



FP7 Grant Agreement N° 312450

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Project type: Network of Excellence (NoE)

Thematic Priority: FP7 Cooperation, Theme 10: Security

Start date of project: March 1, 2013 Duration: 48 months

D5.5 Report on the Secure Design of Next Generation Infrastructures (NGI)

Due date of deliverable: 28/02/2017

Actual submission date: 10/02/2017

Revision: Version 1

Nederlandse Organisatie voor toegepast natuurwetenschappelijk onderzoek (TNO)

Project co-funded by the European Commission within the Seventh Framework Programme (2007–2013)		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Authors	Marieke Klaver (TNO) Eric Luijff (TNO) Michal Choras (UTP) Vittorio Rosato (ENEA)
Contributor	Theo van Ruijven (TNO)

Security Assessment	See deliverables table for security assessment requirements
Approval Date	Gregorio D'Agostino (ENEA) 06/02/2017 Dominique Sérafin (CEA) 06/02/2017
Remarks	No Security Issues

The project CIPRNet has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 312450.

The contents of this publication do not reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the authors.

List of Abbreviations

Acronym	Explanation
C2M2	Cybersecurity Capability Maturity Model
CAD	Computer-Aided Design
CC	Cloud Computing
CEN	Comité Européen Normalisation
CENELEC	European Committee for Electrotechnical Standardisation
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CIPRNet	Critical Infrastructure Preparedness and Resilience Research Network
CIR	Critical Infrastructure Resilience
CPS	Cyber-Physical System
DER	Distributed Energy Resource
DSO	Distribution System Operator
DSS	Decision Support System
Dxy	Deliverable number y for Work Package x
ECN	European CIIP Newsletter
EEGI	European Electricity Grid Initiative
EERA	European Energy Research Alliance
EII	European Industrial Initiatives
EISA	(US) Energy Independence and Security Act
EISAC	European Infrastructures Simulation & Analysis Centre
EM	Emergency Management
ENTSO-E	European Network of Transmission System Operators for electricity
ETP	European Technology Platform
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
GSGF	Global Smart Grid Federation
GWAC	Gridwise Alliance Architecture Council
IEA	International Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IPT	Intelligent Public Transport
ISGAN	International Smart Grids Action Network

Acronym	Explanation
JRC	(EU) Joint Research Centre
KIC	Knowledge and Innovation Community
MOOC	Massive Open Online Course
MS&A	Modelling, Simulation and Analysis
NGI	Next Generation Infrastructure
NIST	(US) National Institute for Standards and Technology
NMDC	(NL) National Model and Data Centre
NRF	Network Resilience Function
PESTLE	Political, Economic, Social, Technological, Legal, and Environmental
PV	Photo-Voltaic
RFID	Radio-Frequency IDentification
SCCM	Smart City Concept Model
SETIS	Strategic Energy Technologies Information System
SG	Smart Grid
SGAM	Smart Grid Architecture Model
SGMM	Smart Grid Maturity Model
TSO	Transmission System Operator
VCCC	Virtual Centre of Competence and expertise in CIP
WPx	Work Package x

TABLE OF CONTENTS

LIST OF ABBREVIATIONS	3
TABLE OF CONTENTS	5
LIST OF FIGURES.....	6
LIST OF TABLES.....	6
1 INTRODUCTION – RATIONALE OF THIS DOCUMENT	7
1.1 Objective	7
1.2 Scope.....	7
1.3 Approach used	7
1.4 Structure.....	7
2 NEXT GENERATION INFRASTRUCTURES (NGI)	8
2.1 Drivers for NGI.....	8
2.2 Why modelling, simulation and analysis of NGI?.....	13
2.3 NGI move to complex adaptive systems	14
2.4 Need for Security and Secure Design	15
2.5 What EISAC services could be used by NGI?.....	15
3 CASE STUDY 1: THE SECURE DESIGN OF SMART GRIDS	16
3.1 Smart Grid Communities – short description	17
3.2 Types of Smart Grid models	18
3.3 Types of analysis that the Smart Grid Community requires.....	23
3.4 Types of analysis that might be provided by EISAC.....	25
4 CASE STUDY 2: THE SECURE DESIGN OF INTELLIGENT GRIDS	26
4.1 Intelligent Infrastructure/Grid Community – short description	26
4.2 Types of existing models	27
4.3 Main challenges for the Intelligent Infrastructure/Grid Community	29
5 CASE STUDY 3: USE OF CIPCAST/RECSIM FOR COST-EFFECTIVE GRID UPGRADES	30
5.1 RecSIM application	30
5.2 Case example: Risk-based planning of NGI.....	33
5.3 Case example: Monitoring and control in Smart Grids	33
6 OUTREACH TO NGI COMMUNITIES.....	35
6.1 Description of communities.....	35
6.2 Feedback of these communities on the possible use of EISAC services.....	38
6.3 Summary: MS&A for NGI which may be provided by EISAC @TNO	39
7 CONCLUSIONS ON THE POSSIBLE ROLE OF AN EISAC IN THE SECURE DESIGN OF NGI.....	41
7.1 Summary of the findings.....	41
7.2 Further development of MS&A services focused on NGI.....	42
8 REFERENCES	43

List of Figures

Figure 1: Bridges constructed in the 60s are still heavily used today [Beeldbank1].....	8
Figure 2: US bridge: “nearly 10 percent of the 600,000 bridges in the United States are structurally deficient” [Meko] (the red dots).....	9
Figure 3: Limited space for infrastructure renewal (source: [Beeldbank2])	12
Figure 4: SGAM Framework [SGAM]	20
Figure 5: NIST Conceptual Domain Model [NISTSG].....	21
Figure 6: NIST Conceptual Architecture mapped onto the Architecture Matrix Service Orientation and Ontology [NISTSG]	22
Figure 7: Agent-Based Modelling of smart grids including autonomous behaviour of the prosumer (source: [SGJRC])	24
Figure 8: ENISA's interaction layer model [ENISA]	27
Figure 9: A SCCM view [PAS182].....	28
Figure 10: ENISA's model of smart city stakeholder interaction [ENISA].....	29
Figure 11: Distribution of kilominutes of outages resulting from the shut-off of each of the 100 cabins of a specific tract of the Roma network.....	32
Figure 12: Same distribution of fig.9 made on the network after a single modification (cabin SS98 transformed from its current state of a not telecontrolled cabin into a telecontrolled cabin)	32

List of Tables

Table 1: Service groups and services for NGI (dark blue/white: key; brown: supporting).....	15
Table 2: SGMM maturity levels.....	23
Table 3: Types of analysis that EISAC nodes may provide regarding Smart Grids	25
Table 4: Types of analysis that EISAC nodes may provide with CIPCast/RecSIM	32
Table 5: Types of services for NGI that EISAC may provide (summary)	40

1 Introduction – Rationale of this document

1.1 Objective

According to the description of work (DoW), CIPRNet, the VCCC and EISAC will support developers of Next Generation Infrastructures (NGI):

- to validate the robustness of their architecture and resilience of the design,
- to verify the robustness and resilience of the NGI with respect to its critical dependencies with other Critical Infrastructures (CI),
- to validate the effectiveness of NGI emergency management processes in relation to new emergency challenges related to the NGI structure and CI dependencies.

1.2 Scope

As part of CIPRNet's outreach to the various Next Generation Infrastructure (NGI) community(ies) in Europe, this report will use smart grids as an example for the role that the future EISAC may play in support of the secure design of next generation infrastructures such as smart grids.

1.3 Approach used

The following approach was used to reach the objectives of this deliverable:

1. Desk research (chapter 2);
2. Three case studies: on smart and intelligent grids (chapters 3 and 4) and on the use of the RecSIM for cost-effective infrastructure upgrades (chapter 5);
3. Discussions with and outreach to potential stakeholders of a future national EISAC node (chapter 6);
4. Synthesis (chapter 7).

1.4 Structure

Chapter 2 is based on the outcomes of desk research into the drivers for studying Next Generation Infrastructures (NGI), the way modelling, simulation and analysis (MS&A) is used in or may support NGI, and the way future EISAC service offerings may be of value to the NGI communities of stakeholders.

Chapter 3 contains Case study 1: the secure design of smart grids and the type of analysis to be provided by EISAC that may support this R&D domain. In chapter 4, one may find Case study 2 on the secure design of intelligent grids. As an example of support by MS&A to the intelligent grid community, the RecSIM tool is described in chapter 5.

Chapter 6 provides an overview on the discussions with NGI stakeholders about their needs for possible services by a national EISAC node. Chapter 7 provides the synthesis and discusses the possible role of EISAC for the NGI community.

2 Next Generation Infrastructures (NGI)

In this section, we present the importance of Next Generation Infrastructures (NGI) in the context of Critical Infrastructures (CI) MS&A and describe the relevant drivers for NGI.

2.1 Drivers for NGI

2.1.1 Aging of infrastructures

Many of our infrastructures have been designed and installed many decades ago. Some typical operational lifetimes are:

- Dikes along rivers and polders have been put in place several hundreds of years ago.
- Road tunnels are designed with a 100 years' lifespan in mind [NO], but technical systems have a much shorter lifespan [PIARC]. The Maastunnel in Rotterdam was built between 1937 and 1942. A complete technical renovation will start mid of 2017 and will take two years.¹
- Bridges are designed and build to last some 100 years ([Rijkswaterstaat]). Structural upgrades and major overhauls may extend the lifetime manifold, but often maintenance and upgrades are performed late. [Meko] stated that in Nebraska „*older bridge spans make up 60 percent of deficient bridges; one in five bridges were built in the early 1930s*“. On the other hand, some Roman build bridges are still used today carrying modern cars.



Figure 1: Bridges constructed in the 60s are still heavily used today [Beeldbank1]

- Asphalt roads have a typical lifespan of 25 years. Technical traffic systems, for instance lane signals, traffic jam warnings and so on may operate some forty to fifty years when maintained well.
- Metro systems may use trains, cabling systems, and control systems that are intended to last 30 to 50 years. In 2010, an accident report about Washington's DC metro states "*The remote terminal units on the Metrorail system are electronic data multiplexing systems with varying installation dates; some have been in place as long as 35 years. The original units are hardware-based devices using discrete logic chips ...*".
- Drinking water transport pipelines are planned to last some 60 years (e.g., [Oasen]), but longer time periods occurs, e.g. New York's drinking water transport aqueducts and reservoirs which bring water from Upstate New York to the New York City comprises of:
 - The New Croton Aqueduct completed in 1890,
 - The Catskill Aqueduct completed in 1916, and

¹ Special attention is required as the tunnel constructed with sunken elements is a first of its kind in the world and has the status of national monument.

- The Delaware Aqueduct completed in 1945.
- Sewage system pipelines have an average lifetime of 60 years, but depending of the soil type and the building activities above the ground the lifetime varies from 30 to 100 years in the Netherlands [RioNed]; in France and the UK 19th century sewage systems are still being used [Masood].
- Underground power distribution and copper telecommunication cables have a lifetime of up to 50 years.
- Long-haul oil and natural gas pipelines have been put in place in the 60's and early 70's across Europe and the USA. The average lifetime of gas grid in the Netherlands is 45 years, while most infrastructure was put in place between the 60's and 90's. [Alem].

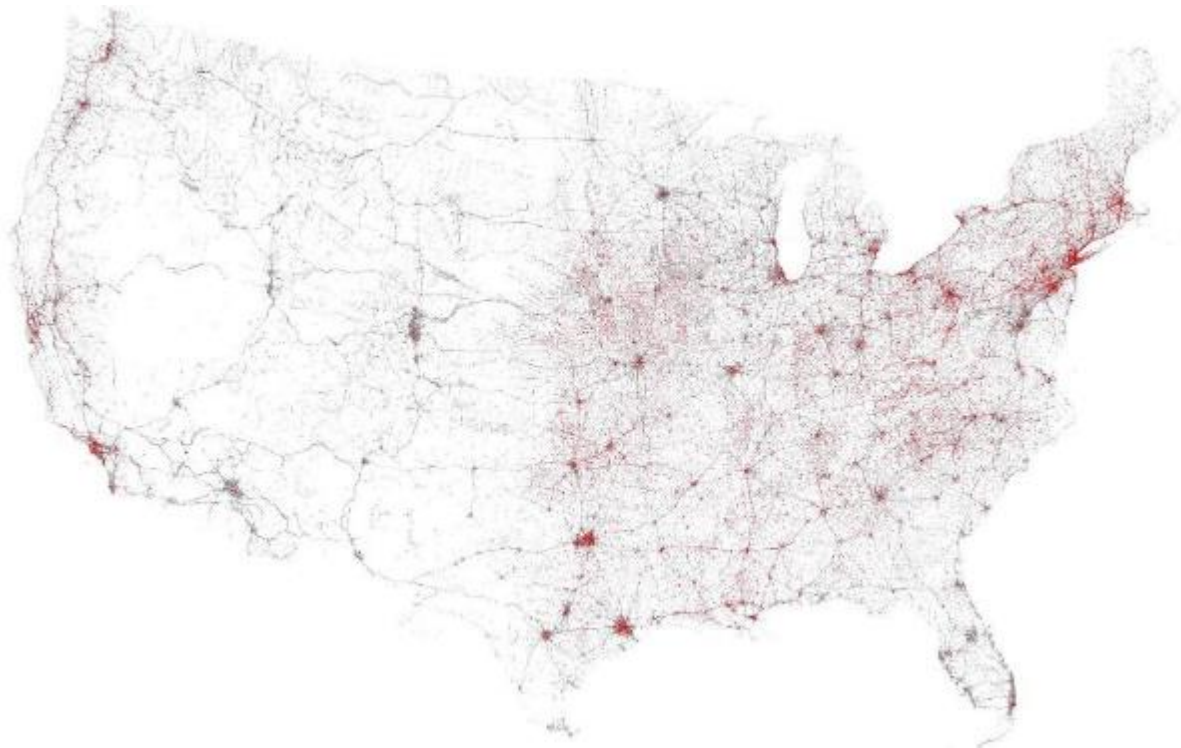


Figure 2: US bridge: “nearly 10 percent of the 600,000 bridges in the United States are structurally deficient” [Meko] (the red dots)

Aging of infrastructures may become a worrying challenge for our CI unless careful maintenance schemes are applied, knowledge is kept actual, and there is no lack of spare parts (see [Luijff2014]). For example, more than half of the US pipelines are at least 46 years old. Not only economically when one must replace the infrastructure, but also from the aspect of safety for the population. Pipeline explosions of old pipelines have occurred several times in the past years as pipelines may corrode after forty to fifty years, see e.g. [Sider].

In addition, the trend is to add information and communication technologies (ICT) to key elements of the physical infrastructures. Where old process control technologies may have an operational lifespan of several decades, the use of modern technologies drastically reduces that lifespan. Like the office environments, the move to software with the continuously increasing need for faster decision-taking and control, and the need for more and more sensor inputs require more processing power and doubling of the size of memory elements each couple of years. This drives the need for major updates of the technical parts of infrastructures faster than infrastructure operations were used to.

Another trend is to outsource the maintenance of infrastructures to third parties which workforce is not concerned about reporting more structural decaying aspects of infrastructures as a next day repair will provide work. Structural maintenance with aging may cause surprisingly prolonged outages.

2.1.2 Privatisation and unbundling

Privatisation of infrastructures caused a move towards a different model of operations. When exceeding its technical lifespan, publicly operated infrastructures start with the replacement of the old infrastructure (components) irrespective assessments that a much longer operational lifespan is feasible. With privatisation and unbundling it is reversed. The bean-counters will ask how long a CI element can be used after its technical lifespan. When there is no clear and urgent answer, any plans for replacement will be postponed. Decisions are taken on commercial grounds: only when regular breakdowns occur affecting the imago of the operator, when authorities start complaining, or when customers start to move to competitors, actions are taken.

2.1.3 Urbanisation pushing current infrastructures to the limit

Most infrastructures in cities are hidden underground to the public, e.g. cables and pipelines. Key infrastructure elements are hidden behind high walls, in man holes, steel boxes, and behind non-descript doors, e.g. lift stations, drinking water storage tanks, gas pumps, transformers, and cable distribution boxes. An international trend, also in Europe, is urbanisation. A movie about the growth of Amsterdam since the year 1000 is illustrative to that [Amsterdam]. Cities develop into megacities, a trend that is observed in Europe as well [EUUrban]. Infrastructures are extended further and further, stressing the old infrastructures and their key elements. It is often hard to meet the extra needed capacities. Infrastructures are therefore operated near their operational limits daily where their design was based on a maximum peak of some 50%. Therefore, just a small system overload because of a minor incident may cause a wider area collapse of services. The combination of aging and near to overload operational conditions due to privatisation and urbanisation may result in unreliable operating infrastructures.

2.1.4 Climate change risk and sustainability

Climate change may pose additional risk, and thus challenges, to CI [RAEng]. The effects of extreme weather events such as “water bombs”, “flash floods” and extreme thunderstorms, prolonged heat waves, and drought may have effect on CI. For example, “*according to 2013 data from the Department of Energy (DOE), the US power grid outages have risen by 285% since records on blackouts began in 1984, for the most part driven by the grid's vulnerability to unusual and extreme weather events*” [USpower]. Authorities, critical sector operators and other CI stakeholders in Europe and beyond have a notion about climate change and the need for adaptation of infrastructures, e.g. [DEFRA] and [RAEng]. On the other hand, there is still a lack of insight in the dimensions of the climate change problem, the possible impacts, and the possible countermeasures and solutions. Various European climate change reports express this uncertainty: “More knowledge about climate change effects, extreme weather conditions and impact on CI is required” (e.g. [Benelux]).

At the same time, more extreme weather events already hit infrastructures for instance by flooding, extreme thunderstorm and wind events, and droughts. Overhead power lines and

pylons have been downed due to wind speeds exceeding the 1:500 of 1:1,000-year design conditions ([AUS280916], [Tennet140710]).

The drive for sustainability and reduction of greenhouse gasses in combination with new technologies may result in disruptive infrastructural changes, for example the drive to replace the gas distribution infrastructure by electric power for heating and cooking [Alem], and to replace owned cars by on-call autonomously moving transport vehicles.

“In 15 years, more electricity will be sold for electric vehicles than for light.”

Thomas Alva Edison (1910)

2.1.5 Limited space for infrastructures

Infrastructures require zoning space for safety and security reasons. Space for infrastructure is very limitedly available and therefore costly, especially in urban areas. Maintenance, incident response and renewal may require access to the infrastructure. Insufficient zoning or some deviations in the original planned routing of infrastructures as found on maps may result in cut glass fibres, broken water mains, shorts in the power grid and or broken gas pipelines when contractors start digging. An example is the accident in July 2004 when 24 people died and more than 150 were seriously injured in Ghislenghien, Belgium following construction damage to the Fluxys high-pressure gas pipeline [CEMAC].

Infrastructure renewal brings some other negative societal aspects as well. First, people and shops in cities are complaining that the repair crew for the pavement after renewal of one infrastructure is followed within a day by a crew starting the digging for work on the next infrastructure, and so on. In rural areas, landowners and environmental groups oppose and delay the permit and land acquisition process required for new infrastructure. The timespan between planning and the realisation of a power transmission line easily takes ten to fifteen years. [Sider]

Moreover, in some narrow corridors multiple critical infrastructures may use the same tunnel as became clear when several cars of a CSX train derailed in the Howard Street tunnel in Baltimore and ignited a fire in 2001. Drinking water, power, telephone and internet with global impact, were some of the affected infrastructures. In June 2016, another train derailed at the same location but luckily no fire ignited.

In a similar way, glass fibres of multiple operators may be obliged to make use of the same duct. Moreover, the redundancy provided by a ring-architecture fails when two sides of the ring are squeezed into the same duct. An incident affecting the duct will mean that all telecommunications of multiple telecommunication operators and their (critical) customers such as 1-1-2 and police are out-of-service. It is therefore required that a careful safety and security design takes place when multiple infrastructures are routed alongside of each other or cross each other.

As most long-haul infrastructures in the UK have aged sometimes far beyond their technical life expectancy, it has been proposed to address the renewal or major overhaul of infrastructures not on a case by case basis but to plan for the replacement of all infrastructures and their zonal planning in a single effort. That would save a lot of costs as the crossing of infrastructures and natural features, e.g., a road, railway, river, and canal must be addressed only once.



Figure 3: Limited space for infrastructure renewal (source: [Beeldbank2])

To do that properly by looking forward for the next 30 to 50 years, one needs to assess all threats (including cyber threats), climate change effects and all other challenges, partly from the set of unknowns. Modelling, simulation and analysis (MS&A) of infrastructures, their dependencies, vulnerabilities and related risk to the population may provide inside in pros and cons of the various zoning options. A major challenge is to get all, mostly private, infrastructure owners to take part in such an approach. In the end, a cost-effective renewal of infrastructure may save society a lot of costs and may result in a much higher performance of the infrastructure services.

2.1.6 Drive towards smart investment in renewal of infrastructures

As discussed above, replacement of infrastructures, especially when it concerns underground, ground level and overhead infrastructures may be complex and costly. For example, US national power grid is currently valued at 876 billion dollars. The most important parts of the grid were developed after the second world war and currently supplies power to 150 million customers through more than five million miles of power lines and around 3,300 utility companies. Upgrading of the national grid will cost 150 billion dollars a year. Moving to a smarter national grid with better protection against blackouts will cost somewhere between 338 and 476 billion dollars [USpower].

Across the world, infrastructure operators are facing the challenge that many infrastructures reach the end of their technical lifetime soon as many were developed in the rebuilding and expansion period of nations following the second world war. Combining the renewal of multiple infrastructures and making them ‘smart’ at the same time may reduce costs considerably, even when intended replacement is performed earlier than planned. Smart investments therefore may save (some) money that can be used for taking additional redundancy measures. The need to collaborate and replace/renew multiple infrastructures simultaneously may not be clear immediately to each individual operator as it will require more coordination. MS&A may show the joint benefits to all companies and the authorities.

Please note that the simultaneous upgrade of all infrastructures, increases the risk involved. Again MS&A may help to identify and analyse the risk involved and make sure that the design is secure and robust.

2.1.7 Resilience of NGI against deliberate attacks

Infrastructures in general and NGI in particular may be vulnerable to deliberate attacks, e.g. by terrorists. Proper analysis and design may increase the resilience of the infrastructures. MS&A-based what-if analysis is the base methodology which supports such analyses, see e.g. the “Understanding malicious attacks against infrastructures” study [NGIBSIK].

2.1.8 Dependent CI services

There are many dependencies between infrastructure sectors and failure in one may quickly lead to a cascading failure [RAEng]. Understanding dependencies and analyses of cascading and common cause failures is required to make NGI more resilient.

2.1.9 Drive towards smart infrastructures and cities

Given the drivers above, new infrastructure developments include the digitisation of the infrastructures or “smartness”. Moreover, the creation of more efficient and effective end-user services is expected to provide economic benefits and an increase in customer satisfaction. Multi-purpose infrastructure will be more cost-effective, may take less space and could be more resilient, e.g. reservoirs that can be used as flood defences [RAEng].

An example of smart infrastructure is the centralised collection of household waste where the underground containers signal the weight and remaining capacity. The collection of waste can be organised smart and dynamically while optimising the collection scheme and energy consumption of the trucks. The digitisation of dependent infrastructures, urbanisation, adaptation for climate change, urban and environmental planning, self-resilient operations, and a complex governance structure together drive the smart infrastructures and smart cities developments, as well as other “smart” developments. Future, sustainable city developments collectively make up the physical, economic and social systems of our future cities and regions. NGI have an important role in these developments. Some dreams about the future with “plug and play” buildings and infrastructure connectivity may appear sooner than one expects, see e.g. [ARUP].

Mixing the future vision and need for preparing for future infrastructure services with current developments such as smart grids cause some confusion as the notion ‘next generation infrastructures’ is often used as a substitute for smart (grid) infrastructures. In our opinion, NGI research tries to look some thirty years further ahead and derives conclusions from that for currently needed developments.

2.1.10 Hesitation: can we plan NGI?

One hesitation exists. Can we really plan NGI? Some developments in infrastructure services are disruptive. A planned and being built infrastructure may not be needed in ten years’ time! On the other hand, a new service might be that popular that the capacity planning turns out to be factors wrong. Careful planning and making infrastructure sustainable are the policy options to strive for [NGI].

2.2 Why modelling, simulation and analysis of NGI?

All the drivers and challenges mentioned above, require futureproof analysis of infrastructure planning and behaviour. According to [Masood], NGI analysis must identify and understand the user needs as well as the requirements of businesses and of the large set of stakeholders (e.g., public authorities, infrastructure owners, infrastructure operators, infrastructure main-

tainers, regulatory bodies, treasury, and investors). The development of new infrastructures requires so-called PESTLE (Political, Economic, Social, Technological, Legal, and Environmental) analyses: what are the key political drivers of relevance, important economic factors, treasury rules and budget availability, main societal and cultural aspects, current technological imperatives, changes and innovations, current and impending legislation and environmental considerations affecting NGI?

Experimenting with existing infrastructure to derive analysis results is hardly possible. The users of infrastructure services do not accept disruptions and outage risk. Post-mortem analysis of events² in the infrastructure may provide insight to some extent. Testing in testbeds of cyber-physical systems may provide capacities for component level testing and size limited architectural testing.

Analysis of functionalities and new behaviour of NGI including the analysis of multi-infrastructure dependencies in a wider context, however, cannot be performed in existing infrastructures and testbeds. Modelling, simulation and analysis (MS&A) therefore is the obvious methodology to assist researchers, technology developers, and infrastructure planners. MS&A can be used as well to train CI operators and crisis managers for effectively dealing with infrastructure incidents which hopefully will not occur at all. A key issue is the required granularity of the modelling and analysis approach. Can one work with simple functional data or does one need a very detailed component level model with a large data set of parameters? An issue that was discussed in the CIPRNet Master Classes and that will come to the fore in the planning for and development of the European Infrastructures Simulation and Analysis Centre (EISAC).

2.3 NGI move to complex adaptive systems

De Bruijne ([DeBruijne] pp. 399-401) states that there is a fundamental problem with NGI, especially restructured CI. NGI increasingly become complex adaptive systems which cannot be managed just by a risk-based approach. Risk assessments will cause a set of prevention and preparation measures to be taken, but fail to recognise an increased unpredictability of CI behaviour. The unpredictability of the (perceived) threat of large-scale cascading failure, stealthy developing new risk, and more often appearing major incident triggers are inherent to NGI. In Smart Grids, the complexity of factors like a large set of new actors, changed or even fragmented roles and responsibilities of existing actors, and a large set of new threats as discussed in Chapters 3 and 4, may cause unforeseen reactions by these actors regarding the restructuring of existing processes in the energy sector. In the end this affects the reliability of the energy system. Based on his analysis, De Bruijne concludes that infrastructure operators “have a need for flexible response” to find a new operational equilibrium in the restructured setting. This requires “not too much regulation” and “prepare for a system to deal with unplanned reliability threatening events”. He pleads for investing in deep knowledge and experience of operators who operate CI. Based on their knowledge-based judgement, bypassing predetermined procedures, infrastructure incidents may not result in major grid breakdowns. The opposite is true as well. Lack of understanding between connected infrastructure parts caused the blackout of parts of the European power grid in 2006, see (UCTE, 2007). Such understanding requires what-if analysis operator training as well as MS&A of the NGI.

² See CIPedia© for definitions of notions as event, incident, disruption.

2.4 Need for Security and Secure Design

When designing and planning new infrastructure, there is a need to understand both the physical and cyber security issues for society and citizens. How can one mitigate the risk to an acceptable level? Moreover, the set of natural and man-made threats is large. Using MS&A, various architectural design options can be evaluated using a wide range of threats and common cause failures. The results will provide a set of options to decide from a technology and architectural point of view. These results need to be aligned with the other PESTLE factors before a balanced decision can be made on next infrastructure enhancements, infrastructure element replacements, or a new infrastructure layout.

The pitfall of any ICT-based NGI is the focus on functionality disregarding the old lessons identified before in many infrastructures: a lack of cyber security and privacy protection. The vulnerabilities and the risk delay, stall, or even revoke the acceptance by citizens and society of NGI services. Cyber security has always been an add-on after major intrusions and disruption occurred. Security-by-design, already pleaded for by [Tettero] in 1997 shall be the way out, although it is a question whether a thoroughly secure design and implementation of NGI will take place unless the lessons identified in the past about cyber security failures in infrastructures are really learned. Based on historical experiences, however, Luijff has predicted that NGI will fall prey to similar cyber security vulnerabilities as the ones found in the past [Luijff2013].

Table 1: Service groups and services for NGI (dark blue/white: key; brown: supporting)

SERVICE GROUP	Services
Advanced Decision Support	Decision Support (crisis management; operations centre)
	What-if Analysis (planning, crisis management; operations centre)
Training	Training support (crisis management; NGI operations)
	(Inter)national CIP/CIR exercise support
Information Brokerage on CIP/CIR	CIP/CIR Policies and Good Practices
	Knowledge brokerage
	Expert access
Research Platform for CIP/CIR Collaboration	Web Portal Research Platform
	Modelling, Simulation & Analysis
	- CIP/CIR bibliography
Dissemination	Support CIP/CIR conferences
	Support C(I)IP Newsletters

2.5 What EISAC services could be used by NGI?

Considering the main aspects discussed above, stakeholders involved in NGI developments may require a set of services from an EISAC node (see: service groups and services in [D4.7]). Based upon the discussions above, Table 1 highlights the key EISAC services for the secure design of NGI and further infrastructure development.

3 Case study 1: the secure design of smart grids

A Smart Grid (SG) essentially encompasses the smart automation of complete utility grids using various ICT systems, including cyber-physical systems (CPS). The combination of classical grid operations with ICT creates new functionalities and new capabilities to monitor and control a utility grid more efficiently. Moreover, farmers ‘farm’ power with windmills and photovoltaic panels and citizens transform into prosumers: they produce Photo-Voltaic power (PV) in daytime and use power at the night. The network operator needs SG to keep up with the challenges to maintain the balance of the grid due to the distributed energy production [NGIBSIK].

SG is an important concept that yet has a long way ahead before it is fully implemented and becomes an every-day reality. SG research and developments are ongoing and there are different initiatives that are pushing it forward. Currently, most SG technologies developments focus on electricity, but gas, district heating/steam distribution, sewage and drinking water grids will follow suite.

Within the electric power grids, SG can be described as enabling a two-way energy and information exchange between electricity producers/suppliers and the consumers. SG covers the complete energy chain from (central and distributed) generation to consumers and the new role of prosumers. In terms of electricity infrastructure, SG will cover the functional areas of generation, storage, transmission and distribution.

Before we outline some of the standardisation efforts in electric power SG in more detail, it should be noted that there are quite different drivers for adding ICT to the power grid in Europe and the United States. Although in the end technologies will integrate, one shall understand that in the USA the power grid reliability is magnitudes less than that in Europe due to:

- extreme long transmission lines which are vulnerable to storms, thunderstorms, derechos, hurricanes, tornados, winter storms, and wood fires,
- overhead distribution power cables which are vulnerable to broken branches and fallen trees because of the extreme wind and winter conditions,
- transformers hung in overhead systems which are vulnerable to any animal that crawls, gnaws and mates and thus causes shorts and fires.

SG in the USA promise:

- increased grid reliability using islanding techniques where isolated grid parts can continue with a limited service,
- smart load demand management where the current overload of the long-haul transmission lines can be reduced are the main SG priorities,
- insight to Distribution System Operators (DSO) in the size of the area and the count of customers without power as smart meters issue a loss of power message.
- and, secondary, solutions for all energy supply challenges and issues in the USA.

In Europe, the main drivers for SG come from the European Commission’s Climate and Energy Package also known as the 20-20-20 goals for 2020 (20% cut in greenhouse gas emissions, 20% of EU energy from renewables, 20% improvement in energy efficiency; all relative to the 1990 levels) [ECCEP] where a higher energy efficiency, as well as less CO₂ and other greenhouse emissions is aimed for by:

- the use of more Distributed Energy Resources (DER) which comprise all kind of (local) energy production by wind, photovoltaic and other renewable energy means,
- the dynamic matching and control of the demand (e.g., smart appliances) with the dynamics of supply,
- increased use of e-vehicles using the grid to load batteries and possible act as energy supply when needed,

will result in higher energy efficiency, as well as less CO₂ and other greenhouse emissions. Therefore, complete different objectives between the USA (and Canada) and Europe affecting different parts of the power grid. [Luijff2017] These differences shall be kept in mind when trying to understand the SG developments and initiatives described below. This chapter will focus on the SG developments and international standards from the European perspective.

3.1 Smart Grid Communities – short description

There is not a single organisation or initiative at a global or a European level that coordinates the progress in SG technologies and implementations. However, there are thousands of grid operators worldwide that operate in different environments and many solutions emerge to meet their local needs. Therefore, avoidance of this fragmentation of research and of existing solutions is a big challenge.

Facing such challenges, there are some initiatives in SG research and technology implementation that are important in this context and should be mentioned here:

1. At the global level, there exists the **IEEE & Smart Grid** organisation [SGIEEE] that aims at facilitating and guiding the evolution toward SG. It gathers key stakeholders at different events, fosters publications and standards, and hosts a SG-related website. It has 395,000 members being research institutions, governments and companies and their engineers. Therefore, IEEE may raise some critical mass to take a leading role in SG development, identification of lessons during the deployment and evolution of SG. IEEE runs the IEEE Xplore digital library with scientific articles on latest research in SG [XPIEEE]. Nearly 2,500 papers relevant to SGs have been published in over 40 IEEE journals. The events organised by IEEE are e.g. “IEEE Innovative Smart Grid Technologies 2010” and the “IEEE Smart Grid World Forum” [SGIEEEWF]. IEEE has approximately 100 standards and standards in development focused on SG.
2. At the European level, there are several SG-related initiatives. There are approximately 200 SG research, development and demonstration projects. However, the coordination between different activities is lacking. This creates a very big challenge as the lack of coordination results in inefficient use of resources. Moreover, even very good individual activities have a hard way to achieve a real impact on the SG communities.
3. The **European Strategic Energy Technology Plan (the SET-Plan)** is an initiative aiming at accelerating the development and deployment of low-carbon technologies [ECSETP]. It coordinates research and innovation and co-finances projects focusing on technologies enhancement and on ensuring their cost-effectiveness. The SET-Plan was adopted by the European Union in 2008 and it is the main tool supporting decision makers in the European energy policy. The first milestone for the SET-Plan is the 20-20-20 energy transition plan of the European Commission by 2020. The second milestone of the SET-PLAN is 2050, for the worldwide transition to a low carbon economy (limiting climate change to a global temperature rise of no more than 2° C by considerably reducing greenhouse gas emissions). The SET-Plan’s budget is approximately of €71.5 billion. The SET-Plan encompasses several implementation mechanisms, such as the SET-Plan Steering Group, European Industrial Initiatives (EII), the European Energy Research Alliance (EERA) [EERA], and the Strategic Energy Technologies Information System (SETIS) [SETIS]. Note that the 2015 United Nations Climate Change Conference in Paris introduced a new milestone: > 40% less greenhouse gasses, >27% use from renewable energy and >27% higher energy efficiency in 2030. It is expected that the EU will aim at >30% higher energy efficiency.

4. The **European Electricity Grid Initiative (EEGI)** is one of the European Industrial Initiatives that is focused on the SG sector. EEGI is a nine-year programme (until 2018) for research, development and demonstration to foster innovation of the electricity grids. EEGI brings together all stakeholders in the SG sector, such as researchers, industry, EU Member States and the European Commission. The EEGI focus is on system innovation and on integration of new technologies in real life conditions [EEGI].
5. An important initiative that considerably contributes to the SET-Plan is **ERA-Net Smart Grids Plus** [ERANetSG]. Its ambition is to expand the EEGI initiative. ERA-Net Smart Grids Plus gathers 21 European countries and regions with the aim to achieve the SG vision and goals of Europe. The initiative fosters new technologies and market designs, as well as prepares customers to the adoption of new solutions. The members of ERA-Net Smart Grids Plus are entities responsible for national and regional programmes funding research in SG. The initiative is building a structure for cooperation between those entities and with external initiatives at the European level. The initiative promotes the electric power system that integrates renewable energies and is more flexible, efficient and secure, with low greenhouse gas emissions and with an affordable price. It promotes open markets for energy products and services. The initiative also seeks Europe's leading role at the world arena in low-carbon energy technologies. All this requires the research to be both cross-sectoral and interdisciplinary. ERA-Net Smart Grids Plus has the ambition to be the most important platform in the fields of all SG-related research in Europe.
6. Several leading European distribution system operators (DSOs) has created **EDSO for SmartGrids** [EDSOSG]. The aim of EDSO for SG is to coordinate the SG research and influence regulations at the national and European level. It considers itself the main interface between the DSOs and the European institutions. EDSO for SG focuses for instance on the development of new SG models and on testing the SG models at a large scale.
7. One other initiative is **KIC InnoEnergy** [KICIE], a Knowledge and Innovation Community (KIC) focused on sustainable energy, fostered by the European Institute of Innovation and Technology (EIT). It is a European network, a commercial company with the shareholders being top ranking industries, research centres and universities, key players in the energy field. Its goal is to reduce costs in the energy value chain, increase the security of supply, and reduce CO₂ and other greenhouse gas emissions. Smart Electric Grid is one of the technology areas out of eight technologies KIC InnoEnergy focuses on.
8. One of the FP7 projects that creates SG communities is **ETP SmartGrids** (the European Technology Platform for Electricity Networks of the Future) [ETPSG]. ETP SmartGrids is the key forum in Europe for the crystallisation of policy and technology research and development pathways for the SG sector, as well as the link between EU-level related initiatives. One other project in this area is **GRID+**, a Coordination and Support Action with the aim to support the development of EEGI [EEGI].
9. Some other initiatives worth mentioning are the **International Energy Agency (IEA)**, an autonomous organisation promoting reliable, clean and affordable energy not only to its 28 member nations [IEA] but also to other nations. The **International Smart Grids Action Network (ISGAN)** promotes an international cooperation on SG adoption in the world [ISGAN], and the **Global Smart Grid Federation (GSGF)** aims at the development of smarter, cleaner electricity systems around the world [GSGF].

3.2 Types of Smart Grid models

There is no single definition for the notion SG and there is no one-fit-all SG model given the diverse SG objectives outlined before. The International Energy Agency defines a SG as “*an electricity network that uses digital and other advanced technologies to monitor and manage the transport of electricity from all generation sources to meet the varying electricity de-*

mands of end users. Smart grids co-ordinate the needs and capabilities of all generators, grid operators, end users and electricity market stakeholders to operate all parts of the system as efficiently as possible, minimising costs and environmental impacts while maximising system reliability, resilience and stability.” [IEA] In other words, an SG is a highly complex system where ICT play a crucial role, ensuring communication between different SG system components. These different components should be interoperable. Therefore, there is a need for standardisation of the technical solutions and components in the SG such as interfaces, communication protocols, and processes. Currently, there exist several standards related to introducing SGs developed by the International Electrotechnical Commission (IEC) and the US National Institute of Standards and Technology (NIST). Moreover, there are initiatives that aim at giving guidance on how to introduce the standards and to provide the models describing SG functions and technology. A group of institutions in Europe, the European Commission’s Mandate 490 (M/490) for Smart Grid, the European Telecommunications Standards Institute (ETSI), European Committee for Standardization (Comité Européen Normalisation – CEN), and the European Committee for Electrotechnical Standardisation (CENELEC), created the CEN-CENELEC-ETSI Smart Grid Coordination Group Smart Grid Reference Architecture [SGCG]. NIST developed a Framework and Roadmap for Smart Grid Interoperability Standards. The experts behind those initiatives in Europe and in the United States have started cooperation with the aim to align their work results including the European Reference Architecture. The final (third) version of the NIST Framework was released in October 2014 [NISTSG]. Some of these developments are described in more detail in the next sections.

3.2.1 Smart Grid Reference Architecture

The European Commission’s Smart Grid Reference Architecture [SGCG] is a widely accepted model in Europe. The mandate presents a consistent architecture composed of a set of standards, digital computing and communication technologies and electrical architectures, the processes and services. Its aim is to foster an easier adoption of SG in Europe. The mandate does not cover business models. The Smart Grid Architecture Model (SGAM) has been proposed by the mandate [SGAM]. SGAM unifies different approaches and methodologies for building SG-infrastructure. The SGAM is composed of five layers: Business, Function, Information, Communication, and Component, taken from the Gridwise Alliance Architecture Council (GWAC). The Business layer focuses on business strategic goals, processes and services and it also concerns regulations. The Functional layer contains the description of use cases including logical functions or services independent from physical implementation. The Information layer provides the information objects and data models that are being used and exchanged between functions, services and components. Information exchange interoperability is guaranteed by using common semantics for functions and services. The Communication layer contains protocols and mechanisms for the exchange of information between components. The Component layer describes physical components which host functions, information and communication means.

Each of the SGAM layers is divided in five domains each of which is subdivided in six zones. The five domains are Generation, Transmission, Distribution, Distributed Energy Resources (DER), and Customer Premises. The six zones are Market, Enterprise, Station, Operation, Field, and Process. The SGAM framework (called SGAM cube) is presented in Figure 4.

The presented SGAM model may be used to make a description of the current grid infrastructure, the possible data flows, the comparison of the current situation to the future, and the planned infrastructure. It will help identify standards that should be applied at the individual layer, domains and zones and to verify whether there is no overlap between standards. A crucial advantage of SGAM is that it provides a good visualisation of the overall SG architecture,

which is a highly complex system of systems, and of the interactions of the stakeholders. The SGAM is flexible and will be updated to address new technical deployments.

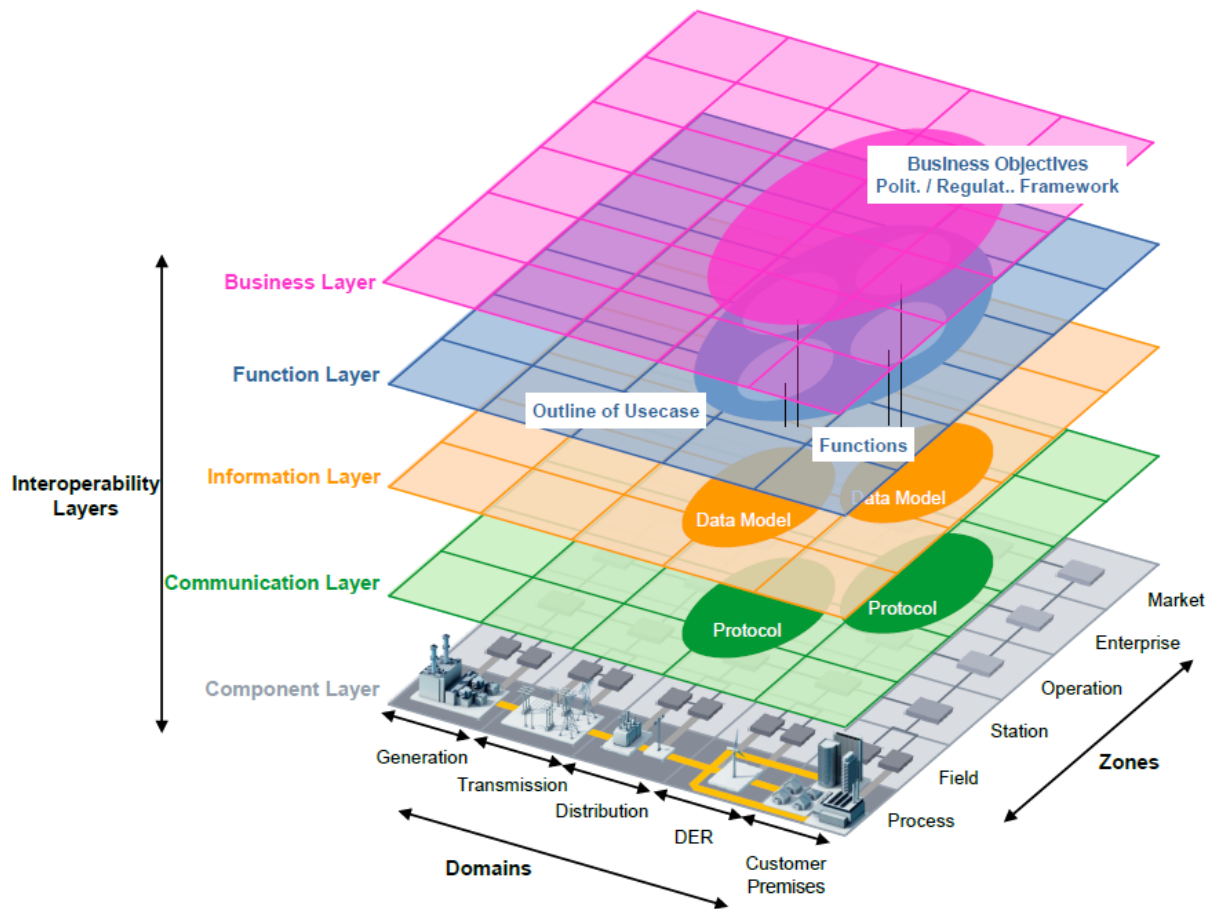


Figure 4: SGAM Framework [SGAM]

3.2.2 Framework and Roadmap for Smart Grid Interoperability Standards

The NIST Framework and Roadmap for Smart Grid Interoperability Standards [NISTSG] is a reference architecture model for Smart Grids developed in the USA. In its latest release, the NIST model has been harmonised with the European Smart Grid Reference Architecture. NIST was made responsible to undertake such work under the U.S.' Energy Independence and Security Act (EISA) of 2007.

The NIST framework provides a holistic vision for the US SGs based on relevant policies regarding the energy market in the USA. NIST has been working on the subsequent versions of the framework with the Smart Grid Interoperability Panel (SGIP), the SG community that was established by NIST to accelerate the development of standards and protocols for the interoperability of the SG [SGIP]. The status of SGIP has changed over the years and is now an industry-led non-profit organisation. Important features of the NIST framework is that it provides a list of protocols and standards that support interoperability of SG devices and systems and that there are the building blocks for the SG. The framework now contains over 65 standards or families of standards that ensure the SG system elements are interoperable and work seamlessly, be it wind turbines, solar panels, conventional generators, batteries, smart meters, transmission and distribution sensors etc.

The NIST architectural framework provides a general view of SG architecture, the processes and methodology of introducing the SG, with diagrams and descriptions that help identify the

characteristics of the SG. Based on this high-level model different standard organisations may propose more detailed propositions. The framework is technology neutral and it enables all electric resources to contribute to the SG.

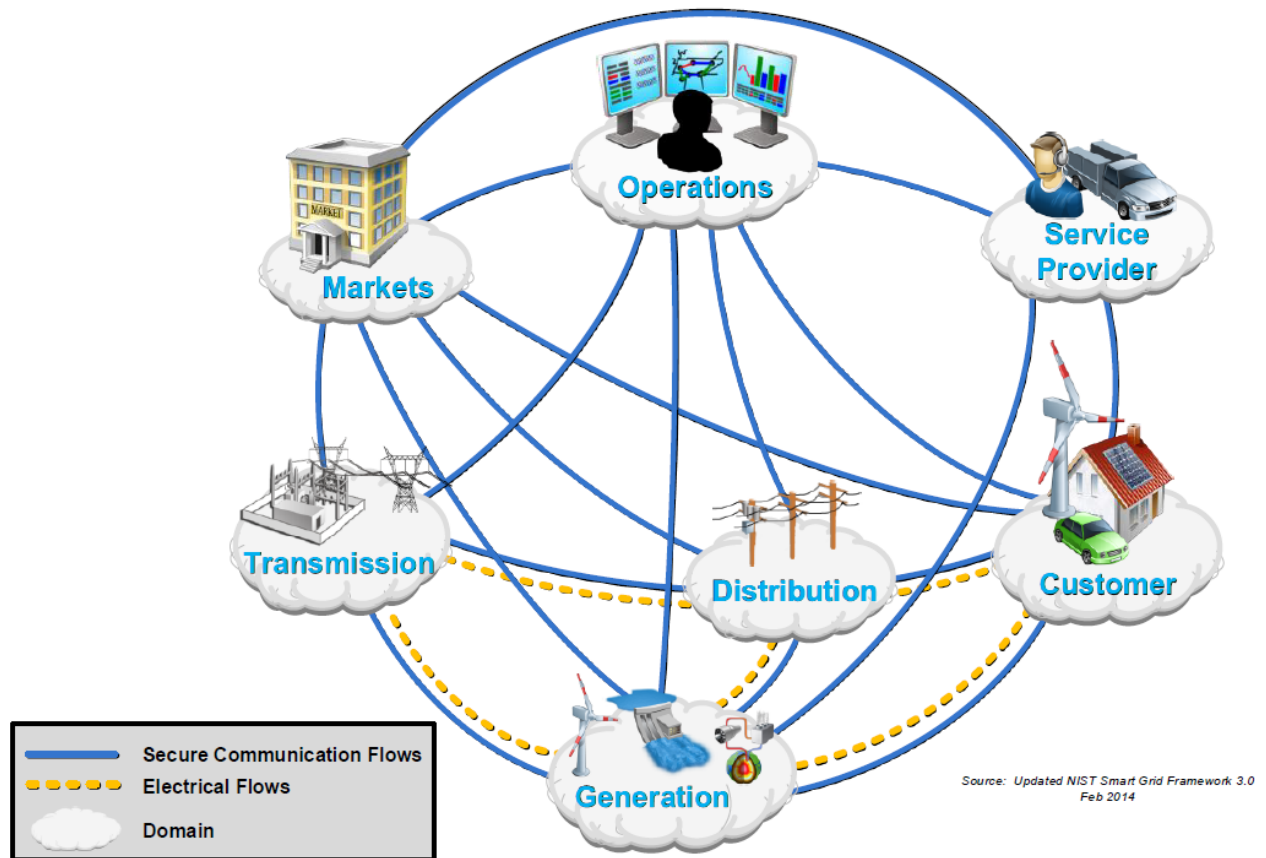


Figure 5: NIST Conceptual Domain Model [NISTSG]

The cyber security framework describes standards, guidelines and strategies for the electric sector to ensure the security of the ICT systems in SGs, their confidentiality, integrity and availability. The issue of cyber security has been deepened in NIST Guidelines for Smart Grid Cyber security [NISTIR7628].

NIST originally created a conceptual domain model useful in activities such as planning, requirements development, documentation, and organisation of the diverse, expanding collection of interconnected networks and equipment composing the SG. The SG was divided into seven domains: Customer, Markets, Service Provider, Operations, Generation, Transmission, and Distribution, see Figure 5.

Each domain is assigned conceptual “roles” and “services” describing types of services, interactions, and stakeholders that make decisions and exchange information necessary for performing identified goals such as: customer management, distributed generation aggregation, and outage management.

NIST proposed the conceptual architecture to provide SG stakeholders building blocks they could use to easily and rapidly build the architectures of their own systems. This architecture contains abstract roles and services necessary to support SG requirements. The architecture does not present details concerning application or interface specifications. However, NIST in its further work and in cooperation with different stakeholders modified the Conceptual Domain Model and proposed an architecture matrix, presented in Figure 6.

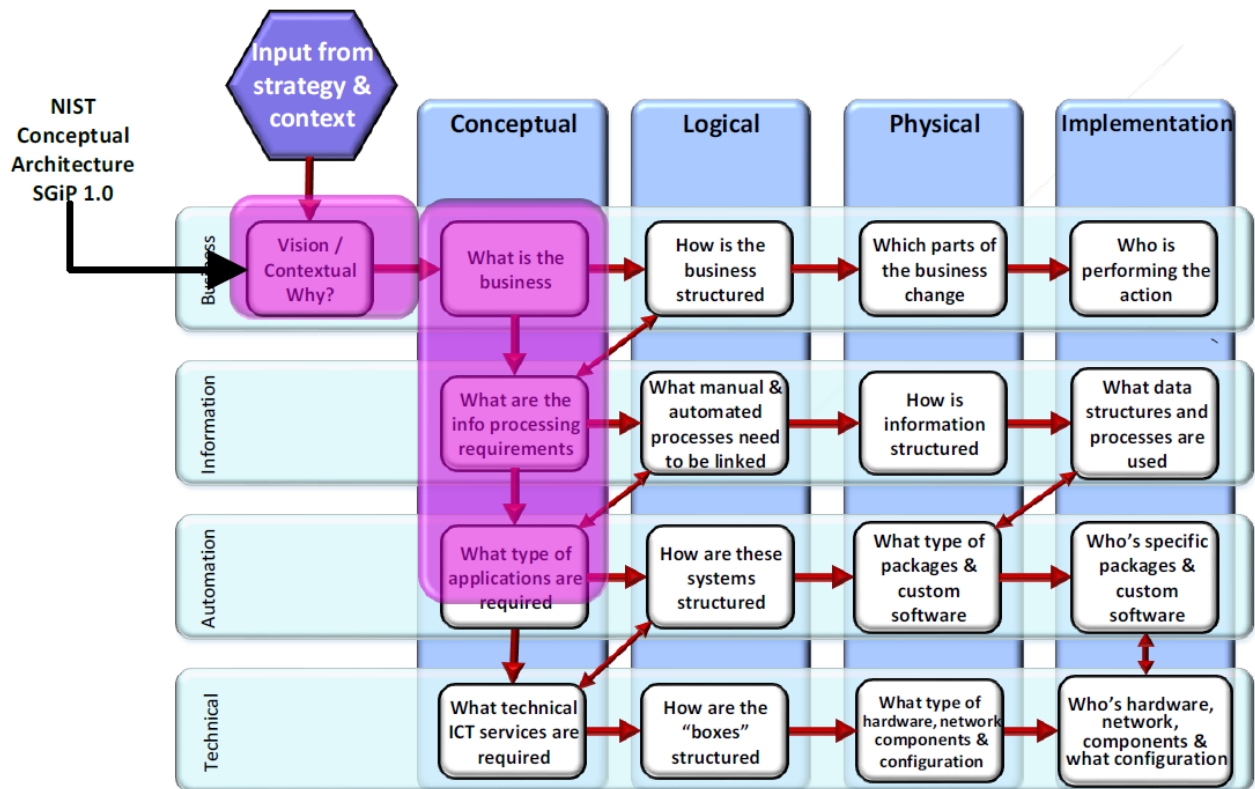


Figure 6: NIST Conceptual Architecture mapped onto the Architecture Matrix Service Orientation and Ontology [NISTSG]

3.2.3 Smart Grid Maturity Model

There are several models that are very helpful for an electric power utility to assess itself and see where it is now in its way towards a SG and to get inspiration for the actions that are still needed. We will discuss two models.

The SEI Smart Grid Maturity Model (SGMM)

The first model is the Smart Grid Maturity Model (SGMM) maintained by the Carnegie Mellon Software Engineering Institute (SEI). The SGMM addresses electric power utilities that want to introduce the SG innovations [SGMM]. SGMM will help utilities manage all aspects related to passing to SGs. Using SGMM, utilities will be able to tell in which areas they already made progress and to measure the progress, to prioritise the actions planned, and to ensure all areas are covered.

SGMM covers eight domains and has overall 175 characteristics to assess the maturity of a utility using SG. These eight domains are:

- Strategy, Management, and Regulatory,
- Organisation and Structure,
- Grid Operations,
- Work and Asset Management,
- Technology,
- Customer,
- Value Chain Integration,
- Societal and Environmental.

A utility may make a self-assessment by analysing its own characteristics against the ones in the model. The maturity levels of SGMM are shown in the table below (Table 2).

Table 2: SGMM maturity levels

Maturity Level	Name	Maturity Characteristics
5	Pioneering	Breaking new ground, industry-leading innovation
4	Optimising	Optimising smart grid to benefit entire organisation; may reach beyond organisation; increased automation
3	Integrating	Integrating smart grid deployments across the organisation; realising measurably improved performance
2	Enabling	Investing based on clear strategy; implementing projects to enable smart grid (may be compartmentalised)
1	Initiating	Taking the first steps, exploring options, conducting experiments, and developing a smart grid vision
0	Default	Default level (status quo)


The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) covers the area of electrical grid security. It has been created by the initiative of the USA government. This model has been created based on the Cybersecurity Capability Maturity Model (C2M2) that was designed to be used by any organisation to enhance its own cyber security capabilities (regardless of size, type, or industry). However, C2M2 contains some part that specifically concern the electricity subsector. Based on this model, it is also possible for an entity to assess its own maturity in cyber security.

3.3 Types of analysis that the Smart Grid Community requires


Currently, the number of interconnections between physical and cyber words is constantly increasing. Many critical SG services rely on public networks and open internet technologies as they adopt mainstream ICT because of economy of scale. Thus, users and operators should deal with the threats and issues related to the cyber domain. Moreover, the SGs and smart infrastructures are data-driven information systems, which (among others) transfer, process and store private and personal data. Therefore, there is a high need for solutions, analyses and guidelines in SG data safety, cyber security, and customer privacy reflecting European laws and regulations such as the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). EU projects like SPARKS and SEGRID address some of these R&D challenges [SEGRID] [SPARKS].

The ICT advancements have significant impact on SG development. For instance, the idea of adapting cloud computing (CC) for SG applications (in order better utilise resources, increase the flexibility and reduce costs) shows that, in many cases, the wheel has not to be reinvented. Obviously, to upgrade classical power grids to be compliant with the SG concepts (advanced forecasting, dynamic consumption moderation, dynamic pricing and dynamic load shaping, etc.) one would need significant amount of computational resources and enough capacity to store and analyse the data generated by monitored physical processes and customers. This can be solved with Big Data tools/technologies and CC services, which are currently gaining traction.



Agent Based Modeling

- It is aimed to assess the integration of renewable energy sources and electric vehicles (EVs) in the future smart grid through:
 - **Development of innovative, cooperative multi-agents methods** for simulating the emerging behavior of different agents (consumers/prosumers/EVs) at several aggregation levels (e.g. building, district, ...) able to:
 - (i) enhance the energy use efficiency of the consumers/prosumers;
 - (ii) enable large scale integration of renewable energy sources;
 - (iii) enable efficient use of the energy stored in the EVs batteries including development of smart charging/discharging strategies.



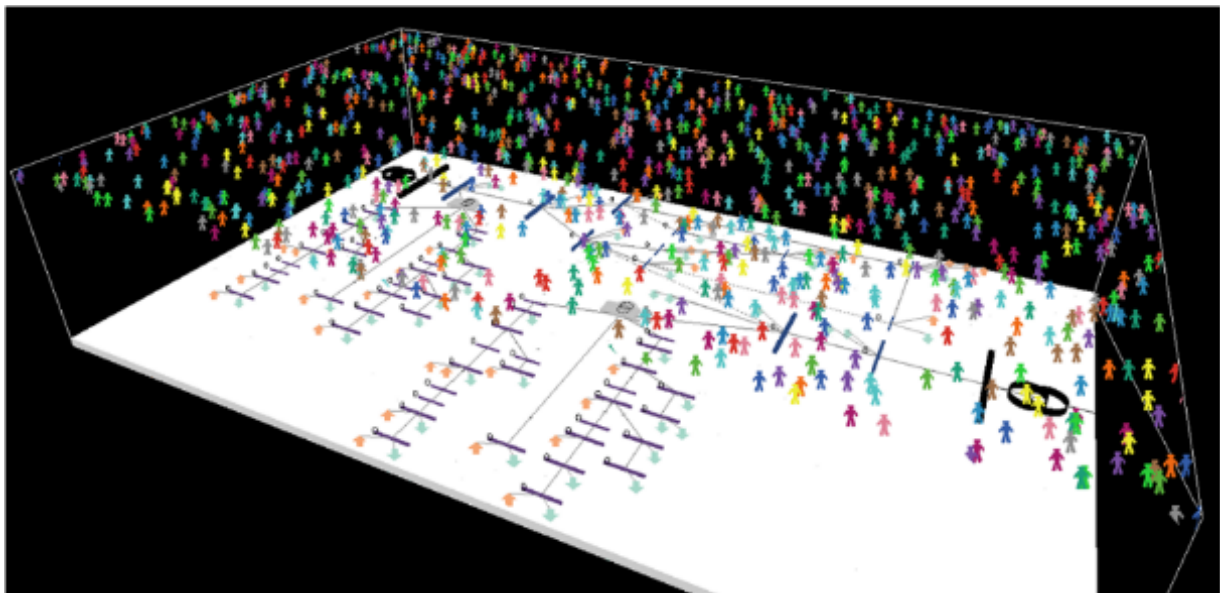


Figure 7: Agent-Based Modelling of smart grids including autonomous behaviour of the prosumer (source: [SGJRC])

It is also noticeable that the SG community requirements also tackles non-technical aspects such as social and political issues of “fair” availability of electricity, fairness of complex rate systems and regulations telling who should pay for what (in many cases it is the customer who will pay for the infrastructure upgrades, e.g. smart meters). Models and tools should also address these types of factors, by integrating the human behaviour e.g. via agent based models as developed by EU’s Joint Research Centre (JRC) in collaboration with TU Delft. [SGJRC]

Finally, standardisation will increase the interoperability of different smart components. At the low level (e.g. communication protocols), standardisation is happening since late 90's. Nevertheless, standardisation processes take long, especially as they should consider the multi-sectoral nature of SGs, the large number of different stakeholders, and the problem of multi-technology integration.

3.4 Types of analysis that might be provided by EISAC

Depending on the national governance and R&D structure, EISAC nodes may have a role in addressing some of the SG challenges. Services and roles that can be thought of are shown in Table 3.

Table 3: Types of analysis that EISAC nodes may provide regarding Smart Grids

Service Group	Possible EISAC.node service
Advanced Decision Support	<p>Identifying threats, hazards and impact by natural phenomena (e.g. rain, flash floods, earth quakes, hurricanes, etc.) on CI and NGI for emergency management authorities and CI operators, e.g. by spatial and now-casting analysis.</p> <p>What-if analysis in support of risk analysis in the design phase of NGI.</p> <p>What if analysis including aspects of human behaviour, e.g. based on agent-based models.</p> <p>Identifying possible attack paths and their impact.</p>
Research Platform for CIP/CIR Collaboration	MS&A of SG and NGI.
Information Brokerage on CIP/CIR	<p>With the growth of IoT (Internet of Things), users' data privacy and its security may be threatened. An EISAC node may provide CI operators and citizens with analyses and guidelines that will help to follow current law regulations and directives in NGI.</p> <p>An EISAC node may be an information hub for NGI using the Ask the Expert (ATE) service and underlying knowledge base.</p> <p>An EISAC node may provide a catalogue of past incident data and analysis of both cyber and physical incidents in CI and NGI.</p> <p>Currently, the information is dispersed (among different national web services) in many cases and hard to find using internet sources.</p>
Other services	<p>A national EISAC node may have a trusted national role with respect security and safety aspects and analysis of CI including SG and NGI.</p> <p>A national EISAC node could be the main contact point in matters as: security posture assessment, security and standard definitions, safety and security simulation, security guidelines definitions, etc.</p>

4 Case study 2: The secure design of intelligent grids

4.1 Intelligent Infrastructure/Grid Community – short description

The Smart City is designed and developed based on a broad use of advanced technologies such as ICT integrated into the urban environment offering advanced services to its citizens, SME and other businesses. Such technologies may include sensors, electronics, and networks which are connected to IT systems. Intelligent infrastructures are tightly related to the term “Smart City”. Nowadays, smart cities can be considered as one of the most important emerging phenomena taking advantage of information-related technologies and emerging Internet of Things (IoT). Like the case of traditional (“not smart”) cities, CI in smart cities are subject to security concerns from two perspectives:

- a. smart CI is important for the citizens and urban functions, thus their disruption or unreliability impacts citizens similarly to the unavailability of traditional CI (with lesser inter-connection to ICT technologies), and
- b. emerging technologies embedded into smart environments can be considered as offering additional vulnerabilities in CI and may invoke additional security threats.

The City of San Diego has over 11, 000 employees, 24 networks, and over 40.000 network end-points. Smart city technologies already in use:

- Smart electrical Grid (www.sdge.com/smartgrid/smart-grid-sdge)
- LED city lights
- Intelligent parking using street sensors
- Intelligent library
- Smart HVAC systems in its 43 libraries
- Resilient emergency communications
- City-operated photovoltaic energy resources
- Mapping of all city-owned trees
- Intelligent port using sensors [JHiner]

The challenges related to the security of modern (smart) cities and CI are complex due to the ever-changing technologies embedded in these cities. According to [Ijaz], three groups of security concerns in smart city are:

- Socioeconomic factors which include cyber security and data integrity risk to “smart” communication. The risk includes cybercrimes and cyberattacks aimed at e.g. e-banking and e-commerce services, as well as the individual privacy of citizens,
- Governance factors which include the proper use of citizens’ data, **security of Critical Infrastructures**, smart mobility, and city management with use of ICT tools,
- IoT technologies which include the security of RFID (Radio-frequency identification) tags, security of sensors and sensor networks, secure M2M (machine-to-machine) communications, use of smartphones and **threats related to electrical SGs**.

Related to CIPRNet is the R&D area of CI security in the light of the growing digitisation of critical components such as in the health sector, the telecommunication sector (including crisis communications), energy and power distribution, and ICT-support for disaster management. The second CIPRNet related area deals with the overall security of smart cities including is the cyber security of SGs. Threats to these infrastructures are for instance denial-of-service attacks, attacks targeted to data integrity and customer privacy.

4.2 Types of existing models

There are several models of smart cities developed by the European organisations. MS&A attempts to model security in intelligent infrastructures have been described in literature. It should be noted, that modelling of the whole smart infrastructure operating in a city with all dependencies is a very complex task. Therefore, most models focus on a selected, narrow part of the city infrastructure.

4.2.1 ENISA model

In December 2015, European Union Agency for Network and Information Security (ENISA) published its document titled *Cyber security for Smart Cities: An architecture model for public transport*. The document is focused on the transportation sector, with attention put on the security of the Intelligent Public Transport (IPT) systems that are a key element in Smart Cities [ENISA]. The security model presented in the publication focuses on aspects of data exchanges between local public and private transport operators, as well as between them and non-transport operators (such as energy or banking), public safety institutions, and regulators. The architecture model of interactions in the transport sector in smart cities has been described from the perspective of stakeholders' communication. Two separate models are defined and described:

- A model that focuses on stakeholders' interactions, functional processes and data exchange between various stakeholders (Figure 8).
- A model of interaction model including elements that are used by stakeholders to interact from a business, information/data, technology and a physical link perspective (Figure 10).

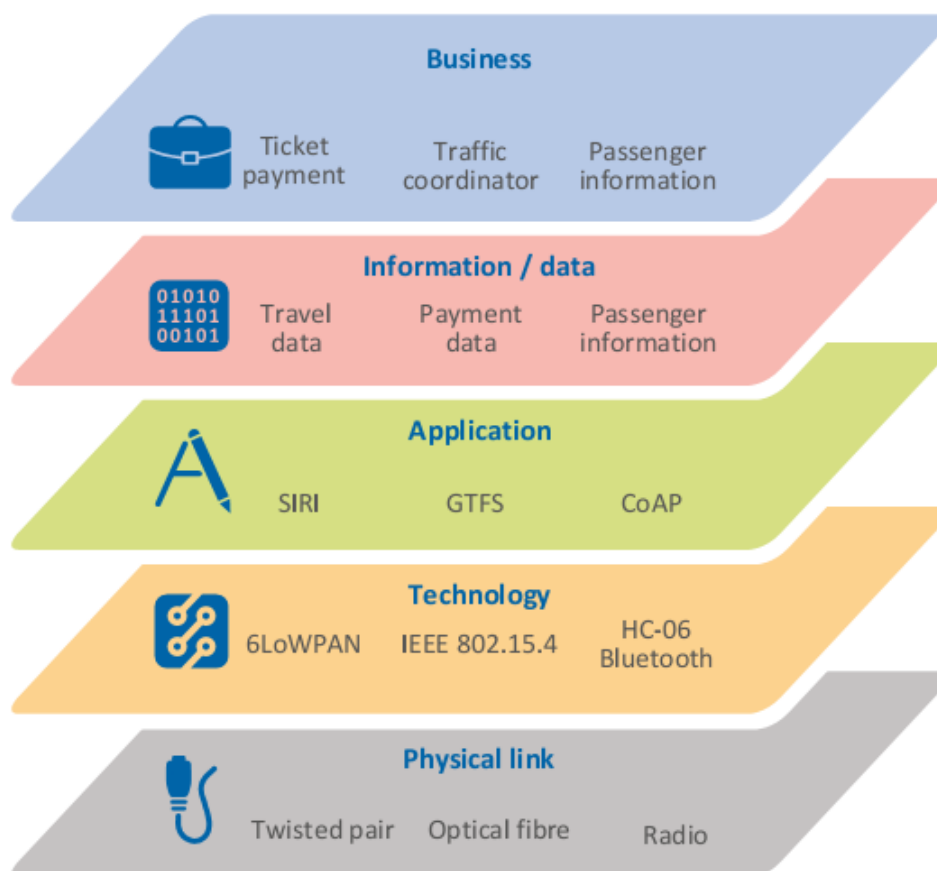


Figure 8: ENISA's interaction layer model [ENISA]

4.2.2 BSI SCCM (Smart City Concept Model)

The BSI group, an organisation focusing on standardisation for business purposes developed its own model of Smart City dependencies [PAS182]. This Smart City Concept Model (SCCM) is focused mainly on the *data flows* that can be observed in a Smart City. The model is comprised of 27 concepts representing typical actors, roles and dependencies that can be found in smart cities. Examples of concepts from the model include such terms as: community (a group of persons and/or organisations to which a common feature such as place can be assigned), assumption (a predicted or presumed state), etc. According to the model authors, these concepts and a common understanding of them facilitate sharing and re-using information by decision-makers.

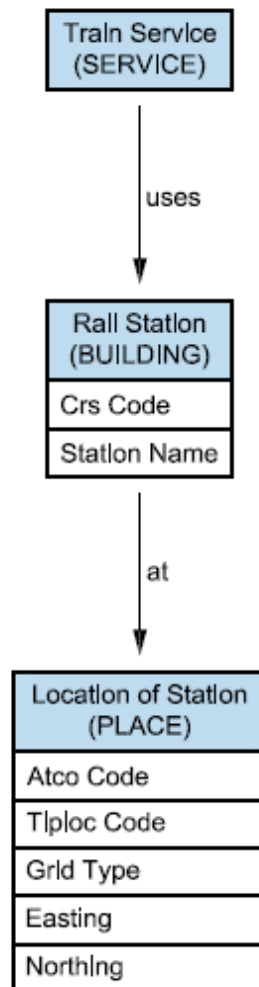


Figure 9: A SCCM view [PAS182]

The SCCM can be applied to analyse both open data, shared under open licences, and the data for which the security and privacy of the content is protected. According to the model developers, observation of the strategic decisions and tracking of the data is possible by applying the model by the smart city actors. The SCCM is relevant to a broad range of unstructured and semi-structured data streams as well as to structured data. One of examples is cross-analysis of social media streams and traffic sensors that can provide information about how a smart city community views its transport links, for example from the traffic security perspective.

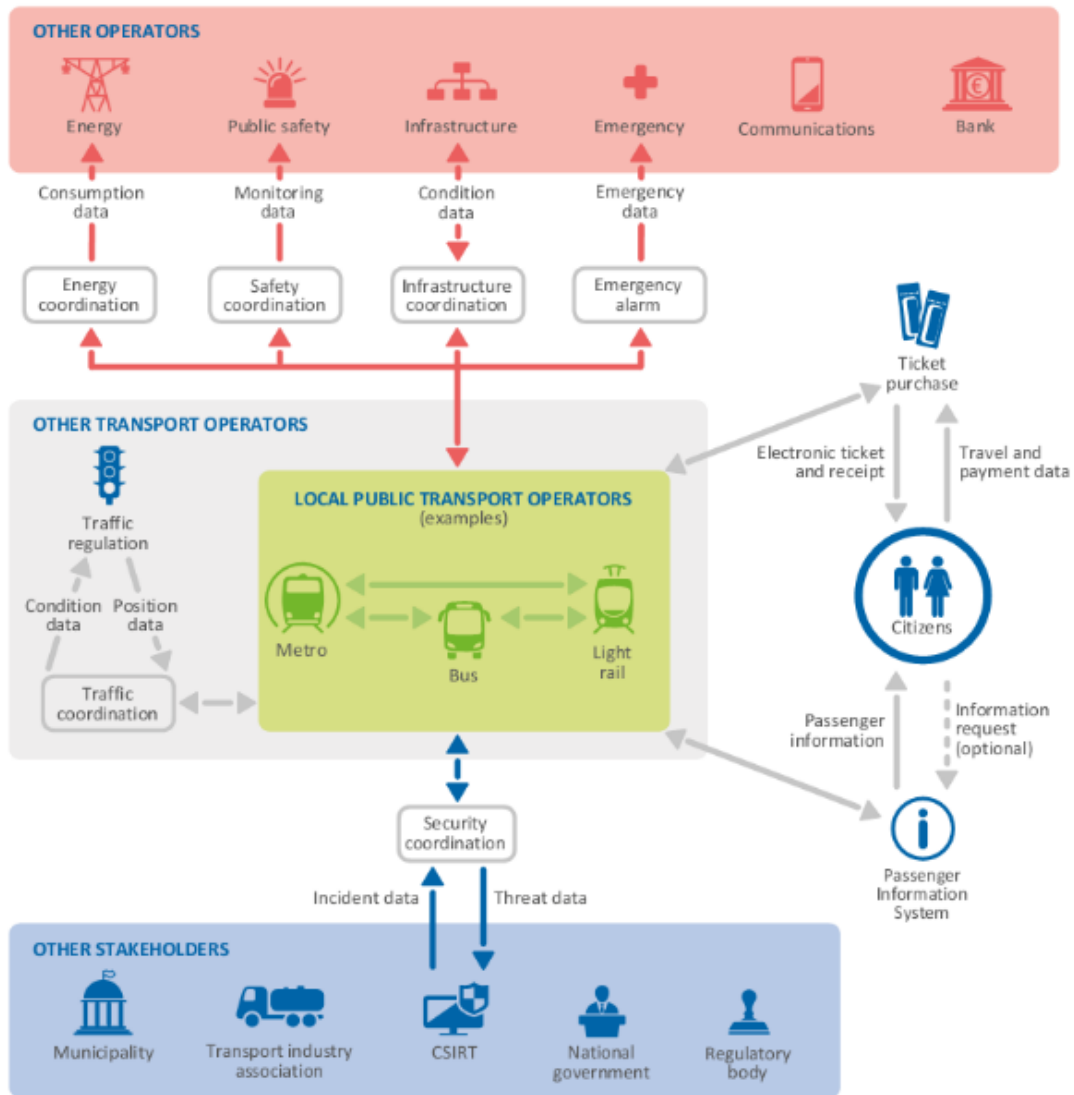


Figure 10: ENISA’s model of smart city stakeholder interaction [ENISA]

4.3 Main challenges for the Intelligent Infrastructure/Grid Community

Per the ENISA report [ENISA], the following challenges and limitations related to cyber security of the smart city ICT are most pressing:

- Collaborations in smart cities across sectors, between various actors and different smart cities and across national borders are not sufficiently defined and modelled;
- Lack of a reference architecture for data exchanges in smart cities;
- Insufficient cyber security awareness within a smart city and smart services operators;
- Not effective information sharing on threats and incidents for and by smart cities operators (lack of common platform, procedures, and willingness to share sensitive security information);
- Lack of integration of cyber security in solutions dedicated for smart cities and provided by different vendors to smart city operators;
- Lack of measures and metrics that can assess cyber security measures effectiveness.

For each of these challenges, MS&A can support the analysis process.

The next sections describe the possible use of models and tools in the (re)design of these networks.

5 Case study 3: Use of CIPCast/RecSIM for cost-effective grid upgrades

5.1 RecSIM application

The RecSIM application which has been developed by ENEA as part of CIPCast to transform damages into services outages. Other than being used in real-time in the CIPCast operational mode, RecSIM can also be used “off-line” in a what-if simulation mode to predict the impacts on network(s) due to specific fault(s).

The user can synthetically introduce one or more CI faults, for instance in an electro-telco system, and see which will be the faults propagation and the recovery times of the different CI elements, as a function of estimated durations of all recovery actions. It is assumed that the recovery times can be optimised from the operator’s point of view, i.e. the operator should reduce (by contract) the total number of *kminutes* that is the product of the number of customers and the total number of minutes a customer experienced the outage.

Now, imagine the combined electro-telecommunication system, where one’s knows the following parameters:

1. the topology of both networks,
2. the dependency matrix in both directions,
3. for each electrical cabin, if it is telecontrolled, not telecontrolled or automatic (each type reacts differently when involved in a fault),
4. the number of technical crews available and the number of available electrical generators,
5. the city map with roads (and typical traffic situation).

With this information and RecSIM one could simulate the following “perturbation simulation”: one could set in off-state, one at a time, each single element of the electrical network. After having optimised the recovery strategy using the operator’s viewpoint (lowest possible *kminutes*) one stores the total number of *kminutes* resulting from that outage.

After having repeated the simulation setting off-state in fault each electrical cabin, you will have at the end the distribution of *kminutes* resulting from the “initial” setting of the parameters described in points 1-5 above.

The resulting *kminutes*’ distribution will be a sort of fingerprint of the current setting of the electrical network which considers also the dependency relations with the telecommunication network and the main operation capabilities of the operator (the points 3 and 4 above). This function is the “Network Resilience Function” (NRF) which is the distribution of *kminutes* resulting from the simulation. After all, the NRF stores the global ability of the electrical system to withstand a perturbation and to (be) recovered from it up to a new equilibrium configuration where all users are supplied again. The smaller the integral of the NRF, the larger the system capability to withstand and recover from a perturbation. This function therefore relates to the notion of resilience.

Imagine now that the CI operator is willing to improve its current NRF by making some investments. The operator can invest in network improvement by changing the current network settings (i.e. one of the points 1-5 above). According to our model, he/she can change the following properties in its network:

1. the topology (by adding/removing/changing specific lines etc.),
2. transform a not telecontrolled cabin into a telecontrolled one,
3. transform a telecontrolled cabin into an automatised cabin,
4. increase the number of simultaneously available technically crews,
5. increase redundancy in electro-telecommunication across dependencies.

The operator could thus “guess” an improvement among the 5 above mentioned “properties”, introduce it into the network, estimate the resulting NRF by repeat the “perturbation simulation” to see which is the extent of benefits it has produced into the NRF function. If the NRF integral reduces, the system would increase its resilience. Usually all changes thought by the operator will improve resilience. Using this method, however, one could examine different improvements to determine which of them will introduce larger benefits (this is a function of its ratio with the relative cost).

In Figure 11 and Figure 12, one can see the NRF of the current section of the Roma network under study and the simulated resulting NRF upon transformation of a currently not telecontrolled network into a telecontrolled one. Simulations have focussed on the benefit introduced in a specific part of the network (containing 100 cabins) by transforming a not telecontrolled cabin into a telecontrolled cabin. Currently, 48 of the 100 cabins in the portion of the network under analysis are currently not telecontrolled. Simulations have been performed by transforming, one at a time, each of these 48 not telecontrolled cabins into a telecontrolled cabin, to estimate which one would introduce the maximum benefit in terms of NRF when upgraded.

A simulation first estimates the NRF of the network in its current state. To achieve this datum, each cabin has been shut-off and the resulting crisis estimated in terms of the total number of kilominutes produced. This produces 100 kilominutes values (one for each crisis (outage)) that can be plotted as a distribution (Figure 11) which constitute the current network fingerprint, the initial NRF. Then, one at a time, each of the 48 not telecontrolled cabins has been transformed into a telecontrolled cabin and the same simulations have been performed with the new network setting. For each cabin improvement, 100 simulations have been performed (by shutting-off one at a time the 100 cabins of the network) and recording the 100 kilominutes values resulting from each of them. Also in this case the 100 values could be inserted into a distribution that could be directly compared with the initial NRF fingerprint.

The difference between the integral of the two distributions provide an indication on the increase of Resilience, expressed in the total number of kilominutes that the network improvement can produce. Figure 12 represents the distribution of kilominutes resulting from crisis in the area if the cabin (labelled SS98) were modified (from not telecontrolled to telecontrolled). This function can be compared with that of Figure 11 where the distribution refers to the network in its current state.

These results say that there would be a Resilience benefit estimated in a saving of 80 kilominutes if the SS98 cabin were transformed from not telecontrolled to telecontrolled.

All calculated benefits (each coming from the transformation of a not telecontrolled cabin into a telecontrolled cabin) could be compared to estimate which transformation should be the object of the first intervention, as it would introduce more benefits into the network Resilience. The same simulation strategy could be applied by modifying each one of the properties (1) through (5) above described and see how much that transformation will contribute to the improvement of the overall Resilience. Each transformation could be correlated to the Resilience enhancement that it would be able to produce by a Cost/Benefit analysis.

As soon as the overall Roma network (>14.000 cabins) will be described into the RecSIM model, there is a plan with ACEA Distribuzione (the electrical DSO in Roma Capitale) to perform this simulation to highlight the “hot spots” in the network (i.e. the cabins whose transformation to telecontrolled would introduce major benefits to the network in terms of kilominutes reduction).

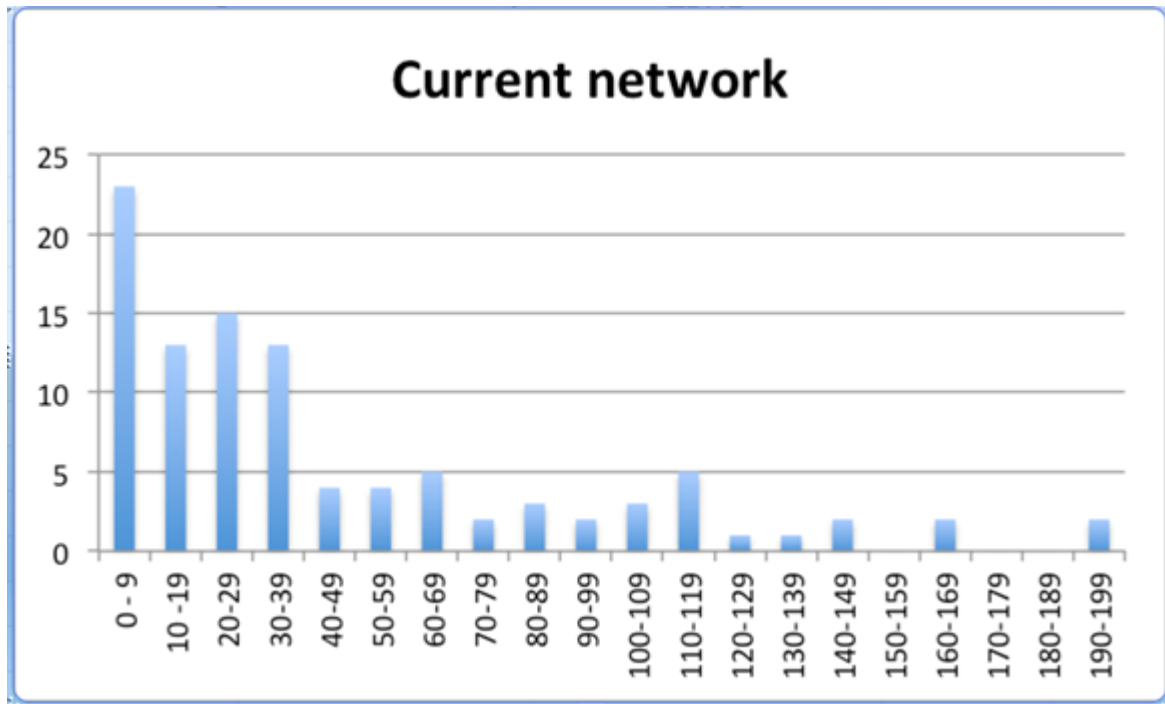


Figure 11: Distribution of kilominutes of outages resulting from the shut-off of each of the 100 cabins of a specific tract of the Roma network.
 The abscissa represents kilominutes resulting from the outage; ordinates represent the number of times in which an outage of a given kilominutes of relevance has been produced.

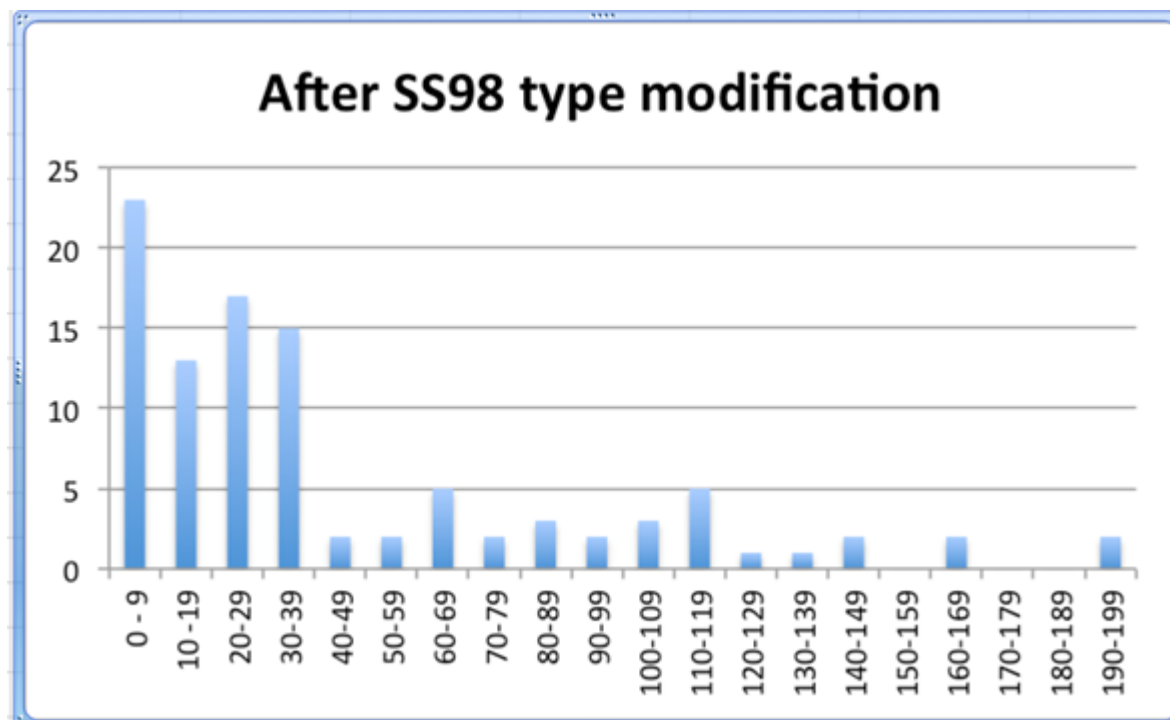


Figure 12: Same distribution of fig.9 made on the network after a single modification (cabin SS98 transformed from its current state of a not telecontrolled cabin into a telecontrolled cabin)

Table 4: Types of analysis that EISAC nodes may provide with CIPCast/RecSIM

Service Group	Possible EISAC.node service
Advanced Decision Support	The operational use of RecSIM to study investment options to enhance the resilience of combined, dependent infrastructures in, e.g., a smart city context.
Research Platform for CIP/CIR Collaboration	The use of RecSIM to study the resilience of combined, dependent infrastructures in, e.g., a smart city context.
Information Brokerage on CIP/CIR	N/A
Other services	Security analysis of intelligent SG and NGI.

5.2 Case example: Risk-based planning of NGI

The current capabilities of risk analysis provided by CIPCast have attracted attention from Italian CI Operators during some of the dissemination events where CIPCast has been presented. The award that CIPCast has received at the SMAU Fair in Bologna³ has attracted much attention, having been broadcasted by several Italian magazines and newspapers.

A first outcome of these dissemination activities concerns with the commitment received from an Italian DSO, to produce a CIPCast-based application enabling to make risk estimates of a new tract of a network during the design phase. The system, whose realisation is on-going, will receive the GIS blueprint of the new infrastructure (as resulting from CAD tool) as input. This blueprint comprises all possible structural data (of sections, of active elements etc.).

The intended result of the analysis is to produce a risk map of the blueprint in relation to the most probable hazards in the area (landslides, floods and earthquakes). The goal is the identification of “hot spots” of the blueprint, i.e. those tracts which are more prone to be disrupted by the main threat or lying in areas which could undergo risk due to induced events such as floods or landslides.

For the earthquake risk, for instance, the application under development will produce a set of synthetic earthquakes in the region (modulated by epicentre, magnitude, depth, location). All the consequences on the infrastructure will then piled up in a Monte-Carlo sum, where consequences are weighted with the probability of occurrence of the generating event.

This “blueprint risk analysis“ for NGI is a relevant type of service that EISAC could produce by exploiting the capabilities of CIPRNet applications. The CI Operator’s requests will also trigger (as in this case) the production of ancillary applications that will further improve the portfolio of offer of EISAC.

5.3 Case example: Monitoring and control in Smart Grids

Another MS&A example for NGI is the work at the Belgium University of Leuven on multi-agent monitoring and control in combined ICT-power infrastructures by Geert Deconinck. [NGIBSIK] Geert stated: “*The research question is how a multi-agent system needs to be designed to provide services for monitoring and control in an electric power infrastructure with high DER penetration at distribution (low voltage) level, with an underlying ICT infrastructure based on standardised components. Specific emphasis goes to the trade-offs between improved efficiency (due to the distributed control) and the increased vulnerability (due to the interdependencies between the ICT and power infrastructure).*”

³ <http://www.smau.it/bologna16/news/innovazione-all-enea-il-premio-innovazione/>

Due to the architectural complexity and intensive interactions of the different stakeholders of smart grids (e.g. generation, transmission, distribution, operation, markets, customer and services), “*a systematic synthesis and coordinated methodology needs to be the core of designing and deploying any smart grid paradigm*”. Moreover: “*how to ensure the stability and integrity of the proposed CI, while facilitating its penetration through the existing utilities with financial incentives?*”. Leuven’s research uses multi-agent systems as MS&A tool to analyse the structure and behaviours of various smart grid components. At the same time, an innovative mechanism based on the foreseen real-time spot market of electric energy has been devised, which promotes the substantiation of the economic and social potentials of smart grids. [Leuven] Apart from the use of agent-based modelling (ABM) for the MS&A of NGI, it becomes clear that the modelling of NGI extends beyond the technical infrastructure. The economics and market behavioural aspects require to be considered in MS&A for NGI as well.

6 Outreach to NGI communities

In addition to the cases studies above, an outreach was made to several Next Generation Infrastructure communities to assess the possibilities for collaboration with or in a future EISAC. This chapter describes the results and analysis of this outreach.

6.1 Description of communities

The following communities were approached:

- the National Model and Data Centre (NMDC),
- the NGInfra association,
- SIM-CI,
- EU's Joint Research Centre (JRC), Institute for Energy and Transport (IET).

6.1.1 The National Model and Data Centre (NMDC)

The Dutch National Model and Data Centre (NMDC) is a joint initiative of seven organisations in the Netherlands: the Dutch National Institute for Public Health and the Environment (RIVM), Wageningen Environmental Research (Alterra), the Royal Netherlands Meteorological Institute (KNMI), the Netherlands Environmental Assessment Agency (PBL), Rijkswaterstaat (responsible for the design, construction, management and maintenance of the main road and water way infrastructures in the Netherlands), the Netherlands Organisation of Applied Scientific Research (TNO), and the Delta Research organisation Deltares. The latter two are CIPRNet partners.

The aim of the NMDC is to bring together knowledge and expertise about modelling and the use of data, primarily in the field of climate change and climate adaptation. The primary aim of the NMDC – which was founded in 2013 – was to join modelling facilities and work together in practice. Over the last three years, the NMDC has also been instrumental to the initiation of new projects, solving disputes about data, model and outcome ownership, and the alignment of efforts of partner organisations with a broader (EU) policy agenda on open data.

The NMDC consists of a partner board and a supervisory board that both consist of representatives of all associated organisations.

6.1.2 NGInfra

The collaboration association NGInfra (Next Generation Infrastructures) consists of Rijkswaterstaat, the Port Authority of Rotterdam, electricity grid operator Alliander, Schiphol airport, the Dutch railway infrastructure operator ProRail and the largest drinking water company in the Netherlands Vitens [NGInfra]. The NGInfra association was preceded by an international research program that ran between 2004 and 2014 [NGIBSIK] at the Technical University of Delft's Faculty of Technology, Policy and Management (TPM).

Many infrastructures have been built decades ago but are still being used intensively. The organisations involved in NGInfra are responsible for the functioning of key Dutch infrastructures and face a similar challenge: how to make their infrastructure adapt to continuously changing conditions and ongoing digital transformation. And how to reach, in collaboration with scientific researchers, an integral vision on infrastructures of the future? Therefore, the aim of NGInfra is to enable 'responsive connections' and adequately adapt infrastructures to prospective changing conditions.

NGInfra focuses on issues regarding the strategic management, maintenance, replacement, expansion, and innovation of infrastructures. It does so by working on four theme centres:

- Exploring the future,
- Availability,
- Value of infrastructure,
- Data and security.

The theme centres change over time and are used to share knowledge and insights between partner organisations about the daily operation of infrastructures. The theme centres are also used to jointly initiate and execute projects.

Besides the work in the theme centres, NGInfra initiates research projects in collaboration with research institutes and the Dutch Organisation for Scientific Research (NWO). NGInfra consists of a program office that supports the theme centres, organises events and publishes the NGInfra magazine. NGInfra has a program council that advises on research themes.

6.1.3 Sim-CI

SIM-CI is a Dutch company that started out as an innovation project within the Dutch electricity distribution operator Alliander. The company employs scientists, mathematicians and software engineers to analyse real network data and scenarios including cascading effects and the simultaneous failure of multiple CI. SIM-CI collaborates with TU Delft, TU Eindhoven, TU Twente in the Netherlands, and the Massachusetts Institute of Technology (MIT) in the USA to integrate fundamental and applied research.

Amongst other developments, SIM-CI has developed a platform with analytical tools for dependent asset and risk management and the analysis of operations and maintenance of CI. For example, MS&A showed that the compressing ratio in a gas grid was much higher than needed. Reducing the gas compression while still guaranteeing an acceptable gas pressure at the end points of a compact gas distribution grid, saved million euros per year in grid costs. Another analysis helps to assess and estimate the size of the influx of sand and mud in case a gas transport pipeline breaks due to a break in a drinking water transport pipeline. Without such support, the approach is to unearth a gas pipeline at several places, cut the pipeline and inspect for influx. A scientific underpinned model using big data and flow models provides reasonable estimates and saves much time in accessing how much cleaning is required.

The SIM-CI platform offers simulation and management facilities as a service (SaaS) and is designed as to be able to integrate multiple models of critical infrastructures and data sets.

6.1.4 Institute for Energy and Transport (IET), EU JRC

The Petten (The Netherlands) and Ispra (Italy) based Institute for Energy and Transport (IET) is part of the EU Joint Research Centre (JRC), which is the scientific and technical arm of the European Commission. For the outreach to NGI communities, the IET's Energy Security, Systems and Market unit in Petten, The Netherlands was contacted. IET research is primarily aimed at (parts of) the EU wide gas transport and electricity transmission systems. IET cooperates with EU Member States, research organisations and universities on a regular basis.

IET's Smart Electricity Systems and Interoperability team performs independent scientific research and supports EU policy-making for the energy sector as critical infrastructure. This includes some efforts with respect to European grid capacity development and future needs. The focus is on the security of supply of power (transmission) and gas (transport): the Transmission System Operator level (TSO). The oil subsector is not much worked on.

The team does so by gathering and processing data and MS&A.

IET uses three main models for *gas transport*:

- GenFlow – a coarse level gas transport model covering 26 EU nations plus its neighbours such as Norway, Belarus and Algeria. Elements: storage, use, and summed capacity of pipelines (directional). The model helps to analyse the nation-to-nation cross-border flows and capabilities. A Monte Carlo technique is used to simulate random grid disturbances and derive a measure of the robustness of the European gas grid. For some nations, detailed data is available. Other nations only provide rough data.
- ProGasNet⁴ – A probabilistic model to analyse the most exposed nodes in a system based on keeping the mass balance while maximising flows. The model is used to analyse the combined gas system of several Member States. Some Member States, however, use such models themselves and do not share data with the EU as that is concerned either national or commercial sensitive.
- EUGas – a hydraulic model for gas transport. The level of detail per Member State is dependent on provided data. Most data sets are coarse grain, although some data sets are provided to the EU by TSO under a non-disclosure agreement.

Using these models, IET has performed risk analysis on parts of the European gas grid, e.g. by analysing thirty scenarios for a specific region. Although possible, IET has not analysed in a “what if” manner how the grid optimally could be made more resilient by adding a pipeline from A to B. IET only considers firm future grid expansions including LNG terminals.

The models support EU prevention planning for a gas crisis in the Member States and considers the effects of fuel switching.

With respect to MS&A of the *power transmission* system, IET uses:

- PowerWorld for capacity analysis with European Network of Transmission System Operators for electricity (ENTSO-E) data, and detailed data from a group of Member States and individual transmission grid operators (TSO).
- Matpower (freeware) to analyse the security of supply. The model propagates failures.
- Plexus for market analysis. Each nation is modelled as a single node. IET looks at transport trends and the evolution of the electricity transmission system over time, e.g. those due the shift in energy mix in each of the nations.

The models are used to analyse and study demand and supply flexibility and security of supply in smart grid systems and the possible effects of the integration of renewable energy technology *at national and EU-wide level*.

No federate MS&A is used. The only combined model is SAINT which helps to analyse the effects of transients in the gas grid on a steady-state power grid. It takes for instance restrictions like the minimum required gas pressure level for power distribution (e.g. 33 bar) into account. This is an off-line simulation.

With respect to cyber security modelling of both the gas and power grids, only the first order outage effects of grid elements are considered; not a fine-grained model of the cyber-physical system.

Validation of the models takes place by analysing incidents and during crisis situations, e.g. the 2009 Ukraine gas problem. The development of reference scenarios using for instance historical public data is being considered.

Currently, IET is consolidating their knowledge and models. From 2019 onwards, further model developments will take place.

⁴ See: <https://ec.europa.eu/jrc/en/publication/probabilistic-gas-transmission-network-simulator-and-application-eu-gas-transmission-system>

On the long term, IET expects to collaborate more with the Member States while taking up expertise from scientific communities (in general, models are better than experts). Joint work with three to four neighbouring Member States seems to be the most effective way forward.

Data (un)availability is a major issue. Open data is too limited; the Platts data collection has too diverse granularities of data sets to make it useful. The ENTSO-E transparency platform data provides historical data that is of help to understand for instance the effects of aggregated wind power. However, the detailed data about capacities of specific power grid lines are not available.

6.2 Feedback of these communities on the possible use of EISAC services

Representatives of the communities mentioned above have been interviewed to collect feedback on the possible use of EISAC services. Their feedback is combined into a description of perceived benefits of EISAC services and a description of potential concerns.

6.2.1 Perceived benefits of EISAC services

The following benefits are perceived by the NGO community:

- All communities second the proposition that dispersion of existing models and outcomes of simulations is an on-going concern. Many models exist (e.g., on electricity transmission systems and smart grids), but their application to solve real-world challenges lags behind. EISAC services to make models and outcomes available to others are welcome. EISAC support for making models available and dissemination of research outcomes is useful both nationally and internationally.
- Tools for MS&A are often developed with a specific aim such as capacity analysis or studying the propagation of failures through infrastructure systems. Such tools can also be used to support the resilience design of NGI and to find optimal improvements for the resilience of CI. EISAC services can support the ‘cross-functional’ application of existing simulations and models.
- Support for the development of standards and agreements on interoperability, both regarding models and data, is deemed useful. Although the issue of different standards and formats is not expected to be solved anytime soon, support from EISAC by making CI models and data applicable for other research themes such as sustainability or urbanisation are a major benefit. EISAC services may specifically address differences in data quality between EU Member States and the quality of open data.
- Sharing good practices is perceived as a major benefit of EISAC. Good practices are shared in existing communities around specific infrastructures (such as railways, electrical grids, and main ports) and research themes (such as sustainability and open data). Cross-sector sharing of good practices occurs in a limited manner and is perceived to be beneficial, especially because of growing dependencies between infrastructures.
- A specific perceived benefit of EISAC services is the combining of models to identify hotspots and analyse contingency plans under specific scenarios. For example, in case of extreme rainfall or flooding it is valuable to know which locations within a city or region potentially have the largest impact on the population’s well-being. Such modelling can be done by combining models from climate adaptation research with models of several CI such as canals, sewage systems, the electricity grid, telecommunications and transport.
- Several interviewees pointed out that current research practices are project oriented with limited overall structures. Limited follow-up occurs on research insights. EISAC can support the development of a more program-oriented approach, conserving insights and the

building and maintaining a research agenda on CI MS&A with specific linkages to other research fields.

6.2.2 Potential concerns regarding EISAC services

The NGI community expressed the following concerns:

- From a strategic management perspective by CI operators, CIP is just one concern amongst others such as efficiency, viability or sustainability. If EISAC services are primarily focused on matters of security and continuity, EISAC may be perceived as too narrowly focussed and limitedly useful for strategic decision-making.
- Some representatives of the communities emphasised the fact that EISAC will (at least partially) operate in a commercial context. Commercial interests of providers of MS&A tools may restrain from sharing models and information. Infrastructure operators may be concerned about ‘vendor-push’ and may view EISAC as a commercial outlet of (semi) private organisations. This may discourage non-commercial partners such as research institutes or universities from participating in EISAC, as their independence and non-commercial way of working is key to their relation with partners and customers. A clear distinction between commercial and non-commercial products and services is deemed necessary.
- All interviewees have emphasised that sharing information and insights is more important than the EISAC organisation itself. The services offered by EISAC, and the added value of these services for organisations that develop MS&A tools & datasets and organisations that use MS&A, must be very clear for organisations before they will spend time and effort in the sharing of models and data and contribute to EISAC events.

6.3 Summary: MS&A for NGI which may be provided by EISAC @TNO

Depending on the national governance and R&D structure, the EISAC central and national nodes may have a role in addressing NGI design challenges such as those in intelligent grids, smart cities. Moreover, the resilience of infrastructures including the resilience of dependent CI is a topic of interest of the NGI community. Services and roles that can be thought of are outlined in Table 5.

Table 5: Types of services for NGI that EISAC may provide (summary)

Service Group	Possible EISAC.node service
Advanced Decision Support	<p>Current advanced decision support by CIPRNet aims at the operational phase of CI. NGI requires decision-support during the (NGI) design or re-design/renewal phases of CI, or in other words: MS&A design support.</p> <p>(Critical) infrastructure models may overlap or be reused, but NGI requires interaction with models that look for instance at economic, market, and the dynamics of user behavioural aspects of NGI.</p> <p>An advantage could be to design economic models for NGI analysis in such a way that they (partly) can be (re)used in what-if analysis before or during a crisis.</p>
Training	<p>Resilient design of NGI requires a deep understanding of CIP/CIR, dependencies, common cause failure and CI MS&A.</p> <p>Useful for the NGI community are: Master class and CIP/CIR materials & book, and the MOOC CIP/CIR courseware.</p> <p>The CIPRTrainer technology may be used to assess possible operational crisis in a NGI and to find ways to improve the resilience in the NGI design.</p>
Information Brokerage on CIP/CIR	<p>CIPedia© may offer a common framework for NGI terminology and a place to store NGI-related definitions. The CI sector glossaries can be extended as well for NGI purposes.</p> <p>The knowledge database may become a depository for NGI good practices, pointers to NGI-related assets, etc.</p> <p>Knowledge brokerage for NGI require more dimensions than just the security / resilience and technical aspects of CI; they consider all the PESTLE (Political, Economic, Social, Technological, Legal, and Environmental) aspects.</p>
Research Platform for CIP/CIR Collaboration	<p>The NGI community will be helped most with a MS&A repository of models, reference data sets, and more.</p> <p>MS&A of the cyber-physical interactions in infrastructures given the increasing risk due to cyber threats is a joint area of interest for the NGI and CIR communities.</p>
Dissemination	<p>The CIPedia© list of conferences and events may include NGI related events to stimulate possible interaction between the NGI and CIP/CIR communities.</p> <p>For the same reason, the ECN - when continued - should outreach to the NGI community and ask for contributions.</p>

7 Conclusions on the possible role of an EISAC in the secure design of NGI

7.1 Summary of the findings

MS&A allows designers of Next Generation Infrastructures (NGI) to experiment with different architectures and to explore the effect of various design choices including the security architecture. MS&A makes it possible to assess various options amongst different conditions, for instance varying in cyber threats, climate change effects, and other challenges. MS&A of (critical) infrastructures, their dependencies, vulnerabilities and related risk to the population may provide insight in the pros and cons of the various zoning options. The visualisation that MS&A provides may show benefits or disadvantages from the various options to all stakeholders.

Therefore, CIPRNet started with the idea that the design of NGI requires new infrastructure models and efforts to federate existing infrastructure models. As part of CIPRNet's outreach, presentations by NGI communities have been attended, e.g. the PowerWeb community, NGInfra community (e.g., harbour, rail, energy of the future), Smart Grid communities, and the 100 Resilient Cities initiative. Discussions with presenters provided improved understanding of the focus and needs of the NGI community. Moreover, several interviews with NGI and other MS&A stakeholders have been held which broadened our understanding.

The discussions with both the NGI research communities and (critical) infrastructure operators made clear that the design of NGI mostly uses single fine-grained technical models at the one end of the spectrum, or coarse grain (EU-wide) grid assessment models with a nation being a grid node.

When looking at the life cycle of infrastructures on the one hand, NGI stakeholders either look at the design and planning phase of infrastructures, and at the modelling of optimising maintenance of infrastructures from a cost perspective. Security aspects that are covered focus on the physical protection, and the security of supply of the service from a capacity-based point of view.

On the other hand, the federated models that are used by, for instance, the CIPRNet community, mostly address the prevention, preparation, response and recovery phases of crisis management. An example of added-value of MS&A bridging both worlds, are the Italian RecSIM activities which aim to reduce infrastructure failure risk by finding less risky routing of new infrastructure and by pinpointing areas where additional infrastructure strengthening is required.

Currently, both communities are less overlapping than expected. On the other hand, the similar challenges have been encountered – often in between the lines – in the discussions with people in both communities:

1. Availability of data. It is often hard to acquire sensitive detailed data on the one hand, and to ask for the proper granularity of data for a proper model outcome on the other hand.
2. The cyber component in infrastructure and the cyber security of cyber-physical systems in (critical) infrastructures are hard to model, e.g. smart grids.
3. NGI often looks at the economic impact of infrastructure design and infrastructure use and maintenance redesign. The interaction of these economic models less often takes place in the realm of crisis management support, but could help in what-if analysis during the preparation and recovery phases.

4. Validation of models is not easy as there is a lack of proper reference data sets and studied outcomes.

7.2 Further development of MS&A services focused on NGI

Based on the feedback from the different communities, Advanced Decision Support is the CIPRNet service that is the most relevant for NGI. For example, the RecSIM application as part of the CIPCast system has already shown some benefits in this field. RecSIM can also be used “off-line” in a what-if simulation mode to predict the impacts on network(s) due to specific fault(s). The system was used to find less risky routing of new infrastructure and by pinpointing areas where additional infrastructure strengthening is required.

The NGI communities also mentioned the importance of information and knowledge sharing and exchange of good practices. The service ‘knowledge brokerage’ could give special attention to some of the issues of the NGI communities.

To strengthen the explore the use of MS&A models and tools by the NGI community the following steps are useful:

- *include human behaviour*: the currently available models mainly explore the technical aspects of the infrastructure; for the design of NGI the modelling of future human behavioural aspects is essential (e.g. modelling different patterns of use of the infrastructure).
- *include economical aspects*: in developing next generation infrastructures other aspects than security and protection are important, e.g. efficiency, viability or sustainability, maintenance and aging versus replacement or modality change, and market behaviour. This requires a more extensive modelling of the economic aspects, e.g. life-cycle costing.
- *further develop knowledge brokerage*: to further develop the outreach to the NGI community, the VCCC website could provide special attention to dimensions that cover the main issues for the NGI community: technical, security, legal, economical, and organisational (as part of the full set of the PESTLE aspects).

8 References

- [Alem] C. van Alem, Gasfornuis en cv rijp voor het museum: Alliander twijfelt over miljarden investeren in nieuwe leidingen, AD, 18 februari 2016, p9.
- [Amsterdam] Growth of the city of Amsterdam from 1000 to 2015, <https://www.youtube.com/watch?v=yNipxN-N8wU>
- [ARUP] Hargrave, J. (2013) “It’s Alive! – Can you imagine the urban building of the future?”, ARUP Foresight & Innovation, London, January 2013, pp 112. On-line: [url=http://discovery.ucl.ac.uk/1469384/1/145-150.pdf](http://discovery.ucl.ac.uk/1469384/1/145-150.pdf)
- [AUS280916] Extreme wind event causes blackout of power grid South Australia on September 28, 2016. <http://www.cryptogon.com/?p=49607>; <http://edition.cnn.com/2016/09/28/weather/adelaide-thunderstorm-power-blackout/index.html>; <http://www.watoday.com.au/national/state-in-the-dark-south-australias-major-power-outage-20160928-grqmn2.html>; <http://www.theaustralian.com.au/news/sa-victoria-brace-for-one-of-most-extreme-storms-in-decades/news-story/211de4b39dd336be787700ba98fc1fe0>; <https://www.aemo.com.au/Media-Centre/-/media/BE174B1732CB4B3ABB74BD507664B270.ashx>
- [Beeldbank1] Photo courtesy of Beeldbank Rijkswaterstaat: <https://beeldbank.rws.nl>, Rijkswaterstaat / Auke Leen
- [Beeldbank2] Photo courtesy of Beeldbank Rijkswaterstaat: <https://beeldbank.rws.nl>, Rijkswaterstaat / RWS Afdeling Multimedia
- [Benelux] Workshop conclusions “Energy Systems in the Benelux and Surrounding Areas Resilience Climate Change”, Brussels 10 November 2016.
- [CA] Consortium Agreement of CIPRNet
- [CEMAC] CEMAC, 30 July 2004, the Ghislenghien gas pipeline explosion... 10 years, 2014. On-line: <http://www.cemac.org/cbe/?p=668>
- [DeBruijne] De Bruijne, M. L., *Networked Reliability: Institutional Fragmentation of service provision in critical infrastructures*. Delft: Febodruk BV., 2006.
- [DEFRA] DEFRA, Climate Resilient Infrastructure: Preparing for a Changing Climate, 2011, pp 176. On-line: www.defra.gov.uk/environment/climate/sectors/infrastructure/companies/
- [DoW] Annex I – Description of Work (Annex to the Grant Agreement of CIPRNet)
- [ECCEP] European Commission, Climate and Energy Package. Website of. On-line: http://ec.europa.eu/clima/policies/strategies/2020/index_en.htm
- [ECSETP] European Commission, website European Strategic Energy Technology Plan On-line: <https://ec.europa.eu/energy/en/topics/technology-and-innovation/strategic-energy-technology-plan>
- [EDSOSG] Website EDSO for SmartGrids, On-line: <http://www.edsoforsmartgrids.eu>
- [EEGI] Website European Electricity Grid Initiative. On-line: <http://www.gridplus.eu/eegi>
- [EERA] Website European Energy Research Alliance (EERA). On-line: <http://www.eera-set.eu>
- [ENISA] Lévy-Bencheton, Cédric, et al. (ENISA), Cyber security for Smart Cities: An architecture model for public transport, 2015
- [ERANetSG] Website ERA-Net Smart Grids Plus, On-line: <http://www.eranet-smartgridsplus.eu>
- [ETPSG] Website of the European Technology Platform Smart Grids, On-line: http://www.earpa.eu/earpa/39/etp_smartgrids.html
- [EUurban] Annex to European urbanisation conference, 2014. On-line: http://ec.europa.eu/regional_policy/sources/conferences/urban2014/doc/issues_paper_annex.pdf

- [GA] European Commission, represented by REA: Grant Agreement FP7-312450-CIPRNet
- [GSGF] Website Global Smart Grid Federation, On-line: <http://www.globalsmartgridfederation.org/>
- [IEA] Website International Energy Agency. On-line: <https://www.iea.org>
- [Ijaz] Ijaz, Sidra, et al., Smart Cities: A Survey on Security Concerns, International Journal of Advanced Computer Science and Applications 7.2 (2016): 612-625
- [ISGAN] Website International Smart Grids Action Network. On-line: <http://www.iea-isgan.org/>
- [JHiner] Jason Hiner, Blog: The smart city security nightmare: How cities can stay awake, Dec 7, 2016.
- [KICIE] Website KIC InnoEnergy, On-line: <http://www.innoenergy.com/>
- [Leuven] Univ. of Leuven, Next Generation Infrastructures and smart grids. On-line: <http://www.nextgenerationinfrastructures.eu/projects/id/606497/>
- [Luijff2013] Luijff, E. "Next Generation Information-Based Infrastructures: New Dependencies and Threats." In: P. Theron (ed.), Critical Information Infrastructure Protection and Resilience in the ICT Sector. IGI Global, 2013. 304-317. Web. 7 Feb. 2013. doi:10.4018/978-1-4666-2964-6.ch015
- [Luijff2014] "Infrastructure dependencies and service quality paradoxes: a balancing act", presentation at NATO Aging and Failing infrastructures, NATO/PfP symposium, Montreux, May 26-27, 2014.
- [Luijff2017] Smart Grids: And the bad news is?, (accepted: to appear in) IJCIP, September 2017.
- [Masood] Masood, T, McFarlane, DC, Parlikad, AKN and Schooling, J (2014) The Role of Futureproofing in the Management of Infrastructural Assets. In: International Symposium for Next Generation Infrastructure, 2014-9-30 to 2014-10-1, Vienna. On-line: <http://www-smartinfrastucture.eng.cam.ac.uk/files/the-role-of-futureproofing-in-the-management-of-infrastructural-assets-masood-et-al>
- [Meko] T. Meko, Six maps that show the anatomy of America's vast infrastructure, Washington Post, 1 December 2016. On-line: https://www.washingtonpost.com/graphics/national/maps-of-american-infrastrucure/?tid=ss_tw
- [NGI] TU Delft/NGI, 6 speerpunten van toekomstbestendige architectuur, Stadszaken Delft, mei 2016. On-line: <http://www.stadszaken.nl/ruimte/mobiliteit/vitale-infra-6-speerpunten>
- [NGIBSIK] Next Generation Infrastructures: 10 jaar Improving by Understanding – eindbericht BSIK-onderzoeksprogramma, NGI, TU Delft, 2015
- [NGInfra] Next Generation Infrastructure alliance website. On-line: <http://www.nextgenerationinfrastructures.eu>
- [NISTIR] Guidelines for Smart Grid Cybersecurity, NISTIR 7628 rev 1, September 2014. On-line: <http://dx.doi.org/10.6028/NIST.IR.7628r1>
- [NISTSG] NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0, October 2014. On-line: <http://www.nist.gov/smartgrid/upload/NIST-SP-1108r3.pdf>
- [NMDC] Nationaal Modellen- en Data Centrum website. On-line: <http://www.nmdc.eu/>
- [NO] Statens Vegveser, Etatsprogrammet Moderne vegtunneler 2008 – 2011 Road Tunnel Strategy Study 2, Norway. On-line: http://www.vegvesen.no/Fag/Publikasjoner/Publikasjoner/Statens+vegvesens+rappor/attachment/368938?_ts=1394cfe7848

- [NTSB] NTSB, Collision of Two Washington Metropolitan Area Transit Authority Metro-rail Trains Near Fort Totten Station Washington, D.C. June 22, 2009, Railroad Accident Report NTSB/RAR-10/02, US National Transport and Safety Board, 2010.
- [Oasen] Oasen, Oasen plans replacement of aged drinking water pipelines. On-line: <https://www.oasen.nl/nieuws/oasen-bereidt-zich-voor-op-vervangingsperiode-leidingnet>
- [PAS182] PAS 182:2014 Smart city concept model – Guide to establishing a model for data interoperability, BSI Group standard, 2014
- [PIARC] PIARC, Life Cycle Aspects of Electrical Road Tunnel Equipment, report 2012R14EN, World Road Association (PIARC), 2012. On-line: <http://www.eesyee.gr/uploads/209/139/169212012R14EN.pdf>
- [RAEng] The Royal Academy of Engineering, Infrastructure, Engineering and Climate Change Adaptation – ensuring services in a uncertain future, London February 2011. On-line: www.raeng.org/adaptation
- [Rijkswaterstaat] Rijkswaterstaat, What is the lifetime of a bridges?, FAQ by Rijkswaterstaat. On-line: <https://www.rijkswaterstaat.nl/wegen/wegbeheer/bruggen/veelgestelde-vragen.aspx#vraag5>
- [RioNed] RoNed, Riolerling in Beeld: Benchmark rioleringszorg 2013. On-line: http://www.cobouw.nl/sites/default/files/archive/binaries/content/assets/beeld/pdf/2013/11/benchmark_rioleringszorg.pdf
- [SEGRID] EU SEGRID project. On-line: <https://segrid.eu/>
- [SETIS] European Commission, website Strategic Energy Technologies Information System (SETIS). On-line: <https://setis.ec.europa.eu/>
- [SGAM] CEN-CENELEC-ETSI Smart Grid Coordination Group, Smart Grid Reference Architecture, 2012/ On-line: <http://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx>
- [SGCG] CEN-CENELEC-ETSI Smart Grid Coordination Group, Smart Grid Reference Architecture, November 2012. On-line: https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf
- [SGIEEE] IEEE, website IEEE & Smart Grid organisation. On-line: <http://smartgrid.ieee.org/>
- [SGIEEEWF] Website IEEE Smart Grid World Forum. On-line: <http://www.ieee-pes.org/smart-grid-forum>
- [SGIP] Smart Grid Interoperability Panel (SGIP). On-line: <http://www.sqip.org/>
- [SGJRC] EU JRC, Agent Based Modelling for Smart Grids, website. On-line: <http://ses.jrc.ec.europa.eu/agent-based-modelling-smart-grids>
- [SGMM] SEI Smart Grid Maturity Model (CMM). On-line: www.sei.cmu.edu/smartgrid/
- [Sider] A. Sider and N. Friedman, Aging Pipelines Raise Concerns: More Than Half of U.S. Pipelines Are at Least 46 Years Old, Wall Street Journal, 2 November 2016. On-line: <http://www.wsj.com/articles/aging-pipelines-raise-concerns-1478128942>
- [SPARKS] EU SPARKS project. On-line: <https://project-sparks.eu/>
- [Tennet140710] Extreme winds down power pylons on July 14, 2010 in the Achterhoek, Netherlands. <http://www.cobouw.nl/nieuws/2010/07/16/Staalwerk-van-vijf-gevallen-hoogspanningsmasten-brak-af.html>; <http://www.gelderlander.nl/voorpagina/achterhoek/6981417/Zes-hoogspanningsmasten-omgewaaid.ece> <http://www.allepersberichten.nl/persbericht/14423/1/TenneT-werkt-aan-noodlijntussen-Doetinchem-en-Ulft/>
- [Tettero] Tettero, O., Out, D., Franken, H., & Schot, J. (1997). Information security embedded in the design of telematics systems. *Computers & Security*, 16 (2), 145-164.

- [USpower] Upgrading the US power grid for the 21st century, Power technology.com. On-line: <http://www.power-technology.com/features/featureupgrading-the-us-power-grid-for-the-21st-century-4866973/>
- [XPIEEE] IEEE, IEEE Xplore Digital Library. On-line: <http://ieeexplore.ieee.org/Xplore/home.jsp>