node 3;

iii. Add a PV generator in Node 2;

iv. Add a wind generator in Node 2;

v. Add a battery storage system in Node 1.

The new system architecture and the component distributions as proposed by stakeholders are shown in Figure 7-2 and Table 7-2.

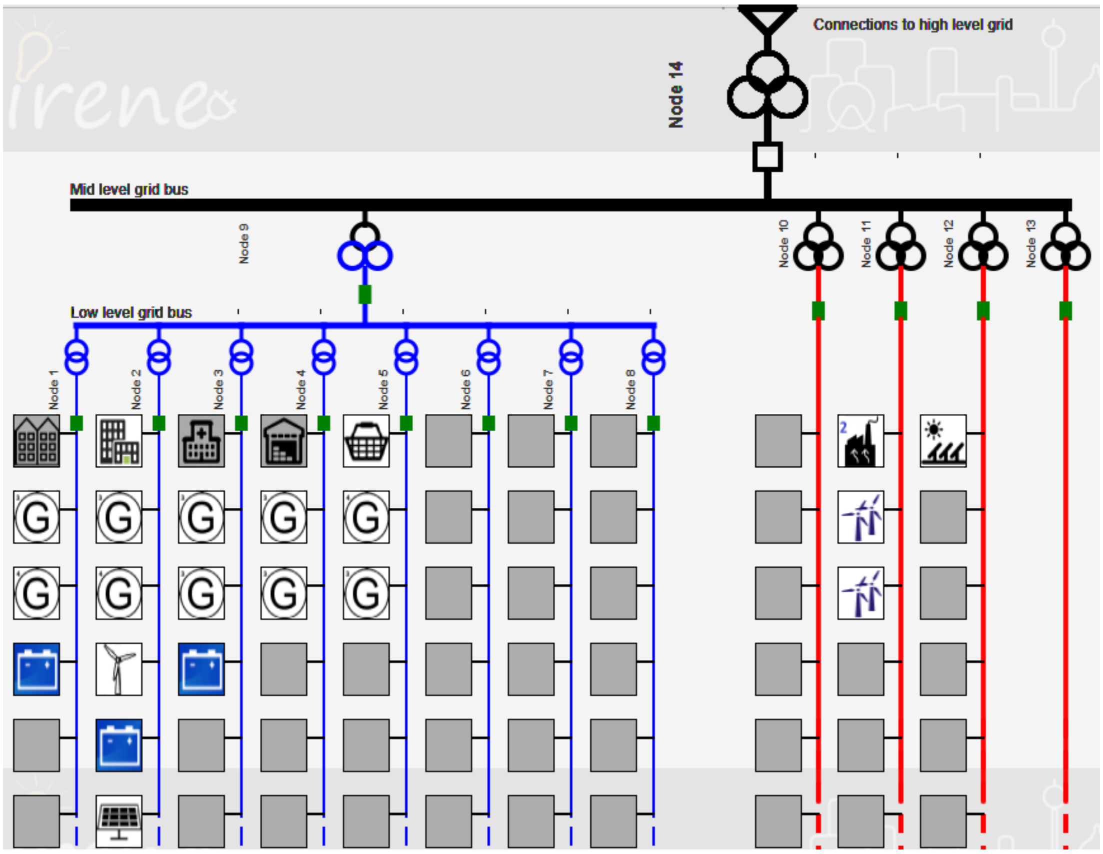


Figure 7-2: The First solution of system architecture as proposed by the Stakeholder.

	Baseline			Group A		
Node No.	Number of distributed generators		Number of energy storage	Number of distributed generators		Number of energy storage
	Non-renewable	Renewable		Non-renewable	Renewable	
1	2	0	0	2	0	1
2	3	0	1	2	2	1
3	3	0	1	2	0	1
4	2	0	0	2	0	0
5	2	0	0	2	0	0
6	0	0	0	0	0	0
7	0	0	0	0	1	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0
11	1	2	0	1	2	0
12	0	1	0	0	1	0
13	0	0	0	0	0	0
14	0	0	0	0	0	0

Table 7-2 Number of distributed generators, energy storages, types of consumer profiles and their populations included as proposed by stakeholders in the first scenario

7.3 Second scenario

The collaborative decisions proposed using the configuration from First scenario (Figure 7-2) and was illustrated in

Figure **7-3** were:

vii. Remove a battery storage system in Node 3;

viii. Add a generator in Node 3.

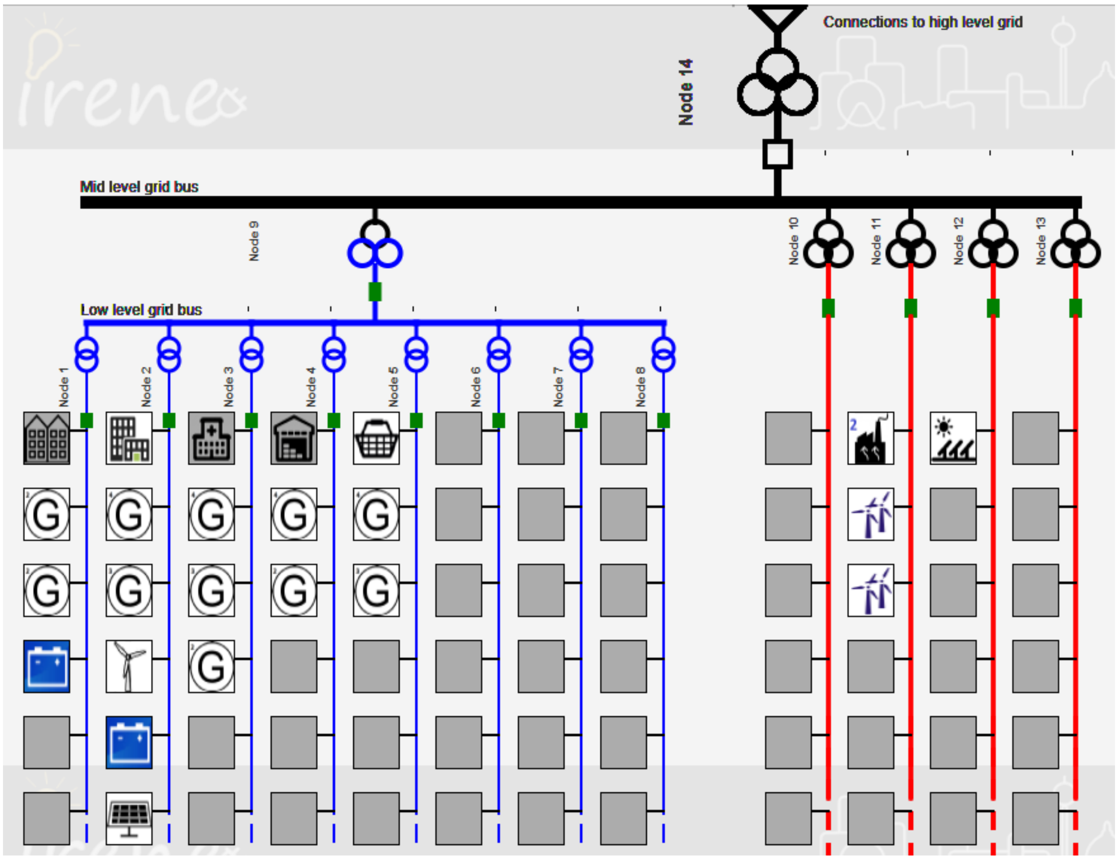


Figure 7-3: The second solution of system architecture as proposed by the Stakeholder.

7.4 Overall Grid Modelling (OGM) tool simulation results

In order to access the effectiveness of the collaborative decisions as made by stakeholders, normal and failure of grid operations are simulated for each node, and also the entire microgrid level, which are similar to the failure simulation and analysis from the previous gaming workshop with students. Decisions placed and the performance of the implemented decisions are compared with the baseline case in terms of resilience coefficients and cost savings [11]. The decisions are simulated using the IRENE's overall grid modelling tool and the timeline for the simulation is allowed for 24 hours, using the new consumer populations: Households = 4500; Offices = 3; Hospitals = 3; Supermarket = 5; Warehouses = 12.

Similar to the gaming exercises, failures occur when there is a line-disconnection between the microgrid and main grid level, and also the line disconnection within the microgrid nodes. When there is a line disconnection due to a failure event, the islanding capability is activated to ensure uninterrupted operation during a utility system outage with *N*-1 compliance [11]. Decisions placed and the performance of the implemented decisions by each groups are compared with the baseline case in terms of resilience coefficients and cost savings [11].

The decisions are simulated using the IRENE's OGM tool and the timeline for the simulation is allowed for 24 hours. The grid with various operating conditions are simulated for the initial grid, the first and second scenario, as shown in Table 6-4.

7.4.1 Case 1 – normal operation

In this case, assuming no failure occurs, the normal mode of operation is applied and therefore the "economic-islanding" capability of microgrid is enabled that employs distributed generations, renewable sources and energy storage systems to provide power at times of high electricity price, rather than drawing the electricity from the main grid [11]. The cost savings and resilience coefficient achieved for baseline, the First and Second scenarios are shown in Table 7-3.

	Baseline	First Scenario	Second scenario
Cost savings (£)	885.72	1023.26	890.76
Resilience coefficient	0	0	0

Table 7-3 Cost savings and resilience coefficient for normal operations

Based on Table 7-3, the collaborative decisions in the First scenario achieve higher amount of cost savings than the Second scenario, and also higher than the Baseline scenario. Hence the decision by stakeholders in proposing the First scenario achieves higher amount of cost savings, particularly for "economic-islanding" normal mode of grid operations. The resilience coefficients are all zeros. This is because the grid is 'not' resilient during the normal mode of operation, without any outage events.

7.4.2 Case 2 – four hours of outage duration

In the second case, it is assumed that an outage within the microgrid or the entire grid occur at 0900 for the duration of four hours. The "economic-islanding" capability is disabled in the case of outage events. Each outage node disconnections is evaluated. Table 7-4 shows the result of the simulation using the baseline, First and Second Scenario. Overall the Baseline scenario promotes highest amount of cost savings than the decisions as imposed by stakeholders. This is because the introduction of renewables require higher amount of cost for generations compared with conventional generators. However, there is a reduction of cost savings in the First scenario, where the battery storage is used rather than the use of diesel generators. As battery storage generates zero cost during the discharging mode, this creates significant amount of cost savings. As all fractions of demands are successfully met during the outage events. The computed resilience coefficients are the identical.

Outage Node	Cost savings (£)			Resilient coefficient		
	Baseline	First	Second	Baseline	First	Second
Node 1	-299.75	-489.9	-489.9	0.111	0.111	0.111
Node 2	-556.84	-546.98	-546.98	0.430	0.430	0.430
Node 3	-291.56	-286.57	-486.07	0.240	0.240	0.240
Node 4	-410.3	-400.01	-400.01	0.144	0.144	0.144
Node 5	-428.09	-437.74	-437.74	0.074	0.074	0.074
Grid outage	-296.76	-325.23	-400.23	1	1	1
Total savings (£)	-2283.3	-2486.43	-2760.93	-	-	-

Table 7-4 Case 2 - cost savings and resilience coefficient for outage operations. Negative sign indicates additional costs are introduced.

7.4.3 Case 3 – eight hours of outage duration

In the final case, it is assumed that an outage within the microgrid or the entire grid occur at 0900 with prolonged outage duration of eight hours compared to Case 2. The "economic-islanding" capability is also disabled. Each outage node disconnections is evaluated. Table 7-5 shows the result of the simulation using the baseline First and Second Scenario. Overall the solution of the First scenario as proposed by stakeholders promotes highest amount of cost savings.

Outage Node	Cost savings (£)			Resilient coefficient		
	Baseline	First	Second	Baseline	First	Second
Node 1	-670.87	-659	-659	0.111	0.111	0.111
Node 2	-1571.89	-955.64	-955.64	0.430	0.430	0.430
Node 3	-867.42	-622.1	-952.1	0.240	0.240	0.240
Node 4	-710.95	-646.53	-646.53	0.144	0.144	0.144
Node 5	-690.21	-689.65	-689.65	0.074	0.074	0.074
Grid outage	-900	-734.14	-734.14	1	1	1
Total savings (£)	-5411.34	-4307.06	-4637.06	-	-	-

Table 7-5 Case 3 - cost savings and resilience coefficient for outage operations. Negative sign indicates additional costs are introduced.

7.5 Evolutionary Threat Analysis (ETA) tool simulation results

Here we list the results of application of the ETA tool on the scenarios that are listed in Section 7.

The first step is to analyse the baseline scenario in Figure 7-1. The ETA tool performs an evolutionary threat analysis, meaning that it builds a threat list starting from the results obtained at the previous steps, if any (see Table 7-6). In particular, the baseline scenario represents the basic setup of the targeted scenario; consequently, all the components (34 buildings and 33 connections) are considered as newly added. The ETA tool identifies 1220 threats from the IRENE threat list that can impact the grid. 69.9% are structural threats, while the remaining 30.1% emerge due to interconnections among different components of the grid. Considering the evolution of the "*Baseline*" suggested from the stakeholders i.e., *1st Scenario* (see Section 7.2), we can see that 54 and 59 structural threats are removed, while 81 and 36 are respectively added to that scenario due to the inclusion of the PV, the wind farm, the battery, and the related connections. A similar trend can be observed looking at the *2nd Scenario* (see Section 7.3), where a battery is removed while a generator is added to the grid. Here the total amount of threats decreases, despite the number of components is exactly the same. This means that the novel component (generator) is affected by a smaller amount of threats with respect to the removed one (battery). Overall, we obtain that the grid at its last evolution stage, can be targeted by 1210 threats. Compared to the overall number of threats of the baseline, we can assert that these evolutions are lowering the total number of threats that are affecting the targeted grid scenario.

Grid Scenario	Components			Structural Threats			Emerging Threats			Threat Stats (%)			
	Buildings	Connections	Tot	Tot	+	-	Tot	+	-	Structural	Emerging	+	-
Baseline	34	33	67	853	853	0	367	367	0	69.9	30.1	100.0	0.0
1st Scenario	35	34	69	890	81	54	344	36	59	72.1	27.9	9.5	9.2
2nd Scenario	35	34	69	880	27	37	330	15	29	72.7	27.3	3.5	5.5

Table 7-6: ETA summary for the considered scenarios.

7.5.1 Insight of scenarios

Looking in detail at the identified threats of the Baseline (see Table 7-7), we point out that all the 38 IRENE threats [4] can occur, while 14 of these 38 types of threat can also emerge from the interconnection of previously disconnected components. In particular, we can observe how the IRENE threat 19 "Conduct physical attacks on organizational facilities." and the IRENE threat 31 "Incorrect Privilege Settings" emerge in the higher number of cases in this scenario. For example, physical attacks can target specific buildings or connections aiming at damage their functionalities e.g., bombing attack on a hospital. Looking at the last column of Table 7-7, we can observe how each of the 38 threats occurs on average in 32.10 different parts of the grid (e.g., on average 24 components of the grid are exposed to DoS or MiM attacks), with a standard deviation of 35.01. Moreover, on each of the 1220 identified threats, 3.14 ± 1.65 high-level mitigation strategies (see [4]) can be implemented to reduce its impact or avoid its happening.

	Structural	Emerging	Total
Threat Types	36	14	38
Most Frequent Threat	(IRENE 19) Conduct physical attacks on organizational facilities.	(IRENE 31) Incorrect privilege settings	(IRENE 31) Incorrect privilege settings
	(IRENE 3) Perform reconnaissance and surveillance of targeted organizations	(IRENE 20) Conduct cyber-physical attacks on organizational facilities, session hijacking or brute force attempts.	(IRENE 19) Conduct physical attacks on organizational facilities.
Occurrences	(Avg) 22.78 (Std) 17.28	(Avg) 24.79 (Std) 19.82	(Avg) 32.10 (Std) 35.01
Mitigations	(Avg) 2.94 (Std) 1.91	(Avg) 3.21 (Std) 1.05	(Avg) 3.14 (Std) 1.65

Table 7-7: ETA Detail for the baseline.

With respect to the in-depth results obtained for the *Baseline*, in the last evolution i.e., *2nd Scenario* grid scenario each threat of the IRENE threat list can occur on average in 31.84 ± 31.23 different places (see last column of Table 7-8). The most frequent threats are the IRENE threats 31 and 19, which call for wrong privilege settings and physical attacks in some part of the grid possibly leading to outages. These threats occur respectively in 101 and 68 separate parts of the grid, also from the interconnections among different groups of components e.g., threat 31 may arise In Node 2 of the topology in Figure 7-3 due to Offices that are competing to get the energy provided by the wind farm, PVs or the battery.

	Structural	Emerging	Total
Threat Types	36	14	38
Most Frequent Threat	(IRENE 19) Conduct physical attacks on organizational facilities.	(IRENE 31) Incorrect privilege settings	(IRENE 31) Incorrect privilege settings
	(IRENE 3) Perform reconnaissance and surveillance of targeted organizations	(IRENE 15) Conduct communications interception attacks.	(IRENE 19) Conduct physical attacks on organizational facilities.
Occurrences	(Avg) 23.25 (Std) 17.61	(Avg) 22.21 (Std) 15.80	(Avg) 31.84 (Std) 31.23
Mitigations	(Avg) 2.94 (Std) 1.41	(Avg) 3.21 (Std) 1.05	(Avg) 2.96 (Std) 1.34

Table 7-8: ETA detail for the 2nd scenario.

Overall, the depicted evolutions in this case lower the total number of threats that are affecting the grid scenario. Additionally, the differences of statistics related to the average occurrences and the most frequent threats within the two scenarios are not remarkable.

7.6 EVALUATION OF STAKEHOLDER WORKSHOP

The stakeholder workshop was successfully conducted with two different scenarios of grid component alterations as decided by fellow stakeholders, in comparison with the baseline case. Additionally, the stakeholder workshop also noted the extensive collaboration within stakeholders in actively increasing the robustness of the electricity network.

The questionnaire feedback session was administered to fellow students at the end of the workshop (refer Appendix F for the Questionnaire feedback). One of the stakeholder with electricity market knowledge agreed that no expert knowledge is required to use the IRENE tools (Q7). Additionally, one of the stakeholder praised the calculations and the scope of the IRENE tools in performing the necessary tasks (Q12). High scores also obtained from fellow stakeholders regarding the practicability of the demand management capability in the IRENE tool (Q3), assumptions on uninterruptible loads (Q3), the efficiency of IRENE tools in running/re-running a simulation (Q5), the ease of understanding the performance metric ‘resilience-coefficient’ in measuring the performance of different grid topologies/configurations (Q7), and being useful as a collaborative-decision making system (Q11).

However, one of the stakeholder (business and citizen representative) argued that specialised industry knowledge is required in order to fully understandable in using the IRENE tools (Q7). Still, the time needed to construct/re-construct the grid components are still inefficient (Q5). Also, majority also voted that high level of knowledge is required in using the tool (Q6). Additionally, the unrealistic practicability of using the metric ‘resilient-coefficient’ in tool simulations (Q9).

Before the end of the workshop, stakeholders suggested several ideas in improving the IRENE tools, where the tools should account the capital costs of investments, integrate flexibility to allow for city configurations, a better user-friendly interface that is simpler to operate, a saved output parameters for comparisons based on different component alterations, and also, a breakdown of cost savings to reflect where changes affect the whole grid system.

A more detailed feedback provided by fellow stakeholders is available in Appendix G.

8 CASCADING FAILURE ANALYSIS TO SUPPORT DESIGN DECISIONS

In this section we describe an approach to evaluate the potential propagation of failures across the grid. The approach presented in this section can be used to analyse, from a quantitative point of view, the impact of failures on the network. Thus it will allow to confirm the analysis achieved during the application of the IRENE framework. The approach is an application of the modular model construction methodology introduced in [1]. More in details, in this section we focus on the effects of overload of network nodes, and on how different topologies and grid properties have impact on cascading failures.

While the approach introduced and applied in the previous sections focuses on planning the grid capacity, and evaluating how different kind of components affect the behaviour of the gird, the approach in this section focus on the impact of topology, assuming a network of identical nodes. In this perspective, the approach can be used to plan the detailed arrangement of a group of network loads.

8.1 ASSESSING NODES CRITICALITY IN POWER GRIDS

Studying the properties of complex networks is an emerging topic cross-cutting several domains, including biology, chemistry, telecommunications, virus spreading, and many others. A comprehensive survey on this topic can be found in [12]. Decentralized infrastructures, characterized by a very large scale and independent local growth, are especially interesting to be studied under the perspective of a complex network.

The power grid clearly falls in this class of systems, and several topology-related analysis techniques are applied in the literature. A common approach is to perform statistical analysis of topological metrics, like the degree of nodes [13, 14] or their betweenness (i.e., how many shortest paths traverse a node) [15, 16] to get an indication of the presence of nodes exposing a critical condition from the topology perspective (e.g., having a very high degree). Using such approaches, the resilience of the grid is assessed by evaluating the ability to efficiently guarantee paths between nodes when nodes or edges in the network are removed, e.g., due to faults or attacks. However, analysing the power grid from a topological perspective only provides a high-level view that may not match the real behaviour of the system. Some works combine topological analysis with physical parameters, using models and methods typical of the power engineering tradition, to represent the flow of power that travels through the power lines [17, 18]. Adding physical parameters to the network is beneficial for results, providing a representation of the way networks tend to disrupt and spread failures closer to reality.

Other approaches specifically focus on aspects related to propagation of failures. A popular approach in this category consists in analysing how overvoltage and/or overcurrent events are propagated through the grid, possibly leading to cascading failures. Also in this category, approaches vary from simple propagation models based on topological aspects [19], to the use of precise mathematical models of the physical layer [19], to the use of ad-hoc power grid simulators [20, 21]. These approaches typically analyse the network in a static setting, or under the effect of deterministic failures, thus being particularly tailored to perform what-if analyses.

While those approaches provide a good view of the system response to failures, they do not provide indications on the nominal behaviour of the system, that is, how good is the nominal grid structure, in terms of node organization and their properties, for supporting the expected network load. To address this problem, approaches in the literature apply stochastic models (e.g., Stochastic Petri Nets [22]) to better represent random behaviour in the occurrence of failures, delays, and random events in general. The work in [23, 24] presents a modelling approach to assess the impact of interdependencies between the Electrical Infrastructure and the controlling Information Infrastructures. The quantification is achieved through the integration of two models: one that concentrates on the structure of the power grid and its physical quantities, and one that concentrates on the behaviour of the control system.

In our approach we combine the use of stochastic models with topology-based approaches for modelling propagation of failures, to obtain a generic framework that can be used both to assess node criticality in the nominal configuration, and to evaluate the consequence of specific failures (what-if analysis). The approach can be used to assess the criticality of certain nodes of the grid, to compare the resilience to failures of different grid topologies, and more in general to offer useful insights for guiding the evolution of the grid.

8.2 Extensible Modelling of Failure Propagation

In this section we describe our extensible model for representing failure propagation in the power grid. Section 7.2.1 recalls the methodology we adopted for the modelling process, Section 7.2.2 details the assumptions we adopted and target metrics, and Section 7.2.3 describes the implementation of the model using the Stochastic Activity Networks (SAN) formalism [25].

8.2.1 Framework

The approach we adopted for modelling was outlined in [1]. Model *templates* are developed for recurrent aspects and/or component of the system, and then composed together to form the global system model. Those templates communicate only through specific, well-defined model *interfaces*.

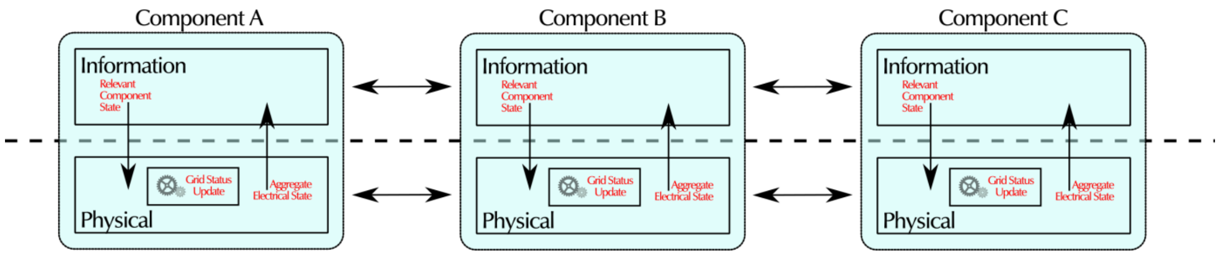


Figure 8-1. Overview of the modular modelling approach. The model of each component has precise interfaces to communicate with the others.

In general, the model of each component can accommodate a *physical layer* (i.e., electric behaviour) and an *information layer* (i.e., control behaviour). Those two layers also communicate with each other through specific model interfaces (Figure 8-1). Changes in the information layer that may have impact on the physical status of the grid (e.g. reconfigurations, failures, recoveries) are notified to the physical layer, which performs a “Grid Status Update”, i.e., new physical parameters are computed by considering the current system state (e.g., number of connected generators, status of transmission lines, on/off status of loads). The new physical parameters could be obtained in different ways, e.g., using external simulators of the physical layer, acquired by actual sensors on the real system, or solving simplified analytic equations.

This composition approach facilitates the extensibility and reuse of the model: templates can be modified in isolation, also extending them to include new functionalities. Changes need to be applied only once, and they are reflected to all the instances of that model template. In the following, we discuss the realization of a *cascading failures propagation model* for the power grid, following this approach.

8.2.2 Assumptions and metrics

As extensively discussed in [26], the literature features a wide range of approaches for modelling cascading failures in power networks. In particular, physical properties can be represented with different levels of detail and assumptions. The model we present in this section abstracts from the details of the power flow equations, in order to focus on failure propagation and the triggering of cascades. As the work in [27], we assume that cascades occur because nodes affected by failures will redistribute part of their load to their neighbours.

More in details, the assumptions of our model can be summarized by the following points:

- The network consists of N identical nodes.
- The initial load of a component, $L_{nominal}$, is uniformly distributed between L_{min} and L_{max}.
- Components have a “hard” limit of operation L_{fail}, beyond which they immediately fail.
- Components have a “soft” limit of operation $L_{critical}$, which if exceeded for a duration T_{trip} causes a breaker to trip, and thus the component to fail.
- With a rate λ a component receives an additional load between ΔL_{min} and ΔL_{max}. We are not interested in the cause that generated such overload, which can be natural (e.g., lightning) or accidental (e.g., short circuit).
- Whenever the load of a component is higher than its nominal load, and the component is not failed, the load is reduced by an amount γ with rate μ.
- When a component fails, its load is immediately redistributed among its neighbours.
- Each of the M neighbours of a failed component currently having load L receive L/M additional load.

Under these assumptions, we want to assess the criticality of nodes of a given grid topology. To quantitatively measure the criticality of a node we use the following metrics:

- $N_{fail}(t)$: The number of nodes that have failed by time t.
- $F(t) = N_{fail}(t)/N$: The proportion of nodes that have failed by time t.
- $P^k_{fail}(t)$: The probability that node k has failed by time t.

The first metric, $N_{fail}(t)$, is an indication of the *resilience of the grid topology as a whole*: the higher the number, the weaker the grid topology. By dividing it by the number of nodes in the grid, $N_{fail}(t)/N$, a proportion of the number of failed nodes is obtained. This leads to the second metric, $F(t)$, a relative metric that can be used to compare different grid topologies.

The last metric, $N_{fail}(t)$, is an indication of the *criticality of node* k: nodes with higher values for this metric have a higher criticality, meaning that they are more subject to fail with respect to others. When performing what-if analysis, assessing this metric for nodes that were not involved in the initial failure gives an indication of the exposition of such nodes to cascading events originated in other nodes in the grid.

8.2.3 Implementation using stochastic activity networks

The model described above is implemented using a single template model, the *NetworkNode* template, which is replicated and instantiated multiple times to represent the desired network topology. The template has been implemented using the Stochastic Activity Networks (SAN) formalism. A schematic view of the model template is depicted in Figure 8-2 and it is described in the following. Dashed boxes highlight interfaces of the model template.

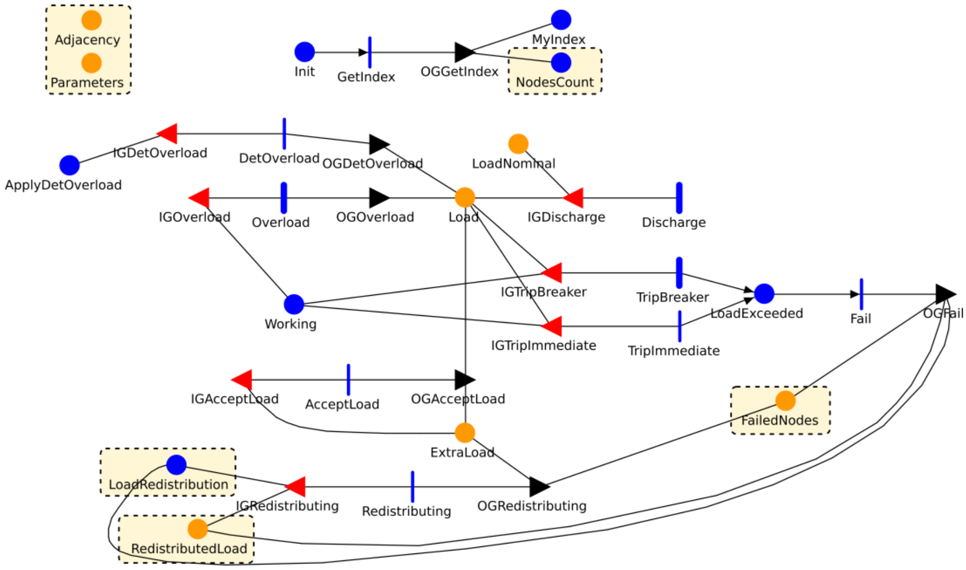


Figure 8-2. SAN implementation of the *NetworkNode* model template.

The interfaces of the model template include the *Adjacency*, *Parameters*, *NodesCount*, *FailedNodes*, *LoadRedistribution*, and *RedistributeLoad* places. A unique integer index is automatically assigned to each instance of the model template, thus allowing to distinguish the different instances. The index is assigned by the firing of activity *GetIndex*, which adds a token in *NodesCount*, and then uses this value as the index, which is then stored in *MyIndex* place. *NodesCount* is shared among all the nodes, so that at the end of the initialization process it contains the total number of nodes in the scenario.

Adjacency is a matrix $N \times N$, which contains the adjacency matrix of the topology that needs to be modelled. The value of *Adjacency[i][j]* is 1 if there exist an edge between node *i* and node *j*. The extended place *Parameters* contains the parameters of all the nodes in the scenario, indexed by the node index. *FailedNodes* records which nodes are currently failed, in the form of an array. *RedistributeLoad* and *LoadRedistribution* are used to share the redistributed load between nodes.

During the initialization of the model, a number uniformly distributed between L_{min} and L_{max} is sampled; the resulting values is put in place *LoadNominal*, and then copied to place *Load*. Based on a switch variable, the model can work in two modalities:

- Random failures (*DeterministicOverload=0*)
- Deterministic failures (*DeterministicOverload=1)*

Random overload is modelled by the *Overload* activity, which is enabled only if *DeterministicOverload=0*. The activity fires with rate λ. When it fires, a number uniformly distributed between OL_{min} and OL_{max} is sampled, and the resulting value added to *Load*. Deterministic overload is modelled by the *DetOverload* activity, which instead is enabled only if *DeterministicOverload=1*. If the index of the node is equal to *DeterministicOverloadNode*, then an amount equal to *DeterministicOverloadAmount* is added to *Load*.

If *Load* becomes higher than *LoadNominal* then the activity *Discharge* becomes enabled, and fires with rate μ. Each time it fires, an amount of load γ is removed from *Load*, until the value in *LoadNominal* is restored.

If the value of *Load* exceeds $L_{critical}$ then activity *TripBreaker* is enabled. If it stays enabled for an interval of duration T_{trip} then it fires, removing the token from place *Working*, and adding one to *LoadExceeded*. Similarly, if the value of *Load* exceeds L_{fail} then activity *TripImmediate* is enabled. However, in this case it fires immediately, also removing the token from *Working* place, and adding one to *LoadExceeded*.

When *LoadExceeded* contains a token, activity *Fail* is then enabled and fires, leading to the failure of the node and to the redistribution of the load. The output gate *OGFail* has two main tasks: i) set the current node as failed in the *FailedNodes* array, and ii) compute the number of neighbours of the current node (from *Adjacency*), and consequently the amount of load to be redistributed to each of them (*RedistributeLoad*). Place *LoadRedistribution* signals to the other nodes that load redistribution took place, and thus they need to retrieve the propagated load from *RedistributeLoad* place.

When *LoadRedistribution* contains a number of tokens equal to the index of the node, then activity *Redistributing* is enabled and fires. If there is load to be redistributed for the current node (i.e., *RedistributeLoad[i]>0*) then that amount is added to *Load*, potentially incrementing the load above the critical and/or failure thresholds. This may cause further failures of the other nodes, in a cascading fashion.

The target metrics defined in Section 7.2.2 are computed as follows:

- $N_{fail}(t)$: The expected sum of tokens present in place *FailedNodes* at time t.
- $F(t) = N_{fail}(t)/N$
- $P^{k}_{fail}(t)$: The probability there is a token in place *FailedNodes[k]* at time t.

8.3 ANALYSIS AND RESULTS

In this section we describe the analysis that has been performed on a representative use case, and the obtained results. Section 7.3.1 describes the analysed scenario, and associated parameters. Section 7.3.2 describes the results obtained in the nominal configuration, i.e., assuming random failures. Section 7.3.3 describes the results obtained in a “what-if” setting, i.e., assuming deterministic failures on specific nodes.

8.3.1 Scenario and parameters

We assume now to analyze the internal structure of “Node 1” as described in Figure 5-1 and Table 5-1, which represents a set of 15.000 households. As a representative case of possible internal network topology, we adopted a modified version of the 30-bus Power Flow Test Case (Figure 8-3) [28]. We note that we mainly used the test case from a topological perspective, and thus derived a simplified graph-based representation of it. The simplified network contains 21 nodes (Figure 8-4). This is due to the fact that, for simplicity, some nodes of Figure 8-3 have been joined together (e.g., 4/12/13 and 6/9/10/11).

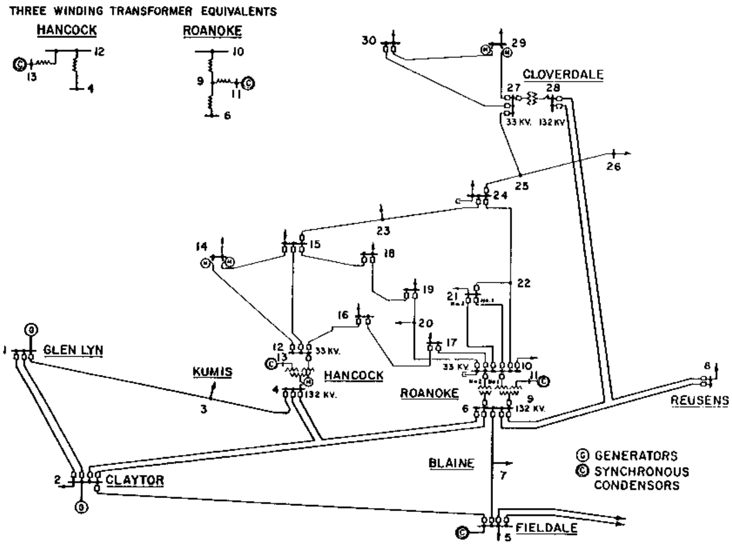


Figure 8-3. 30-bus Power Flow Test Case [28].

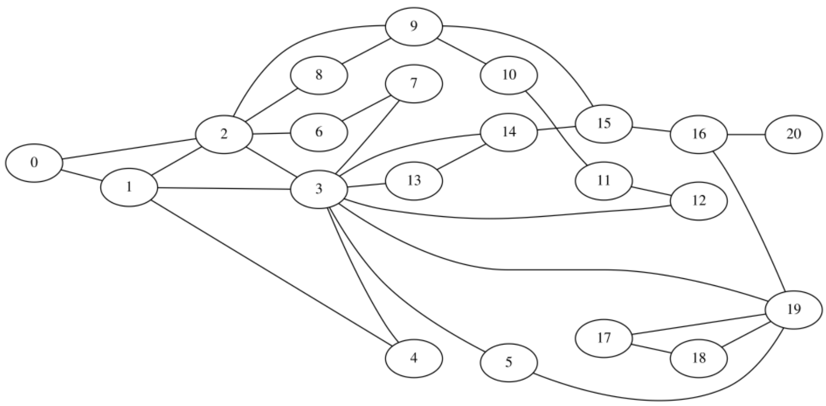


Figure 8-4. Simplified network derived from the 30-bus Power Flow Test Case.

The nominal parameters that will be used in this evaluation are reported in Table 8-1. The unit of measurement for time is minutes. The load levels are expressed as relative numbers. The results in the following have been computed using the discrete-event simulator provided with the Mobius tool-set. All the values have been computed by running at least 10.000 simulation batches, with a relative confidence half-interval of 0.1, and confidence level 90%.

Table 8-1. Model parameters and their default values. Times are in minutes.

Parameter	Symbol	Value	Description
LoadMin	L_{min}	0.2	Minimum initial load
LoadMax	L_{max}	0.6	Maximum initial load

OverloadOccurrenceRate	λ	1.0E-5	Occurrence rate of an overload event
OverloadMin	OL_{min}	0.1	Minimum load amount that is added by a random overload event
OverloadMax	OL_{max}	0.2	Maximum load amount that is added by a random overload event
DeterministicOverloadAmount	–	1.0	Amount of load that is added to a component when in deterministic mode (what-if analysis)
LoadCritical	$L_{critical}$	0.75	Critical load level
LaodFail	L_{fail}	0.99	Maximum load level, beyond which the component immediately fails
BreakerDelay	T_{trip}	20.0	Time after which the component fails if the load remains above $L_{critical}$
OverloadDischargeAmount	γ	0.01	Amount of exceeding load that is absorbed at each discharge
OverloadDischargeRate	μ	0.1	Rate at which discharge of exceeding load occurs

8.3.2 Random failures

In the first evaluation we evaluate the effect of random failures on the grid. Figure 8-5 (left) shows the average number of failed nodes during a month, at varying of the overload rate λ. Note that repairs are not included in the model. Values of λ equal to 5.0E-5 or higher pose a significant threat for the analysed grid topology: on the average at least one node will be failed after 30 days. For λ=5.0E-4 the system is not manageable anymore: on the average more than 9 nodes will be failed after 30 days. This is clearly a situation where cascading failures are occurred, causing a widespread failure of network nodes.

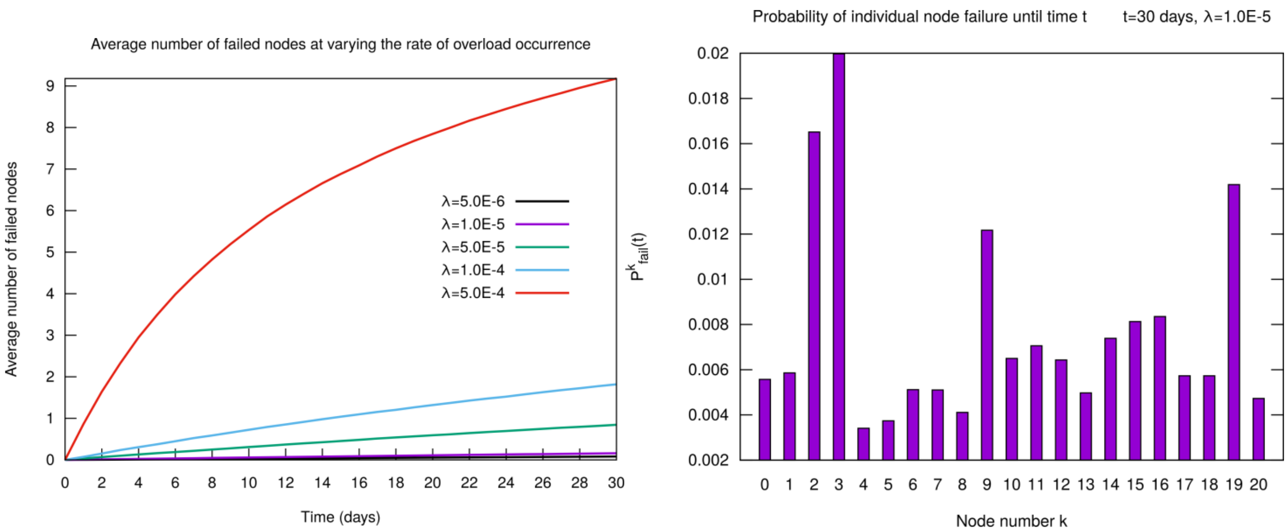


Figure 8-5. Effect of random failures on the grid, considering both average number of node failures (left), and failure probability of individual nodes (right).

Figure 8-5 (right) shows the failure probability of individual nodes after 30 days, in the nominal configuration. From the figure it is evident that some nodes are more subject to be the target of failure propagation with respect to other nodes. In particular, node #3 is the most critical one, followed by #2, #19, and #9. The least affected ones result to be node #4 and node #5. By comparing these results with the diagram of Figure 8-4, the nodes that are deemed most critical are those that have a higher number of neighbours (node degree). The results are explained by the fact that, having more neighbours, they will receive a higher amount of propagated load in case of other nodes' failures.

8.3.3 What-if analysis

In this section we show how the framework can be used to perform what-if analysis. We assume that a large overload occurs on one of the nodes of the network, causing its failure, and we assess if and how the failure has cascading effects on the other nodes of the grid.

Figure 8-6 depicts the effect of a large overload on four different nodes of the network: node 1, node 7, node 9, and node 20. Each graph shows the probability of failure of the other nodes of the network as a consequence of the failure under analysis. The results provide useful insights on the criticality of individual nodes, and on the possible *propagation dynamics* that may arise.

In case of failure of node 1 (top left), its immediate neighbours, nodes 0, 2, 3, and 4, will also fail. However, the cascading effect is limited: for the other nodes the probability of failure is zero or very small. Similarly, the failure of node 7 (top right) has a large impact only on nodes within distance two from it (2, 3, and 6), while it has a limited impact on the others. This is a good indication that the cascading effect will be contained. The interruption of the cascading effect is due to the high degree of both nodes 2 and 3; this allows the excess load to be spread among a large number of nodes, thus being partially absorbed.

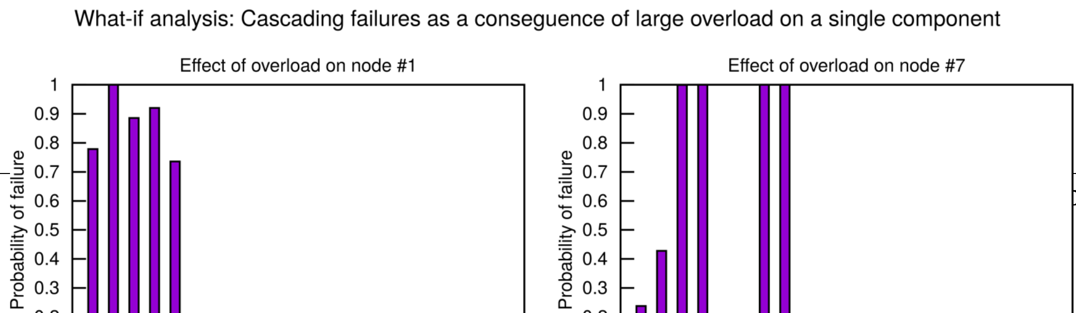


Figure 8-6. Effect of a large overload on specific nodes of the network.

Instead, the failure of node 9 (bottom left) or node 20 (bottom right) causes a large cascading effect on many nodes of the network. In the first case, four nodes have a failure probability greater than 50%, and other three greater than 25%. In the second case, three nodes have a failure probability of almost 100%, three near 50%, and other two greater than 25%, some of which are at distance 4 from the failed node.

It should be noted that, under the "random failure" setting (Section 8.3.2), node 9 was found to be one of the nodes more affected by random failures. The what-if analysis performed in this section indicates that a failure of that node would cause severe cascading effects on the whole network. Therefore these results suggest that node 9 is a very critical node, which could require some specific maintenance actions, e.g. for increasing the maximum load level beyond which the component fails (thus increasing the L_{fail} and $L_{critical}$ thresholds).

8.3.4 Summary

The approach presented in this section can be used to analyse, from a quantitative point of view, the impact of failures on the network. The approach can be used to analyse the effect of random failures in the target grid, as well as to perform what-if analyses. The application of the approach to the presented use case has demonstrated its capabilities to assess the *resilience of the grid topology*, and to identify *most critical paths and nodes* in the grid, which are more vulnerable to cascading failures. These kinds of analyses can be profitably used as support for planning the construction and/or evolution of the network, in order to maximize its resilience to failures.

9 CONCLUSIONS

This document applies a number of constructs as reviewed in D5.1 of the IRENE WP5 [1]. As a result, this forms basis for designing and evaluating outcomes of IRENE gaming simulations and stakeholder workshops. The document also presents the design of the gaming and stakeholder workshop, as well as the questionnaire design in order to assess the scalability of IRENE methods and tools to real-life situations, and report on quantitative assessment from the gaming and stakeholder workshop.

The main output of this document is to present the result and evaluation of the gaming simulation and stakeholder workshop respectively. A baseline grid configuration is developed and fellow students and stakeholders are required to undertake collaborative grid planning and further propose several solutions in order to improve the robustness of the ordinary grid structure. IRENE tools are used to simulate the outcome decision as proposed by fellow students and stakeholders. The survey feedback gathered will not only further supports and complements the analysis, but also to improve the efficiency, practicability and impact mitigation of IRENE tools, methods and policies.

10 REFERENCES

[1] IRENE D5.1, "State-of-the art in gaming simulations and stakeholder workshops for method evaluation (in progress)," 2016.

[2] IRENE D1.1, "IRENE scenario and baseline model," 2015.

[3] A. Vasenev, D. Ionita, T. Zoppi, A. Ceccarelli and R. Wieringa, "Towards security requirements: iconicity as a feature of an informal modeling language," 2017.

[4] IRENE D2.1, "Threat identification and ranking," 2015.

[5] L. A. Bollinger, *Fostering Climate Resilient Electricity Infrastructure,* Delft: Delft University of Technology, 2015.

[6] IRENE D4.2, "Open modelling framework," 2016.

[7] B. Hillmer, "Best Practices: Understanding and Reducing Bias in Your Surveys," Survey Gizmo, 24 1 2017. [Online]. Available: https://help.surveygizmo.com/help/survey-bias. [Accessed 16 2 2017].

[8] O. Friborg, M. Martinussen and J. H. Rosenvinge, "Likert-based vs. semantic differential-based scorings of positive psychological constructs: A psychometric comparison of two versions of a scale measuring resilience," *Personality and Individual Differences,* vol. 40, no. 5, pp. 873-884, 2006.

[9] S. Myagmar, J. L. Adam and Y. William, "Threat modelling as a basis for security requirements," in *In: Symposium on Requirements Engineering for Information Security (SREIS)* , 2005.

[10] IRENE D4.1, "Toolsets of supply demand prediction and threat identification and classification," 2016.

[11] IRENE D3.1, "System architecture design, supply demand model and simulation," 2016.

[12] G. A. Pagani and M. Aiello, "The power grid as a complex network: a survey," *Physica A: Statistical Mechanics and its Applications,* vol. 392, no. 11, pp. 2688-2700, 2013.

[13] D. P. Chassin and C. Posse, "Evaluating North American electric grid reliability using the Barabasi Albert Network Model," *Physica A: Statistical Mechanics and its Applications,* vol. 355, pp. 667-677, 2005.

[14] Z. Wang, A. Scaglione and R. Thomas, “The node degree distribution in power grid and its topology robustness under random and selective node removals,” in *IEEE International COnference on Communications Workshops, ICC, pp. 1-5,* 2010.

[15] P. Crucitti, V. Latora and M. Marchiori, “A topological analysis of the Italian electric power grid,” *Physica A: Statistical Mechanic and its Applications,* vol. 338, pp. 92-97, 2004.

[16] R. Albert, I. Albert and G. L. Nakarado, “Structural vulnerability of the North American power grid,” *Phys. Rev. E 69, 025103(R),* vol. 69, no. 2, pp. 1-10, 2004.

[17] S. Arianos, E. Bompard, A. Carbone and F. Xue, “Power grid vulnerability: a complex network approach,” *Chaos: An Interdisplinary Journal of Nonlinear Science,* vol. 013119, no. 19, pp. 1-6, 2009.

[18] E. Bompard, R. Napoli and F. Xue, “Analysis of structural vulnerabilities in power transmission grids,” *International Journal of Critical Infrastructure Protection,* vol. 2, pp. 5-12, 2009.

[19] Z. Huang, C. Wang, T. Zhu and A. Nayak, “Cascading failures in smart grid: joint effect of load propagation and interdependence,” *IEEE Access,* vol. 3, pp. 2520-2530, 2015.

[20] S. Hong, B. Wang and J. Wang, “Cascading failure propagation in interconnected networks with tunable load redistribution strategy,” in *2015 Prognostics and System Health Management Conference (PHM),* Beijing, China, 2015.

[21] M. Wei and W. Wang, “Combat the disaster. Communications in smart grid alleviate cascading failures,” in *11th Annual High Capacity Optical Networks and Emerging/Enabling Technologies (Photonics for Energy),* Charlotte, NC, 2014.

[22] G. Ciardo, R. German and C. Lindemann, “A characterisation of the stochastic process underlying a stochastic Petri net,” *IEEE Transactions on Software Engineering* , vol. 20, pp. 506-515, 1994.

[23] M. Beccuti, G. Franceschinis, S. Donatelli, S. Chiaradonna, F. Di Giandomenico, P. Lollini, G. Dondossola and F. Garrone, “Quantifications of dependencies in electrical and information infrastructures: the CRUTIAL approach,” in *4th International Conference on Critical Infrastructures (CRIS 2009),* 2009.

[24] S. Chiaradonna, P. Lollini and F. Di Giandomenico, “On a modeling framework for the analysis of Interdependencies in elctric power systems dependable systems,” in *37th Annual IEEE/IFIP International Conference,* 2007.

[25] W. H. Sanders and J. F. Meyer, “Stochastic activity networks: formal definitions and concepts,” in *Lectures on formal methods and performance analysis,* New York, Springer-Verlag, 2002, pp. 315-343.

[26] R. Fitzmaurice, E. Cotilla-Sanchez and P. Himes, “Evaluating the impact of modeling assumptions for cascading failure simulation,” in *2012 IEEE Power and Energy Society General Meeting*, San Diego, CA, 2012.

[27] E. Zio and G. Sansavini, “Component criticality in failure cascade processes of network systems,” *Risk Analysis,* vol. 31, no. 8, pp. 1196-1210, 2011.

[28] R. Christie, “30 bus power flow test case,” *Power Systems Test Case Archive,* August 1993.

A HANDOUT FOR GAMING EXERCISE

We would like to thank you for participating in this exercise. Your feedback will help us to improve a tool oriented to support analysis of grid robustness.

Intro

The collaboration of stakeholders is vital for improving the resilience of a complex system, such as an urban grid. In this exercise, several city-level stakeholders need to collectively decide how to introduce a new component into the urban grid architecture to improve robustness of the grid. Please read the details of stakeholder roles below.

Overview of Stakeholders' Expertise

Several stakeholders work together on deciding how to introduce a grid element into the grid. They aim at *ensuring the continuity of electricity supply to critical city consuming nodes during power outages*. These stakeholders are:

- City Planner (CP), who thinks how the city might develop;
- Distribution Network Operator (DNOs), who controls the grid and ensures it functioning;
- Citizen and Business Representative (CBR), who considers continuity of city functions.

City Planner (CP) is responsible in the renewable energy-related landscape and the overall aim to reduce greenhouse gas emission. For instance, to find a suitable location for a plant, one should account for distances from the site to the sources. In case of solar urban planning, the interplay between the urban form and solar energy inputs is another concern. Not everywhere can be possible to locate solar panels or wind generators. Interrelations between generation and consumption nodes can be complex. Short term goals are linked to long term goals, but are not the same.

DNO ensures the operation of the grid and how to secure electricity supply. Because of the variability in generation, it is essential that IT elements of the grid will be able to act efficiently to manage fluctuations in energy generation. Adversarial attacks, natural disasters, and software&hardware failures can cripple the grid. DNO thinks of possible risks and pay particular attention to changes in the grid, the introduction, updates, or removal of grid components. Still, grid operators may overlook the importance of particular customers for the proper functioning of the city as a whole (see CBR functions) and lack a global picture, provided by CP.

Citizen and Business Representative (CBR) is involved into the planning to help investigate how severe is the blackout. CBR considers the impact of the blackout to citizens and businesses. (S)he has a stake in prioritizing electricity distribution during blackouts.

Exercise

Please choose one of the stakeholder roles, so your group have all three stakeholders represented. Think how your role contributes to collaborative decision making within the 6 step process. Perform the 6-step process in collaboration with other actors present in your group (with the help of the tool). Later, we would like you to reflect on how you see the tool within this process.

We suggest that you structure your interactions with respect to six steps suggested by US NIIP (US National Infrastructure Protection Plan):

- Set security goals: Define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective protective posture;
- Identify assets, systems, networks, and functions: Develop an inventory of the assets, systems, and networks;
- Assess risks: Determine risk by combining potential direct and indirect consequences of a terrorist attack or other hazards, known vulnerabilities to various potential attack vectors, and general or specific threat information;
- Prioritize: Aggregate and analyze risk assessment results to develop a picture of asset, system, and network risk, establish priorities based on risk, and determine protection and business continuity initiatives that provide the greatest mitigation of risk;
- Implement protective programs: Select protective actions to reduce or manage the risk identified and secure the resources needed to address priorities;
- Measure effectiveness: Use metrics and other evaluation procedures to measure progress and assess the effectiveness of the protection program in improving protection, managing risk, and increasing resiliency.

B HANDOUT FOR STAKEHOLDER WORKSHOP

We would like to thank you for participating in this exercise. Your feedback will help us to improve a tool oriented to support analysis of grid robustness.

Intro

The collaboration of stakeholders is vital for improving the resilience of a complex system, such as an urban grid. In this exercise, several city-level stakeholders need to collectively decide how to introduce a new component into the urban grid architecture to improve robustness of the grid. Please read the details of stakeholder roles below.

Overview of Stakeholders' Expertise

Several stakeholders work together on deciding how to introduce a grid element into the grid. They aim at *ensuring the continuity of electricity supply to critical city consuming nodes during power outages*. These stakeholders are:

- City Planner (CP), who thinks how the city might develop;
- Distribution Network Operator (DNOs), who controls the grid and ensures it functioning;
- Citizen and Business Representative (CBR), who considers continuity of city functions.

City Planner (CP) is responsible in the renewable energy-related landscape and the overall aim to reduce greenhouse gas emission. For instance, to find a suitable location for a plant, one should account for distances from the site to the sources. In case of solar urban planning, the interplay between the urban form and solar energy inputs is another concern. Not everywhere can be possible to locate solar panels or wind generators. Interrelations between generation and consumption nodes can be complex. Short term goals are linked to long term goals, but are not the same.

DNO ensures the operation of the grid and how to secure electricity supply. Because of the variability in generation, it is essential that IT elements of the grid will be able to act efficiently to manage fluctuations in energy generation. Adversarial attacks, natural disasters, and software&hardware failures can cripple the grid. DNO thinks of possible risks and pay particular attention to changes in the grid, the introduction, updates, or removal of grid components. Still, grid operators may overlook the importance of particular customers for the proper functioning of the city as a whole (see CBR functions) and lack a global picture, provided by CP.

Citizen and Business Representative (CBR) is involved into the planning to help investigate how severe is the blackout. CBR considers the impact of the blackout to citizens and businesses. (S)he has a stake in prioritizing electricity distribution during blackouts.

Exercise

Please think how your role contributes to collaborative decision making within the 6 step process. Perform the 6-step process in collaboration with other actors present in your group (with the help of the tool). Later, we would like you to reflect on how you see the tool within this process.

We suggest that you structure your interactions with respect to six steps suggested by US NIIP (US National Infrastructure Protection Plan):

- Set security goals: Define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective protective posture;
- Identify assets, systems, networks, and functions: Develop an inventory of the assets, systems, and networks;
- Assess risks: Determine risk by combining potential direct and indirect consequences of a terrorist attack or other hazards, known vulnerabilities to various potential attack vectors, and general or specific threat information;
- Prioritize: Aggregate and analyze risk assessment results to develop a picture of asset, system, and network risk, establish priorities based on risk, and determine protection and business continuity initiatives that provide the greatest mitigation of risk;
- Implement protective programs: Select protective actions to reduce or manage the risk identified and secure the resources needed to address priorities;
- Measure effectiveness: Use metrics and other evaluation procedures to measure progress and assess the effectiveness of the protection program in improving protection, managing risk, and increasing resiliency.

Goals:

- Primary goal: Compared to the initial scenario , the updated scenario should have at least the same resilience coefficient (to meet demand)
- Secondary goal: increase monetary saving

Given:

- Increase of the population by NNN.
- Set of components stakeholders can use
- Outage scenarios
- Grid topology (IEEE-14 inspired tree)

Actionable points:

- Add/remove a PV or Wind to LV Nodes
- Add/remove storages and generators
- Add components to Nodes 6-8.
- Add/change/remove MV elements

Limitation:

- Cannot move consumption elements
- Cannot change (reduced) customer profile – critical loads were already defined
- Only one type of consumer in the tree
- There are no back-up lines between the nodes
- If there is consumption in the LV node, there should be at least two generators (to ensure electricity supply if one generator fails)
- The circuit breaker is used to simulate the node disconnection.

C QUESTIONNAIRE FOR GAMING SIMULATION

T5.2 - Survey Forms

*Required

Evaluation of practicability and efficiency of the methodologies and toolset

Your opinion of the practicability and efficiency of IRENE's methodologies and toolset

1. **Q1. What is your main role in your company, or your role in the workshop?** *
Mark only one oval.
   - Municipal authority planner
   - DNO (Distribution Network Operator)
   - Critical infrastructure owner/operators
   - Business and Citizen representative groups
   - Other: ____________

2. **Q2. Please, rate your current knowledge on smart grids.**
Mark only one oval.

	1	2	3	4	5	6	7	
Very low	○	○	○	○	○	○	○	Very high

3. **Q3. Please rate the practicability of:**
Mark only one oval per row.

	1 (Very incorrect)	2	3	4	5	6	7 (Very correct)
consumer profile data with DSM capability?	○	○	○	○	○	○	○
assumption on controlled generations needed to balance the demand?	○	○	○	○	○	○	○
assumption that the islanded operation is possible during an outage event?	○	○	○	○	○	○	○
assumption on plausible point of disconnected load during the outage?	○	○	○	○	○	○	○
assumption that IEEE-14 bus can be used in the toolset?	○	○	○	○	○	○	○
assumption that some loads are critical?	○	○	○	○	○	○	○
assumption that some loads are uninterruptible?	○	○	○	○	○	○	○

4. **Q4. Please rate the effectiveness of:**
Mark only one oval per row.

	1 (Very ineffective)	2	3	4	5	6	7 (Very effective)
the toolset in addressing the outage?							
the threat assessment within grid components?							
the demand forecast?							

Evaluation of the toolset

Your opinion of using the toolset

5. **Q5. Please rate the efficiency (speed) of:** *
Mark only one oval per row.

	1 (Very inefficient)	2	3	4	5	6	7 (Very efficient)
time needed to run/re-run a simulation?							
time needed to construct/re-construct the grid components?							
time needed to run/re-run a demand forecast?							

6. **Q6. How would you rate the level of:** *
Mark only one oval per row.

	1 (Very low)	2	3	4	5	6	7 (Very high)
knowledge required in using the toolset?							
easiness in using the toolset?							

7. **Q7. If you rate the level of Q6. as 5 or above, please explain why.**

8. **Q8. How understandable is the toolset simulation in:** *
Mark only one oval per row.

	1 (Very easy)	2	3	4	5	6	7 (Very hard)
Resilience coefficient							
Threat assessment							

9. **Q9. How practicable (realistic) is the toolset simulation in:** *
Mark only one oval per row.

	1 (Very unrealistic)	2	3	4	5	6	7 (Very realistic)
Resilience coefficient							
Threat assessment							

10. **Q10. How strongly do you agree that the toolset is:** *
Mark only one oval per row.

	1 (Completely disagree)	2	3	4	5	6	7 (Completely agree)
practicable for evaluation of urban electricity network?							
fast in providing simulation analysis of urban electricity network?							
useful in addressing the outage in urban electricity network?							

Evaluation of a toolset for collaborative grid modelling

Your opinion of using the toolset for collaborative grid modelling purposes

11. **Q11. How strongly do you agree that the grid modelling toolset is useful:**
Mark only one oval per row.

	1 (Completely disagree)	2	3	4	5 (Completely agree)
as a collaborative decision support system?					
in establishing a collaborative planning framework among stakeholders?					

12. **Q12. What would you suggest to improve the toolset?** *
Please provide at least two suggestions.

Powered by Google Forms

D QUESTIONNAIRE FOR STAKEHOLDER WORKSHOP

T5.2 - Survey Forms

*Required

Evaluation of practicability and efficiency of the methodologies and tool

Your opinion of the practicability and efficiency of IRENE's methodologies and tool

1. **Q1. What is your main role in your company? ***
   Mark only one oval.
   - ◯ Municipal authority planner
   - ◯ DNO (Distribution Network Operator)
   - ◯ Critical infrastructure owner/operators
   - ◯ Business and Citizen representative groups
   - ◯ Other: ________________

2. **Q2. Please, rate your current knowledge on smart grids.**
   Mark only one oval.

	1	2	3	4	5	6	7	
Very low	◯	◯	◯	◯	◯	◯	◯	Very high

3. **Q3. Please rate the practicability of:**
   Mark only one oval per row.

	1 (Very incorrect)	2	3	4	5	6	7 (Very correct)
consumer profile data with DSM capability?	◯	◯	◯	◯	◯	◯	◯
assumption on controlled generations needed to balance the demand?	◯	◯	◯	◯	◯	◯	◯
assumption that the islanded operation is possible during an outage event?	◯	◯	◯	◯	◯	◯	◯
assumption on plausible point of disconnected load during the outage?	◯	◯	◯	◯	◯	◯	◯
assumption that some loads are critical?	◯	◯	◯	◯	◯	◯	◯
assumption that some loads are uninterruptible?	◯	◯	◯	◯	◯	◯	◯

4. **Q4. Please rate the effectiveness of:**
Mark only one oval per row.

	1 (Very ineffective)	2	3	4	5	6	7 (Very effective)
the tool in addressing the outage?							
the demand forecast?							

Evaluation of the tool

Your opinion of using the tool

5. **Q5. Please rate the efficiency (speed) of:** *
Mark only one oval per row.

	1 (Very inefficient)	2	3	4	5	6	7 (Very efficient)
time needed to run/re-run a simulation?							
time needed to construct/re-construct the grid components?							
time needed to run/re-run a demand forecast?							

6. **Q6. How would you rate the level of:** *
Mark only one oval per row.

	1 (Very low)	2	3	4	5	6	7 (Very high)
knowledge required in using the tool?							
easiness in using the tool?							

7. **Q7. If you rate the level of Q6. as 5 or above, please explain why.**

8. **Q8. How understandable is the tool simulation in:** *
Mark only one oval per row.

	1 (Very easy)	2	3	4	5	6	7 (Very hard)
Resilience coefficient							

9. **Q9. How practicable (realistic) is the tool simulation in:** *
Mark only one oval per row.

	1 (Very unrealistic)	2	3	4	5	6	7 (Very realistic)
Resilience coefficient							

10. **Q10. How strongly do you agree that the tool is:** *
Mark only one oval per row.

	1 (Completely disagree)	2	3	4	5	6	7 (Completely agree)
practicable for evaluation of urban electricity network?							
fast in providing simulation analysis of urban electricity network?							
useful in addressing the outage in urban electricity network?							

Evaluation of a tool for collaborative grid modelling

Your opinion of using the tool for collaborative grid modelling purposes

11. **Q11. How strongly do you agree that the grid modelling tool is useful:**
Mark only one oval per row.

	1 (Completely disagree)	2	3	4	5	6	7 (Completely agree)
as a collaborative decision support system?							
in establishing a collaborative planning framework among stakeholders?							

12. **Q12. What would you suggest to improve the tool?** *
Please provide at least two suggestions.

....

....

....

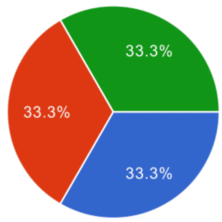
....

Powered by
Google Forms

E QUESTIONNAIRE FEEDBACK FROM GAMING SIMULATION

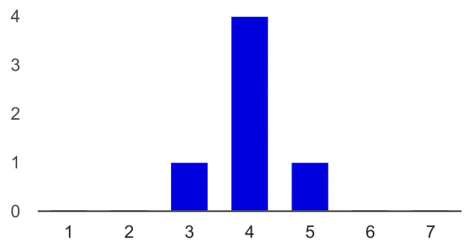
Evaluation of practicability and efficiency of the methodologies and toolset

Q1. What is your main role in your company, or your role in the workshop?



Municipal authority planner	**2**	33.3%
DNO (Distribution Network Operator)	**2**	33.3%
Critical infrastructure owner/operators	**0**	0%
Business and Citizen representative groups	**2**	33.3%
Other	**0**	0%

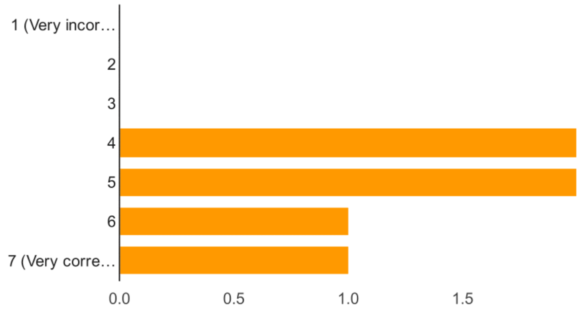
Q2. Please, rate your current knowledge on smart grids.



Very low: 1	**0**	0%
2	**0**	0%
3	**1**	16.7%
4	**4**	66.7%
5	**1**	16.7%

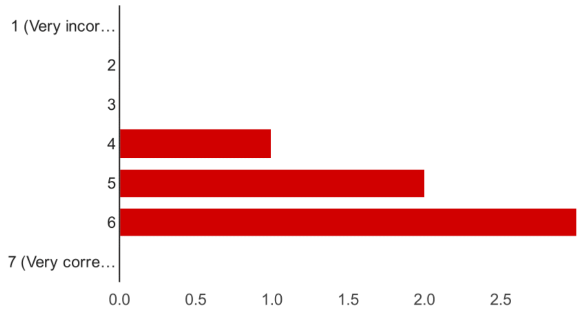
6	**0**	0%
Very high: 7	**0**	0%

consumer profile data with DSM capability? [Q3. Please rate the practicability of:]



1 (Very incorrect)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**2**	33.3%
5	**2**	33.3%
6	**1**	16.7%
7 (Very correct)	**1**	16.7%

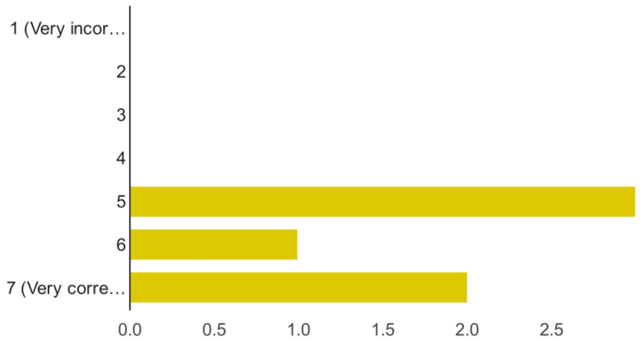
assumption on controlled generations needed to balance the demand? [Q3. Please rate the practicability of:]



1 (Very incorrect)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**1**	16.7%
5	**2**	33.3%
6	**3**	50%

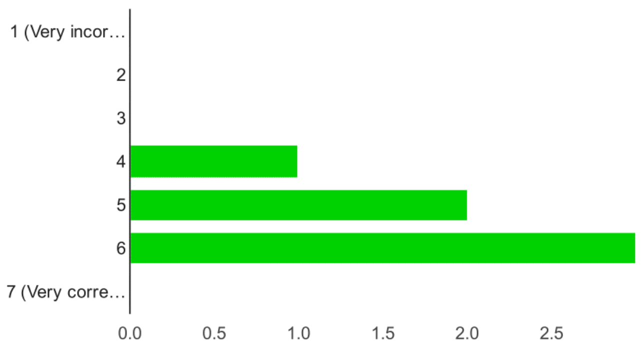
7 (Very correct)	**0**	0%

assumption that the islanded operation is possible during an outage event? [Q3. Please rate the practicability of:]



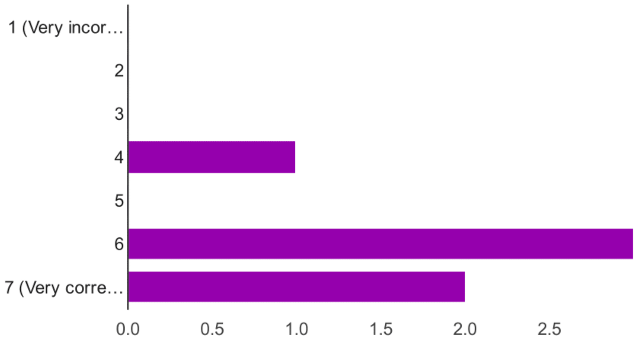
1 (Very incorrect)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**0**	0%
5	**3**	50%
6	**1**	16.7%
7 (Very correct)	**2**	33.3%

assumption on plausible point of disconnected load during the outage? [Q3. Please rate the practicability of:]



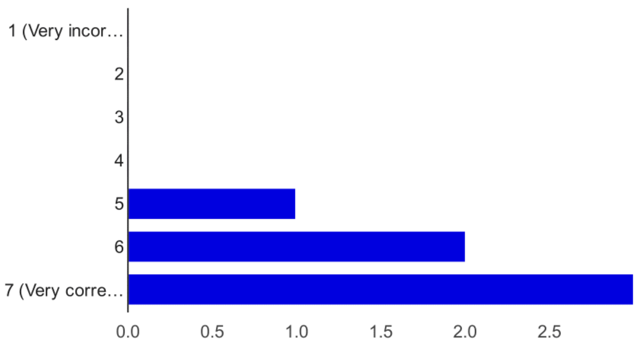
1 (Very incorrect)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**1**	16.7%
5	**2**	33.3%
6	**3**	50%
7 (Very correct)	**0**	0%

assumption that IEEE-14 bus can be used in the toolset? [Q3. Please rate the practicability of:]



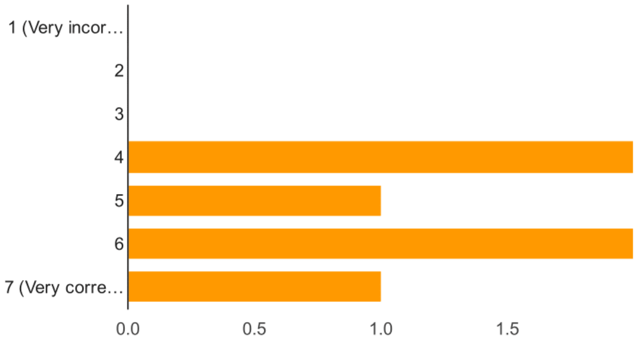
1 (Very incorrect)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**1**	16.7%
5	**0**	0%
6	**3**	50%
7 (Very correct)	**2**	33.3%

assumption that some loads are critical? [Q3. Please rate the practicability of:]



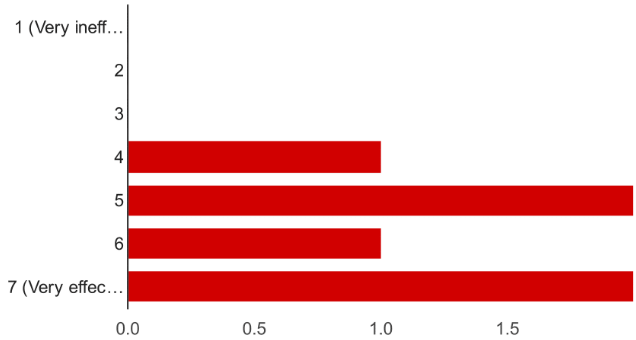
1 (Very incorrect)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**0**	0%
5	**1**	16.7%
6	**2**	33.3%
7 (Very correct)	**3**	50%

assumption that some loads are uninterruptible? [Q3. Please rate the practicability of:]



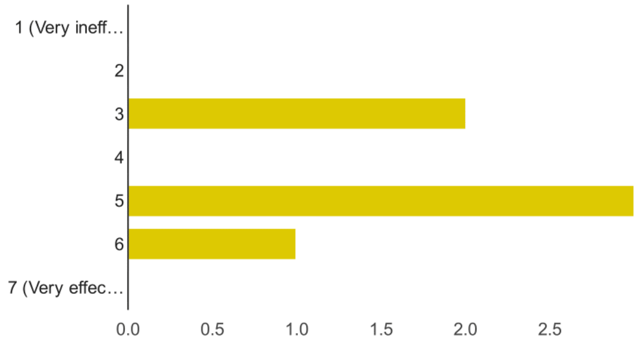
1 (Very incorrect)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**2**	33.3%
5	**1**	16.7%
6	**2**	33.3%
7 (Very correct)	**1**	16.7%

the toolset in addressing the outage? [Q4. Please rate the effectiveness of:]



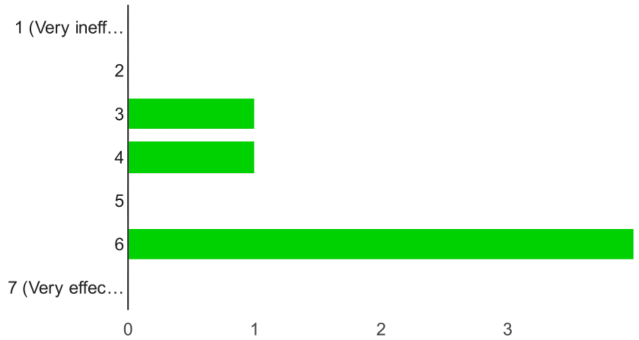
1 (Very ineffective)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**1**	16.7%
5	**2**	33.3%
6	**1**	16.7%
7 (Very effective)	**2**	33.3%

the threat assessment within grid components? [Q4. Please rate the effectiveness of:]



1 (Very ineffective)	**0**	0%
2	**0**	0%
3	**2**	33.3%
4	**0**	0%
5	**3**	50%
6	**1**	16.7%
7 (Very effective)	**0**	0%

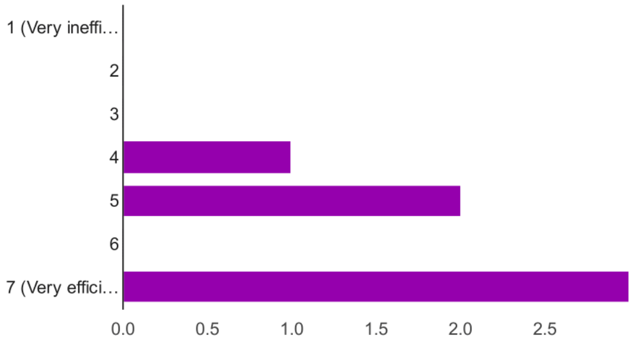
the demand forecast? [Q4. Please rate the effectiveness of:]



1 (Very ineffective)	**0**	0%
2	**0**	0%
3	**1**	16.7%
4	**1**	16.7%
5	**0**	0%
6	**4**	66.7%
7 (Very effective)	**0**	0%

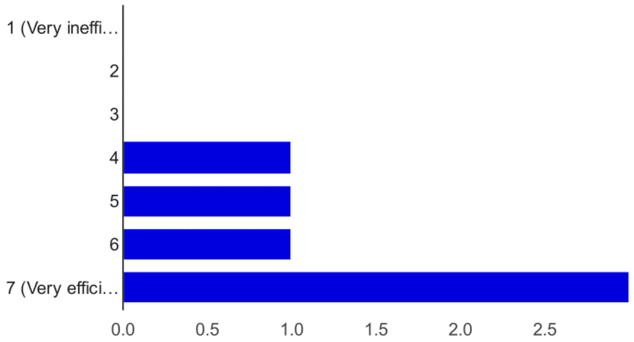
Evaluation of the toolset

time needed to run/re-run a simulation? [Q5. Please rate the efficiency (speed) of:]



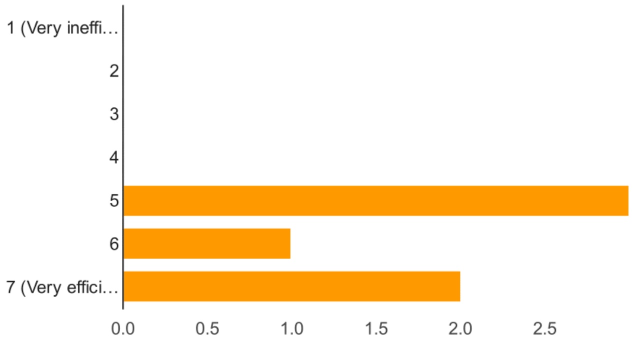
1 (Very inefficient)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**1**	16.7%
5	**2**	33.3%
6	**0**	0%
7 (Very efficient)	**3**	50%

time needed to construct/re-construct the grid components? [Q5. Please rate the efficiency (speed) of:]



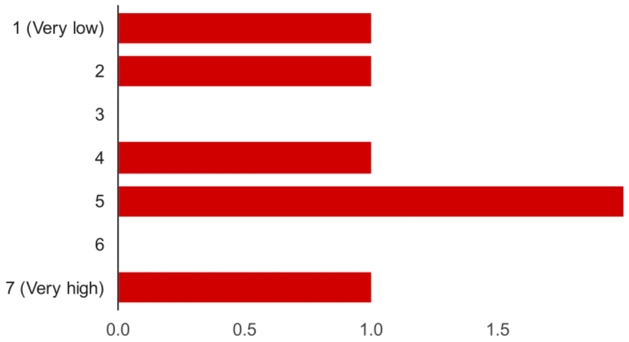
1 (Very inefficient)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**1**	16.7%
5	**1**	16.7%
6	**1**	16.7%
7 (Very efficient)	**3**	50%

time needed to run/re-run a demand forecast? [Q5. Please rate the efficiency (speed) of:]



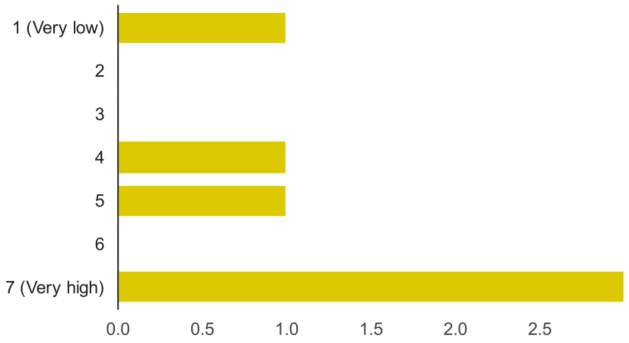
1 (Very inefficient)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**0**	0%
5	**3**	50%
6	**1**	16.7%
7 (Very efficient)	**2**	33.3%

knowledge required in using the toolset? [Q6. How would you rate the level of:]



1 (Very low)	**1**	16.7%
2	**1**	16.7%
3	**0**	0%
4	**1**	16.7%
5	**2**	33.3%
6	**0**	0%
7 (Very high)	**1**	16.7%

easiness in using the toolset? [Q6. How would you rate the level of:]



1 (Very low)	**1**	16.7%
2	**0**	0%
3	**0**	0%
4	**1**	16.7%
5	**1**	16.7%
6	**0**	0%
7 (Very high)	**3**	50%

Q7. If you rate the level of Q6. as 5 or above, please explain why.

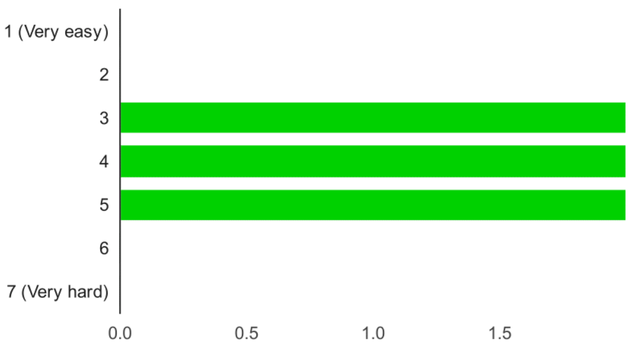
There are many components and the users must have a good knowledge of the relationship between them.

The GUI of the toolset is good and easy to use. However, the scenario is complex, I prefer to have more data to make my decision instead of just having an overview.

There are many components in the toolset which will require background knowledge. It would be more useful to indicate electricity flow direction.

It is very convenient to ass/delete a component in the toolset. And by simply pressing the run button, the results will show.

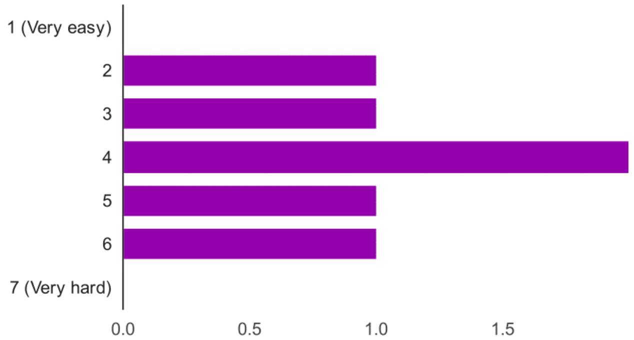
Resilience coefficient [Q8. How understandable is the toolset simulation in:]



1 (Very easy)	**0**	0%

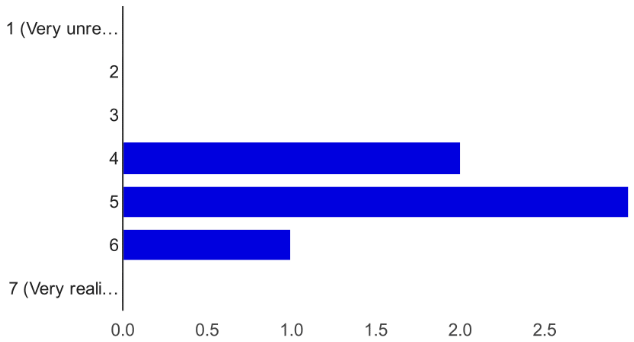
2	**0**	0%
3	**2**	33.3%
4	**2**	33.3%
5	**2**	33.3%
6	**0**	0%
7 (Very hard)	**0**	0%

Threat assessment [Q8. How understandable is the toolset simulation in:]



1 (Very easy)	**0**	0%
2	**1**	16.7%
3	**1**	16.7%
4	**2**	33.3%
5	**1**	16.7%
6	**1**	16.7%
7 (Very hard)	**0**	0%

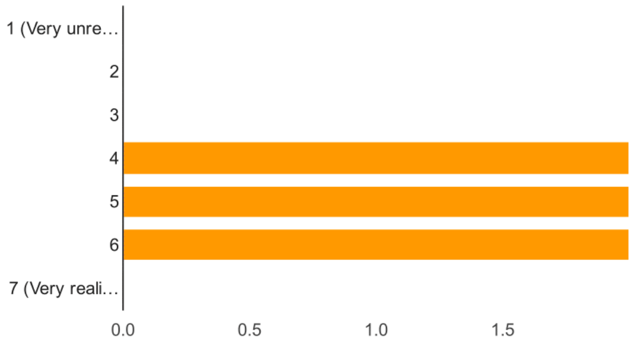
Resilience coefficient [Q9. How practicable (realistic) is the toolset simulation in:]



1 (Very unrealistic)	**0**	0%
2	**0**	0%
3	**0**	0%

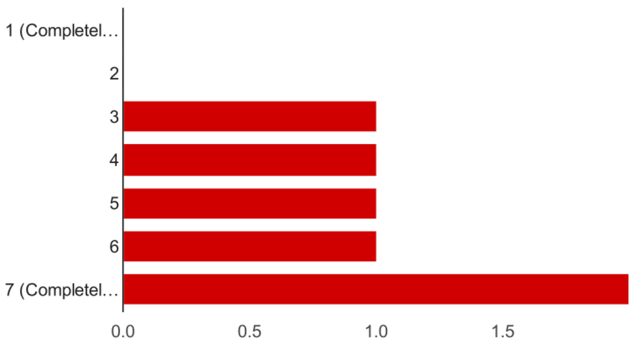
4	**2**	33.3%
5	**3**	50%
6	**1**	16.7%
7 (Very realistic)	**0**	0%

Threat assessment [Q9. How practicable (realistic) is the toolset simulation in:]



1 (Very unrealistic)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**2**	33.3%
5	**2**	33.3%
6	**2**	33.3%
7 (Very realistic)	**0**	0%

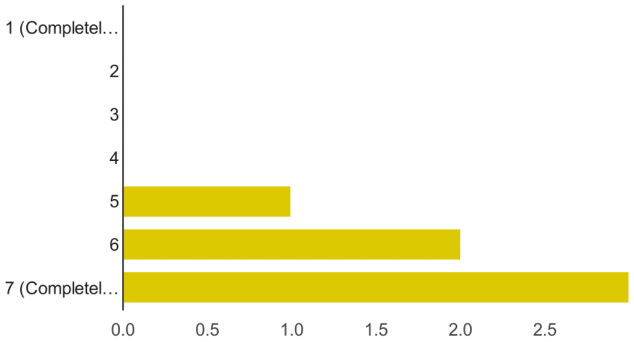
practicable for evaluation of urban electricity network? [Q10. How strongly do you agree that the toolset is:]



1 (Completely disagree)	**0**	0%
2	**0**	0%
3	**1**	16.7%
4	**1**	16.7%

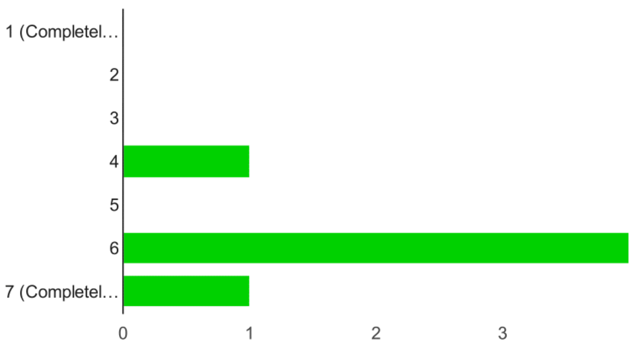
5	**1**	16.7%
6	**1**	16.7%
7 (Completely agree)	**2**	33.3%

fast in providing simulation analysis of urban electricity network? [Q10. How strongly do you agree that the toolset is:]



1 (Completely disagree)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**0**	0%
5	**1**	16.7%
6	**2**	33.3%
7 (Completely agree)	**3**	50%

useful in addressing the outage in urban electricity network? [Q10. How strongly do you agree that the toolset is:]

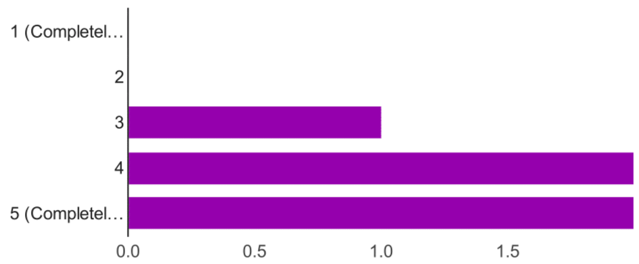


1 (Completely disagree)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**1**	16.7%
5	**0**	0%

6	**4**	66.7%
7 (Completely agree)	**1**	16.7%

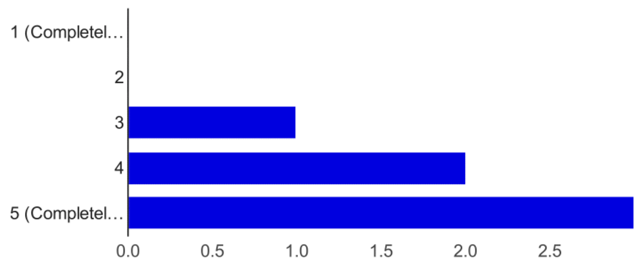
Evaluation of a toolset for collaborative grid modelling

as a collaborative decision support system? [Q11. How strongly do you agree that the grid modelling toolset is useful:]



1 (Completely disagree)	**0**	0%
2	**0**	0%
3	**1**	20%
4	**2**	40%
5 (Completely agree)	**2**	40%

in establishing a collaborative planning framework among stakeholders? [Q11. How strongly do you agree that the grid modelling toolset is useful:]



1 (Completely disagree)	**0**	0%
2	**0**	0%
3	**1**	16.7%
4	**2**	33.3%
5 (Completely agree)	**3**	50%

Q12. What would you suggest to improve the toolset?

1. The functionality of the component is not quite clear. 2. The difference between power suppliers is not illustrated accurately. 3. This software is useful for designing the city development.

1. May provide key parameter in Graphic. 2. A possible panel to support drag and adding icons.

More data to make decision.

1. Give more description/ attributes of the components. 2. Change some word of the (content) to give more clear meaning.

It would be great to specify the different kind of threat which the type of disconnection/hazardous could be different. And the distance or the distribution of the grid planning is not fully presented.

It will be better if the capability of each power generation or renewable components can be presented in the form such as 1 solar can supply 100 supermarket. It is because people may don't have the knowledge about the power unit. practicality. Cos and distance (feasibility) should also be considered in the simulation.

F QUESTIONNAIRE FEEDBACK FROM STAKEHOLDER WORKSHOP – PART 1

laumelvin89@gmail.com

Edit this form

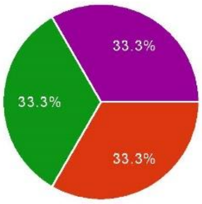
3 responses

Publish analytics

Summary

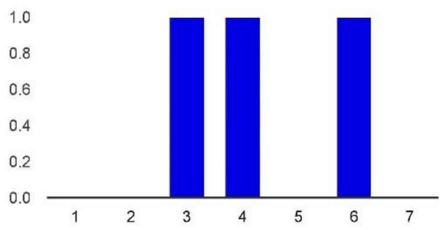
Evaluation of practicability and efficiency of the methodologies and tool

Q1. What is your main role in your company?



Municipal authority planner	0	0%
DNO (Distribution Network Operator)	1	33.3%
Critical infrastructure owner/operators	0	0%
Business and Citizen representative groups	1	33.3%
Other	1	33.3%

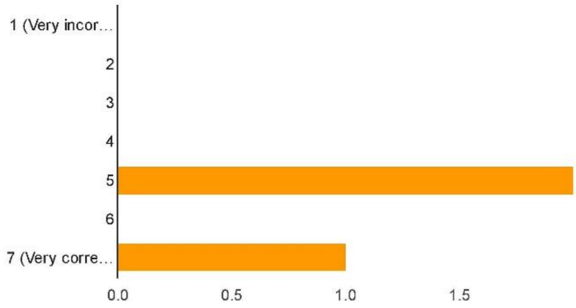
Q2. Please, rate your current knowledge on smart grids.



Very low: 1	0	0%
2	0	0%
3	1	33.3%
4	1	33.3%
5	0	0%

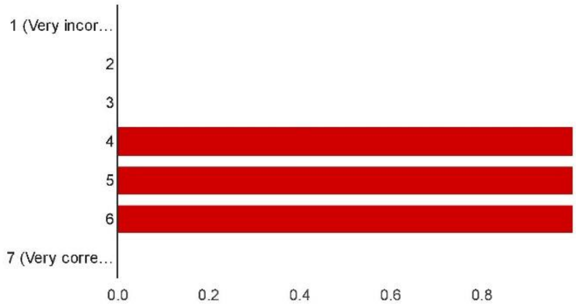
6	1	33.3%
Very high: 7	0	0%

consumer profile data with DSM capability? [Q3. Please rate the practicability of:]



1 (Very incorrect)	0	0%
2	0	0%
3	0	0%
4	0	0%
5	2	66.7%
6	0	0%
7 (Very correct)	1	33.3%

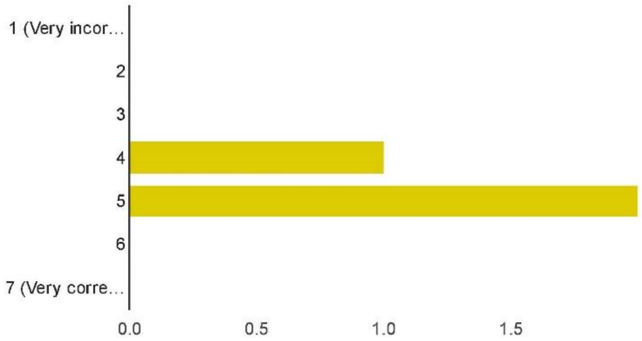
assumption on controlled generations needed to balance the demand? [Q3. Please rate the practicability of:]



1 (Very incorrect)	0	0%
2	0	0%
3	0	0%
4	1	33.3%
5	1	33.3%
6	1	33.3%

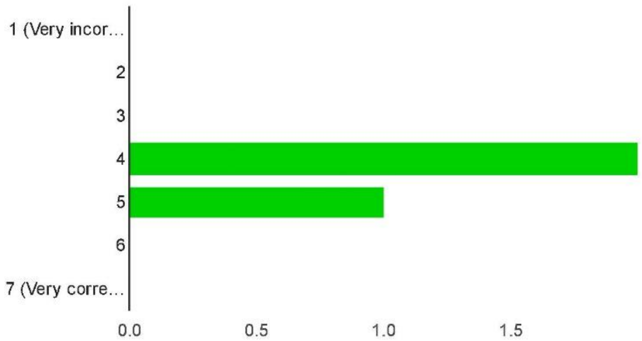
7 (Very correct)	**0**	0%

assumption that the islanded operation is possible during an outage event? [Q3. Please rate the practicability of:]



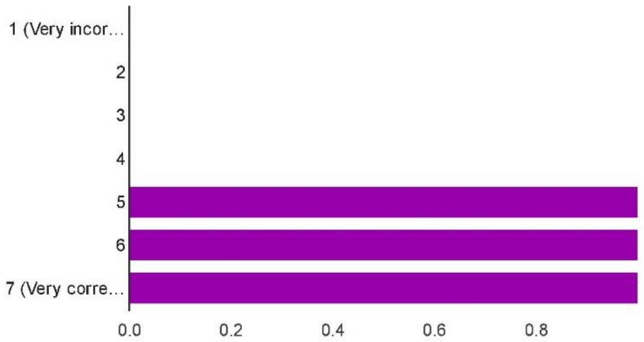
1 (Very incorrect)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**1**	33.3%
5	**2**	66.7%
6	**0**	0%
7 (Very correct)	**0**	0%

assumption on plausible point of disconnected load during the outage? [Q3. Please rate the practicability of:]



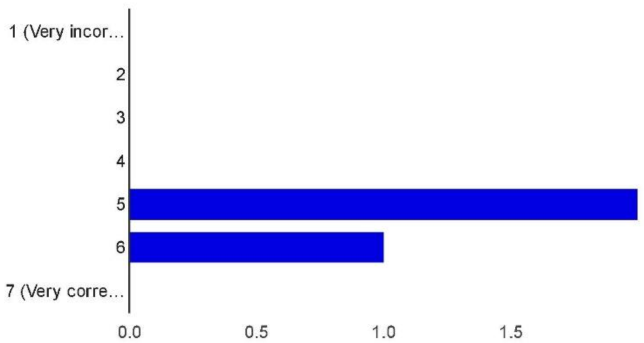
1 (Very incorrect)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**2**	66.7%
5	**1**	33.3%
6	**0**	0%
7 (Very correct)	**0**	0%

assumption that some loads are critical? [Q3. Please rate the practicability of:]



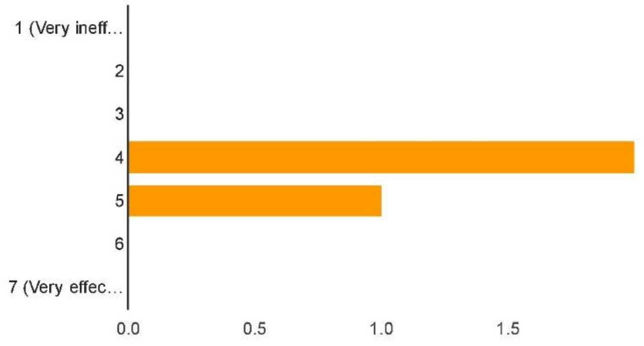
1 (Very incorrect)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**0**	0%
5	**1**	33.3%
6	**1**	33.3%
7 (Very correct)	**1**	33.3%

assumption that some loads are uninterruptible? [Q3. Please rate the practicability of:]



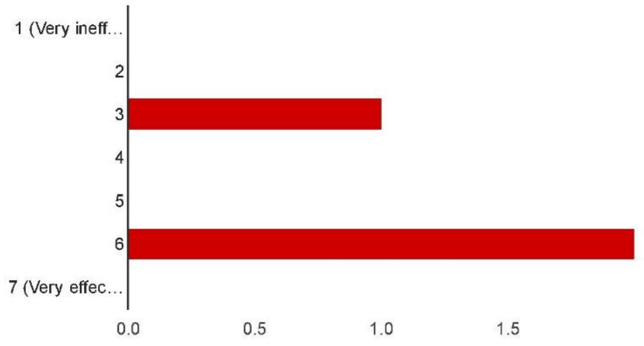
1 (Very incorrect)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**0**	0%
5	**2**	66.7%
6	**1**	33.3%
7 (Very correct)	**0**	0%

the tool in addressing the outage? [Q4. Please rate the effectiveness of:]



1 (Very ineffective)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**2**	66.7%
5	**1**	33.3%
6	**0**	0%
7 (Very effective)	**0**	0%

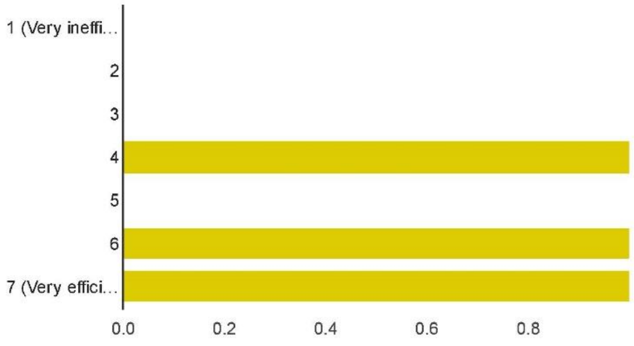
the demand forecast? [Q4. Please rate the effectiveness of:]



1 (Very ineffective)	**0**	0%
2	**0**	0%
3	**1**	33.3%
4	**0**	0%
5	**0**	0%
6	**2**	66.7%
7 (Very effective)	**0**	0%

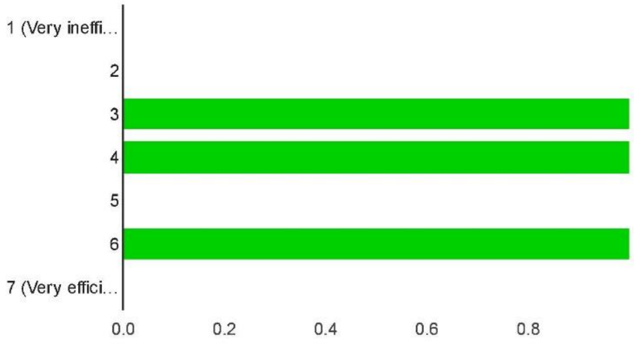
Evaluation of the tool

time needed to run/re-run a simulation? [Q5. Please rate the efficiency (speed) of:]



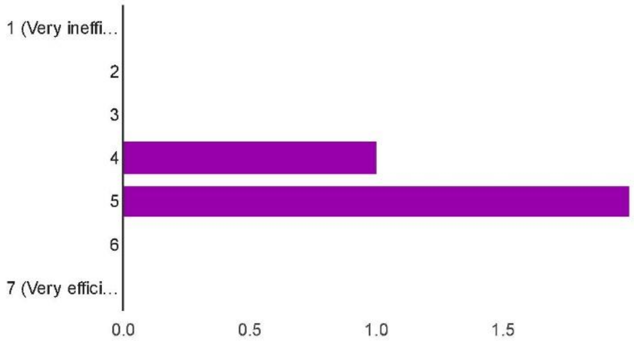
1 (Very inefficient)	0	0%
2	0	0%
3	0	0%
4	1	33.3%
5	0	0%
6	1	33.3%
7 (Very efficient)	1	33.3%

time needed to construct/re-construct the grid components? [Q5. Please rate the efficiency (speed) of:]



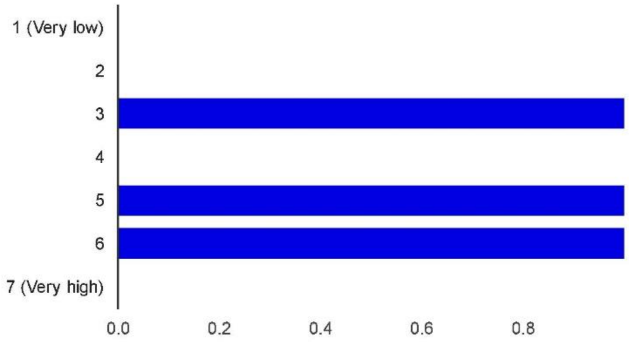
1 (Very inefficient)	0	0%
2	0	0%
3	1	33.3%
4	1	33.3%
5	0	0%
6	1	33.3%
7 (Very efficient)	0	0%

time needed to run/re-run a demand forecast? [Q5. Please rate the efficiency (speed) of:]



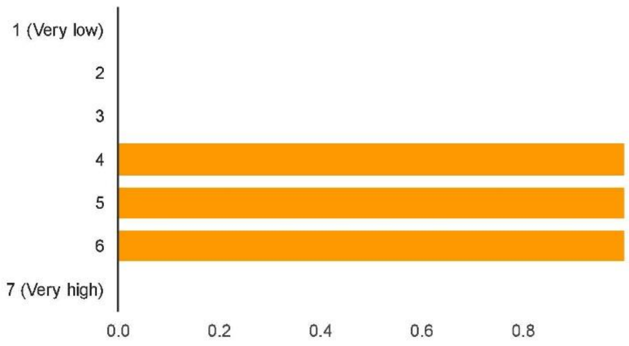
1 (Very inefficient)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**1**	33.3%
5	**2**	66.7%
6	**0**	0%
7 (Very efficient)	**0**	0%

knowledge required in using the tool? [Q6. How would you rate the level of:]



1 (Very low)	**0**	0%
2	**0**	0%
3	**1**	33.3%
4	**0**	0%
5	**1**	33.3%
6	**1**	33.3%
7 (Very high)	**0**	0%

easiness in using the tool? [Q6. How would you rate the level of:]



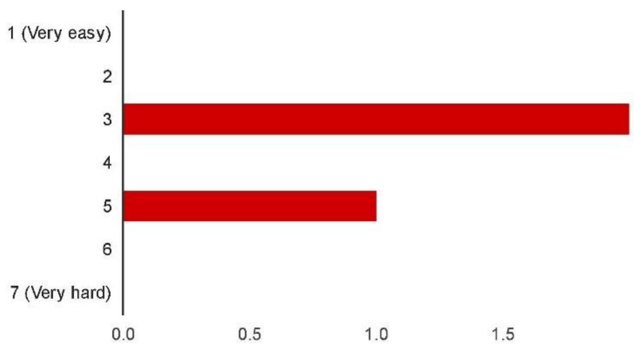
1 (Very low)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**1**	33.3%
5	**1**	33.3%
6	**1**	33.3%
7 (Very high)	**0**	0%

Q7. If you rate the level of Q6. as 5 or above, please explain why.

No expert knowledge required to use tool.

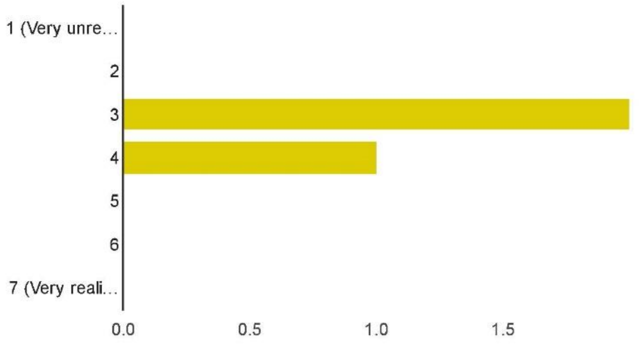
Tool is for special market, so industry knowledge is required

Resilience coefficient [Q8. How understandable is the tool simulation in:]



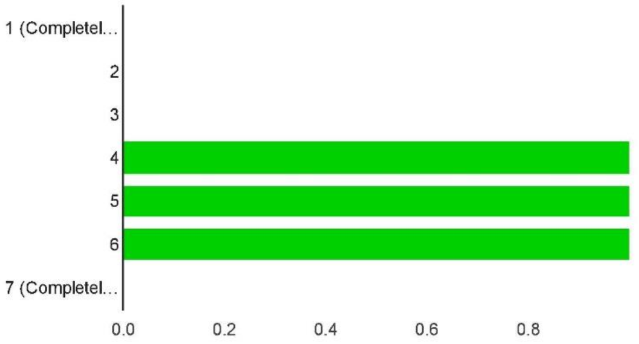
1 (Very easy)	**0**	0%
2	**0**	0%
3	**2**	66.7%
4	**0**	0%
5	**1**	33.3%
6	**0**	0%
7 (Very hard)	**0**	0%

Resilience coefficient [Q9. How practicable (realistic) is the tool simulation in:]



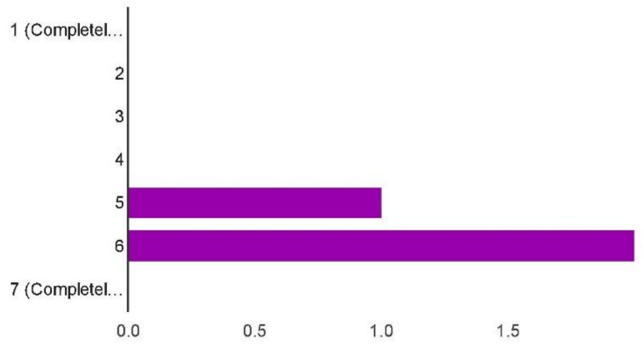
1 (Very unrealistic)	**0**	0%
2	**0**	0%
3	**2**	66.7%
4	**1**	33.3%
5	**0**	0%
6	**0**	0%
7 (Very realistic)	**0**	0%

practicable for evaluation of urban electricity network? [Q10. How strongly do you agree that the tool is:]



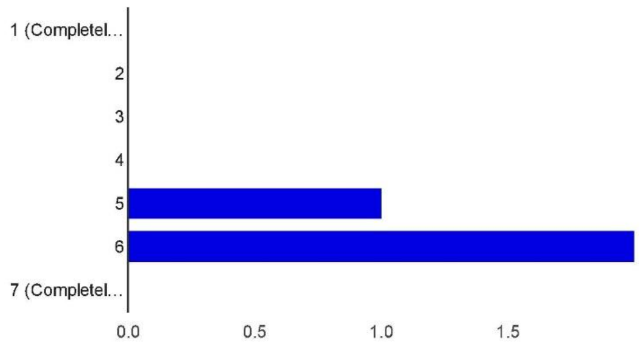
1 (Completely disagree)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**1**	33.3%
5	**1**	33.3%
6	**1**	33.3%
7 (Completely agree)	**0**	0%

fast in providing simulation analysis of urban electricity network? [Q10. How strongly do you agree that the tool is:]



1 (Completely disagree)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**0**	0%
5	**1**	33.3%
6	**2**	66.7%
7 (Completely agree)	**0**	0%

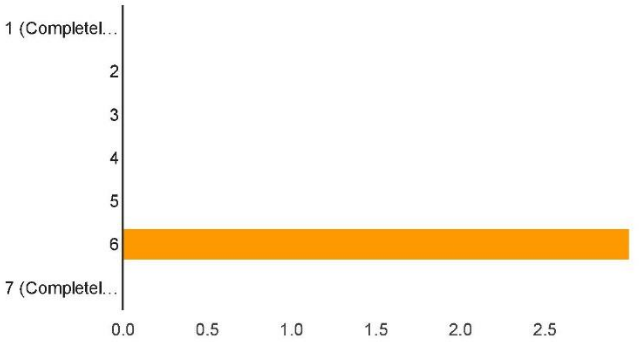
useful in addressing the outage in urban electricity network? [Q10. How strongly do you agree that the tool is:]



1 (Completely disagree)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**0**	0%
5	**1**	33.3%
6	**2**	66.7%
7 (Completely agree)	**0**	0%

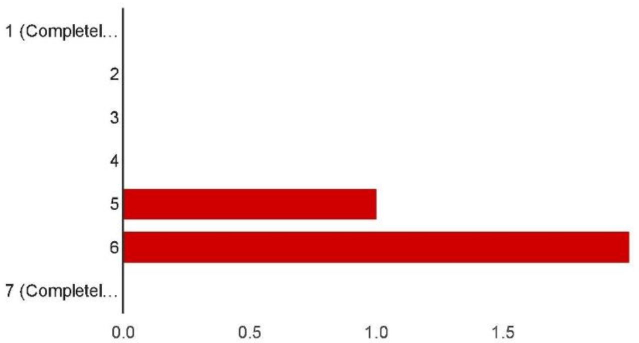
Evaluation of a tool for collaborative grid modelling

as a collaborative decision support system? [Q11. How strongly do you agree that the grid modelling tool is useful:]



1 (Completely disagree)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**0**	0%
5	**0**	0%
6	**3**	100%
7 (Completely agree)	**0**	0%

in establishing a collaborative planning framework among stakeholders? [Q11. How strongly do you agree that the grid modelling tool is useful:]



1 (Completely disagree)	**0**	0%
2	**0**	0%
3	**0**	0%
4	**0**	0%
5	**1**	33.3%
6	**2**	66.7%

7 (Completely agree)	**0**	0%

Q12. What would you suggest to improve the tool?

1. Multiple nodes with the same type of consumer 2. Consider capital cost of components 3. Remove dependency of hard-coding of node types 4. Flag unrealistic configurations 5. Allow savings of scenario configurations so that they may be easily returned to (loaded)

1. Account for commercial costs of installing equipment. 2. Factor in real-world scenario of city expansion and practical requirements of city planners. 3. Integrate flexibility to allow for city configurations. 4. A better user-friendly interface that is simpler to operate.

1. The calculations and scope of what the tool is attempting to do, is great. Some development to the interface to allow quick running of multiple iterations would be great. 2. Perhaps the ability to save output parameters for comparison later would help? 3. A breakdown of the cost savings to show exactly where changes affect the whole figure would be useful.

G QUESTIONNAIRE FEEDBACK FROM STAKEHOLDER WORKSHOP – PART 2

Stakeholder #1:

1. The collaboration framework (I attached a scheme of it to this email);
I think the scope could be widened to include all stakeholders, but is a great basis already.
For the intended audience I fell it could be 'jazzed up a little'

2. Applicability and practicability of the tool;
I *felt the tool was almost immediately applicable, but I do think there needs to recognition that cross connections will also exist in addition to the vertical hierarchy. As a tool to explore islanding, it will need to additionally consider the transition from grid to microgrid and back again, especially in relation to the frequency master.*

3. Efficiency of the tool;
I feel the tool has a lot to offer but needs further development, essential will be the facility to save configured networks so they can be reloaded and returned to at a later date
Usability also needs to be improved, it was apparent at the workshop that considerable familiarity with the tool was needed to use it in its current form, it will be important that a user with domain knowledge but little else be able to use the tool.

4. Market opportunity for the tool.
I think there is a commercial use for the tool, but only once it has been enhanced to offer the save/load functionality and after further testing. This was supported by Stakeholder #2 (who can be considered independent). The tool could be marketed as both the resilience tool it was designed to be and also as a basic system arrangement capture and documentation tool, the later may be of particular interested to city planners and DNO/DSO seniors that may not understand the detailed technical information on existing diagrams (where they exist).

Stakeholder #2:

Based on my understanding - I see opportunity in the ongoing development of the tool. From my perspective the ability of the tool to assist with network congestion is a very important aspect and should be of value to utility companies. I understand there is an aspiration for the tool to be of value to city planning departments. I think this is possible. However I see an immediate benefit if the tool were to be road tested with some utility companies so that the concept can be proved and validated. This would help define the next steps of activity and help make the product adaptable to a range of potential market sectors.

H 2015 CuriousU feedback questionnaire

		Q1 How would you describe the difficulty of the task you just completed? 1 (Very easy) to 5 (Very Difficult)		Q2 How satisfied are you with the tools provided to complete the task? 1 (Not Satisfied) to 5 (Very Satisfied)		Q3 How would you rate the amount of time it took to complete the task? 1 (Very little time) to 5 (Too long)		Q4 How much do you agree with the final version of the model? 1 (Don't agree) to 5 (Fully agree)	
		SCORE	COMMENT	SCORE	COMMENT	SCORE	COMMENT	SCORE	COMMENT
Group 1 (software - symbols)	Participant 1	3	Because we are not really in the energy stuff, but the task was understandable	4		3		2	It's really simple
	Participant 2	2	Becuse we got the information and example on paper	4	Because it's not hard to use the tools	4	Because we need tome to think about the right structure	3	
	Participant 3	2	It wasn't diffuclt, everyhting was clear	4		2	Because it's a lot of things we needed to do and time was already finished	3	Because of the time, we couldn't do it properly.
	Participant 4	1	There aren't any limitations (budget contraint, land constraint) in designing the smart campus	3	The tool is ok but the method isn't so effective since there are too many persons in one group	1		4	
	Average	2		3.75		2.5		3	
	stddev	0.70711		0.433		1.118		0.7071	
Group 2 (software - boxes)	Participant 5	4				3		2	
	Participant 6	4		2		2		2	
	Participant 7	3	On the one hand easy buton the other hand I've never done things like this before so difficult to think out of the box	4	It works. Everything was given what we expected	3	Good timing	4	Regarding the conditions, agree with the model
	Participant 8	3		3		2	More time needed for discussions	4	Not sure it accurately reflects the campus
	Participant 9	3	Never did it before	4		4	It was the right amount of time		
	Participant 10	3		2		3		5	
	Participant 11	3		2		3		2	
	Average	3.28571		2.8333		2.8571		3	
	stddev	0.5		0.8165		0.5		1	

I 2016 CURIOUSU FEEDBACK QUESTIONNAIRE

18 signed Informed Consent Forms;
17 answered questions on Grid Evolution;
12 answered about ArgueSecure;
18 answered about IRENE;
17 answered about Comparing approaches (with two papers being just the same)

maybe better to use barcharts for each of the characteristic...

		Difficulty	Time	Understandability	Correctess of the result	Completeness of the result	Enjoyment	3-step process is clear	3-step process is useful
ArgueSecure	avg	2.545454545	3.5	3.75	3.333333333	3	4.166666667		
	std	0.934198733	1.167748416	0.965307299	0.651338947	1.12815215	0.83484711		
IRENE WP2	avg	3.277777778	3.611111111	3.277777778	3.666666667	3.833333333		3.5	3.833333333
	std	1.017815166	0.777544316	0.95828005	0.48507125	0.707106781		0.857492926	0.985184366
		AV: difficulties due to students' background?	AV: answers include 'education time'?	AV: no inter-table discussions during the exercise?					

Questions:

Evolution of critical infrastructures

1. How much do you agree with the future grid we just envisioned? (1=Completely disagree; 5=Completely agree)
2. How would you rate the difficulty of selecting a future grid scenario from the 2x2 matrix? (1=Very easy; 5=Very hard)
3. Do you think that there are other potential future scenarios worth considering, except the ones in the 2x2 matrix? (Y/N)
4. If yes, which could these be? (Open question)
5. How would you rate the difficulty of selecting future grid components based on the selected future grid scenario? (1=Very easy; 5=Very hard)
6. If you rated the difficulty as 3 or higher, please explain why. (Open question)

Informal, qualitative risk assessment

7. How would you rate the difficulty of identifying risks with ArgueSecure? (1=Very easy; 5=Very hard)
8. How would you rate the amount of time needed to conduct an informal Risk Assessment with ArgueSecure? (1=Very short; 5=Very long)
9. How understandable do you think the final result is? (1=Hard to understand; 5=Easy to understand)
10. How correct do you think the final result is? (1=Very incorrect; 5=Very correct)
11. How complete do you think the final result is? (1=Very incomplete; 5=Very complete)
12. Did you enjoy using ArgueSecure? (1=It was boring; 5=It was fun)
13. How would you improve ArgueSecure? (Open question)

Formal, quantitative risk assessment

14. How would you rate the difficulty of identifying threats with IRENE? (1=Very easy; 5=Very hard)
15. How would you rate the amount of time needed to conduct a formal Risk Assessment with IRENE? (1=Very short; 5=Very long)
16. How understandable do you think the final result is? (1=Hard to understand; 5=Easy to understand)
17. How correct do you think the final result is? (1=Very incorrect; 5=Very correct)
18. How complete do you think the final result is? (1=Very incomplete; 5=Very complete)
19. How would you improve IRENE? (Open question)
20. Consider the process of (1) constructing a model of a grid, (2) selecting a future grid scenario and future grid components and (3) identifying emerging threats with IRENE.
    - 20a. This process is clear (1=Strongly disagree; 5=Strongly agree)
    - 20b. This process is useful (1=Strongly disagree; 5=Strongly agree)

Comparing the various approaches to risk assessment.

21. What do you think are the strengths and weaknesses of each of the two approaches presented (informal risk assessment with ArgueSecure versus formal risk assessment with IRENE) (Open question)

Evolution of critical infrastructures, numbers 1-5 are from 'Very Low' to 'Very High'

Num	1. Agreement with the future grid	2. Difficulty of selecting a future grid scenario using 2x2 matrix	3. Are there more scenarios than in 2x2 matrix?	4. Remarks about scenario, if question 3=.T.	5. Difficulty to select grid components	6. If the difficulty >= 3, please explain why (Open question)	
1	3	4	Y	Culture	2	due to technology policy	
2	3	4	N		2		
3	3	3	N		1		
4	4	3	N		2		
5	3	3	N		2		
6	4	3	N		2		
7	3	3	N		2		
8	4	3	Y	Building energy efficiency	2		
9	3	4	Y	Taking into account feasibility (economic) and social acceptability	3	very unpredictable	
10	4	3	N		4	Not aware of the progress of current technologies	
11	4	4	N		3		
12	4	4	Y	Internediate one, not only low-high	3		
13	4	3	Y	+ houses; electric cars; solar panels	4	by analysis recent technological changes this components are the most expected	the chosen components? (the three elements chosen by the group
14	3	4	N		2		
15	4	3	Y	[no text here]	3		
16	3	4	Y	users (traffic? industry? household?)	4	I think any of these can be different from country to country, e.g. politics and economics. Especially for 'solar' solution, I'm not that optimistic, as it brings in a lot of pollution during production	
17	4	2	N		1		
avg	3.529411765	3.352941176			2.470588235		
std	0.514495755	0.606339063			0.943242218		

Informal, qualitative risk assessment, numbers 1-5 are from 'Very Low' to 'Very High'

Num	7. Difficulty of identifying risks	8. Time needed for an informal RA	9. Understandability of the result	10. Correctness of the result	11. Completeness of the result	12. Enjoyment of use ArgueSecure	13. How would you improve it
1	1	2	5	3	3	4	It's a good idea to give the database 'selected'(?) with all kinds of possibilities
2	3	3	3	3	3	3	create a hard software
3	3	3	4	4	5	4	
4	[no answer]	1	2	3	2	3	You may give info about the the background of the application
5	4	4	3	4	3	4	
6	3	4	3	2	2	3	Nice interface but no way to moderate quality or structure. Maybe some predefined templates?
7	3	4	5	3	4	4	
8	3	4	3	4	4	5	It goes too sideway long
9	2	3	5	4	3	5	
10	3	5	4	4	4	5	
11	1	5	4	3	1	5	
12	2	4	4	3	2	5	
avg	2.545454545	3.5	3.75	3.333333333	3	4.166666667	
std	0.934198733	1.167748416	0.965307299	0.651338947	1.12815215	0.83484711	
	(without row 4)						

Formal, quantitative risk assessment, numbers 1-5 are from 'Very Low' to 'Very High'

Num	14. Difficulty to identify threats with IRENE	15. Time needed for a formal RA	16. Understandability of the result	17. Correctness of the result	18. Completeness of the result	13. How would you improve IRENE	20. Consider a 3-step process: construct grid model; select future grid components; identify emerging threats 20a. Process is clear	20b. Process is useful
1	5	3	4	4	4		2	2
2	5	3	4	4	4	NO IDEA	2	2
3	5	4	2	4	4		4	2
4	3	4	2	3	4		3	4
5	3	3	5	3	3		3	3
6	3	4	4	3	3		3	5
7	3	3	3	3	3		4	4
8	4	4	3	4	4		4	4
9	4	4	2	4	3		2	4
10	3	4	4	3	3		4	4
11	3	2	3	4	4		4	5
12	3	3	3	4	5	easier	4	5
13	2	4	4	4	4	Consideration of external factors, showing the level of threat of a particular entity	4	4
14	4	5	4	4	5		4	5
15	2	3	4	4	5	The language was technical for non expert in the matter, should be given in customers language not experts language. We know basic stuff.	3	4
16	3	5	4	4	4	Introduce a 'stard' (?) procedure that can be applied to different system	4	4
17	2	4	2	4	4		4	4
18	2	3	2	3	3		5	4
avg	3.277777778	3.611111111	3.277777778	3.666666667	3.833333333		3.5	3.833333333
std	1.017815166	0.777544316	0.95828005	0.48507125	0.707106781		0.857492926	0.985184366

21. What do you think are the strengths and weaknesses of each of the two approaches presented
(informal risk assessment with ArgueSecure versus formal risk assessment with IRENE)

1	Informal risk assessment: strengths- easy to understand; weaknesses - not very completely accurate. Informal risk assessment: strengths- a little hard; weaknesses- comparably accurate.
2 (same as 1)	Informal risk assessment: strengths- easy to understand; weaknesses - not very completely accurate. Informal risk assessment: strengths- a little hard; weaknesses- comparably accurate.
3	AS -> W. You don't have to find every risk -> it's just about brainstorming; S. - really easy to create. IRENE: W. The amount of risk couldn't be always well picked and than it could influence the result; S -> may find more risks than AS
4	I do not have enough 'accumulation'(?) about cyber things. So I cannot judge.
5	Both are useful.
6	User friendly (ArgueSecure). Not userfriendly (IRENE).
7	be laid on how STRUCTURAL and EMERGING THREATS are depicted. STRENGTH: ArgueSecure- Qualitative and can consider many more quality factors; IRENE - Effective in terms of time & Cost & Effort.
8	IRENE seems the most complete tool (but not understandable 'cause I have a different background); ArgueSecure was easier but incomplete when it comes to identify threats
9	AS: imaginative, interesting. IRENE - Complete, more useful.
10	ArgueSecure is more visualized but it is a kind of brainstorm, it is not specific and accurate. IRENE is useful and professional but hard to analysis.
11	ArgueSecure: Strengths - 1) Easy to understand, 2) Good interface, 3) Promotion of brainstorming by facilitating good ideas, 4) Consideration of multiple opinions; Weakness - 1) No filter on quality of risk threats, 2) No way to rank threat level. IRENE: Strength - 1) Shows all possible connections, 2) Shows new ideas; Weakness - 1) No way to rank threats, 2) Does not consider external factors.
12	ArgueSecure: Strength - Easier to operate, Simple system; Weakness - Not precise. IRENE: Strength - Precise calculation, More computational (maybe more cool features available); Weakness - Not interpretable easy.
13	ArgueSecure is easy to use, easy interface.
14	ArgueSecure is more free to play with brainstorming while IRENE is more "formal" and straight forward, more hard data.
15	ArgueSecure: very scattering opinion (assessment) like brainstorming. IRENE: 1) formal & Risk are categorized into different aspects/steps, the whole Risk assessment is more in detail & easy understandable, 2) Step by Step assessment, a standardized procedure and more efficient.
16	ArgueSecure: expand the area where we think about or analyze the risk. But the ideas are relatively random and insystematic. IRENE: more concrete and systematic but covers some of the unseen but possible risks.
17	ArgueSecure: Strength - defender arguments could be marked at any time during the assessment; each attacker argument could be counted. Weakness: Creating a new risk could be not accurate enough.