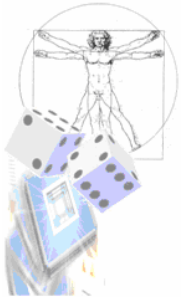
Smart Resilience Indicators for Smart Critical Infrastructures



ISO 31050: Guidance for managing emerging risks to enhance resilience – Thriving in a world of uncertainty

(ISO 31050, European Resilience and Risk Assessment and Rating and SmartResilience project approach, methodology, tools and results)

Beijing, October 30, 2018

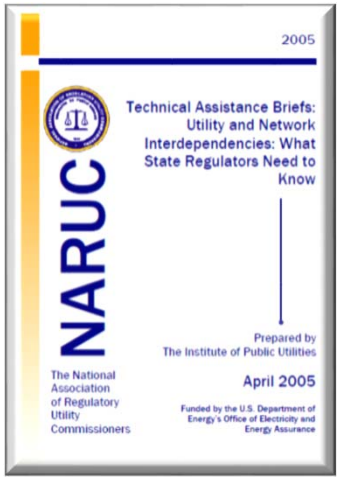
A. Jovanovic

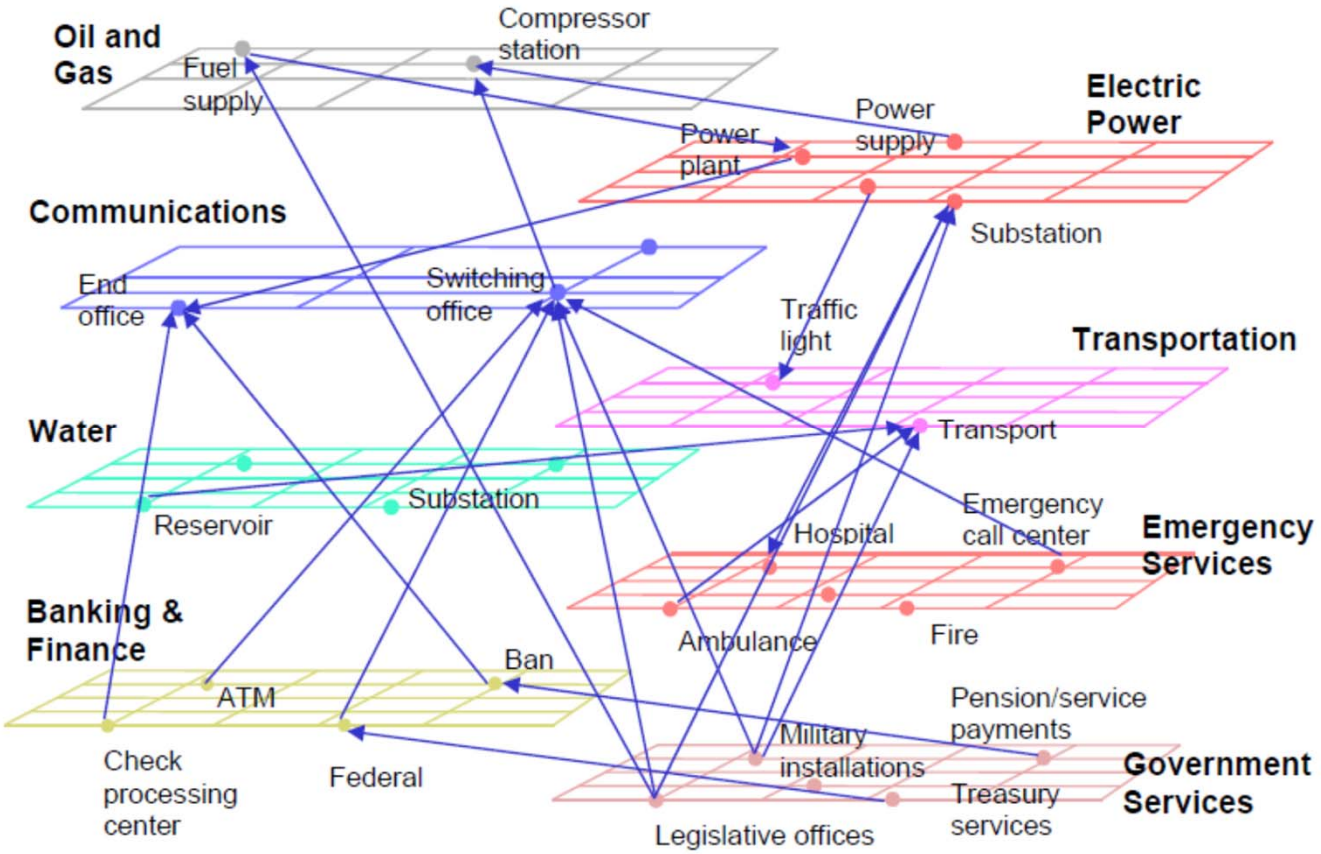
Steinbeis Advanced Risk Technologies, Stuttgart, Germany

University of Stuttgart – ZIRIUS, Stuttgart, Germany

EU-VRi – European Virtual Institute for Integrated Risk Management, Stuttgart, Germany

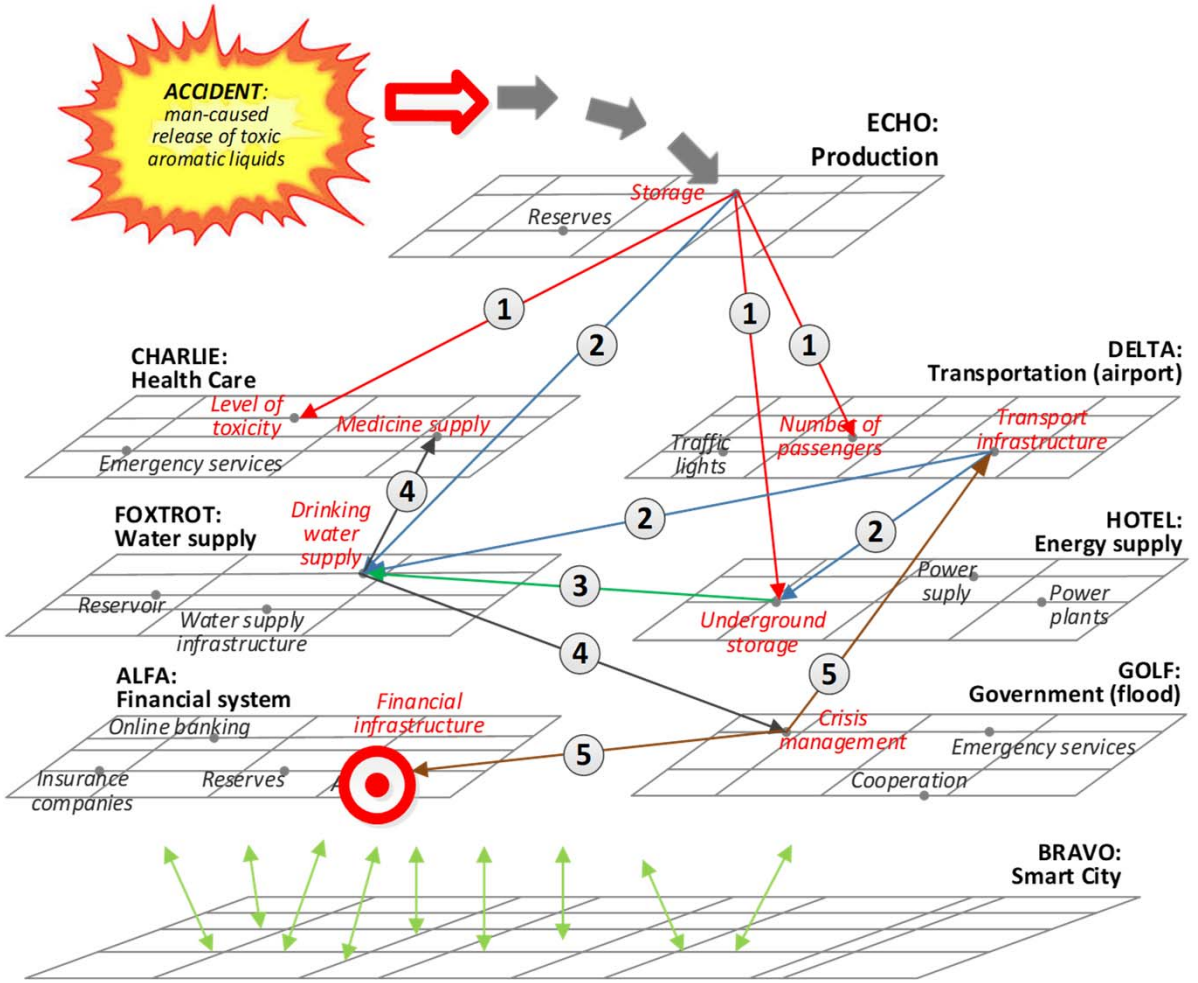
NARUC 2005 –
How much have we progressed?





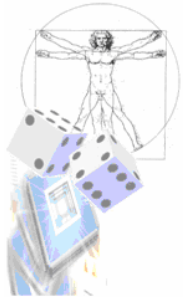
Many single answers, cases, studies, tools…

- … but NO agreed methodology… not even on one country level, let alone something globally agreed
- EU: 600+ projects, many talking about cascading, ripple, inter-this-inter-that…
- Here: Examples from SmartResilience project



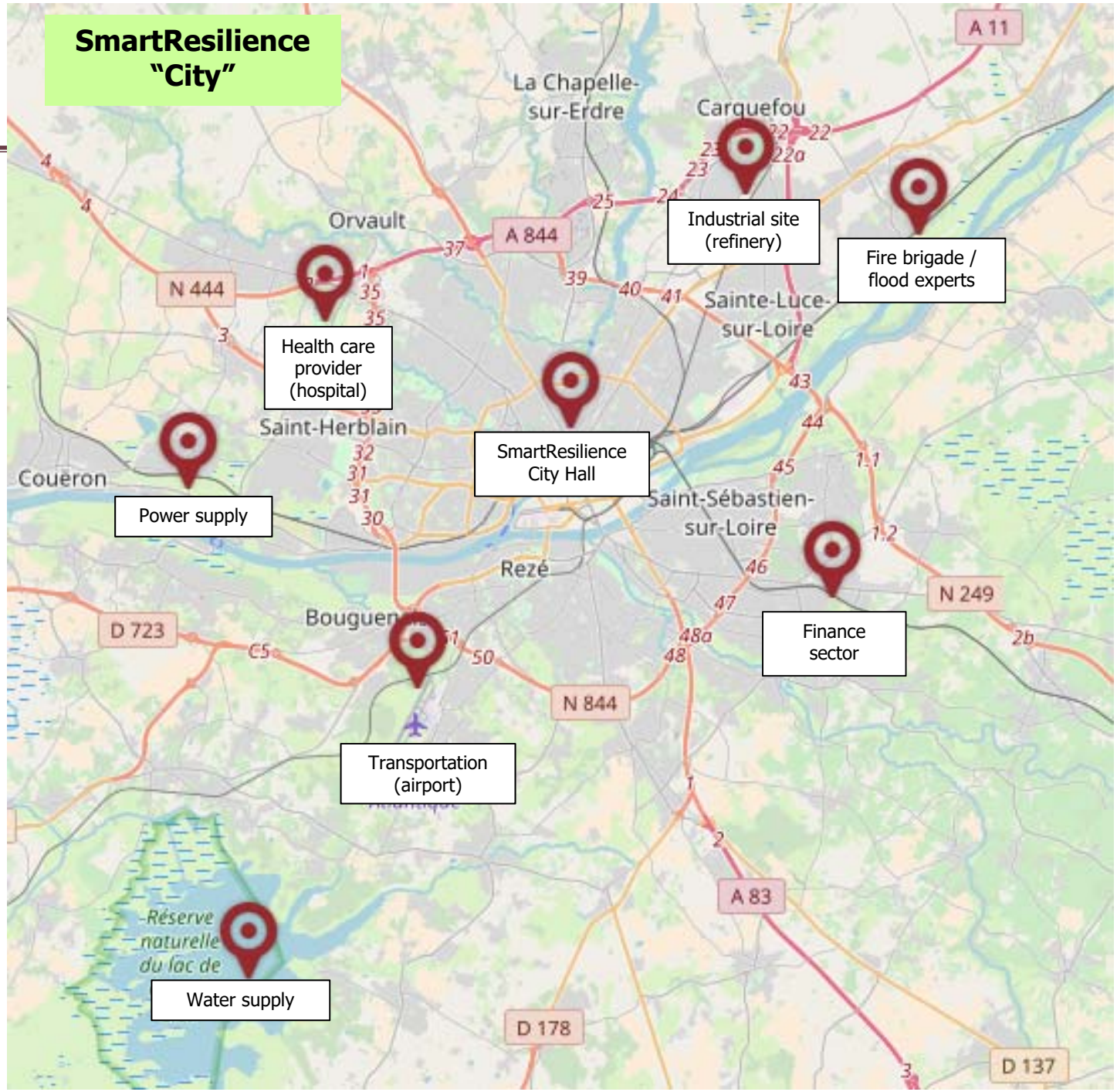
Multiple threats…
terror, cyber, weather, health, …

Infrastructure (CI) / Scenarios	Terrorist attack	Cyber attack	Extreme weather incl. NaTech events	IC-specific events	Cross-cutting issues
• Smart cities (Germany, UK, Ireland)	✓	✓	(✓)	Social unrest, urban floods	Insurance, law enforcements, legislation, …
• Smart health care (hospitals, Austria)	(✓)	✓	(✓)	Massive breach of privacy	
• Smart energy supply systems (Finland)	✓	(✓)	(✓)	Solar storms (space weather)	
• Smart industrial/production plants (new and refurbished plants, Industry 4.0 plants)	✓	✓	✓	Interruptions in the critical supply chains	
• Smart transportation (airports; Hungary)	✓	✓	✓	Border control	



Imagine an accident/event… in an infrastructure-of-infrastructures (the “INDIA” case in SmartResilience project)

infrastructure-of-infrastructures



SmartResilience "code names"

ALPHA:
Finance sector

BRAVO:
Smart city hall (headquarters HQ)

CHARLIE:
Health care provider (hospital)

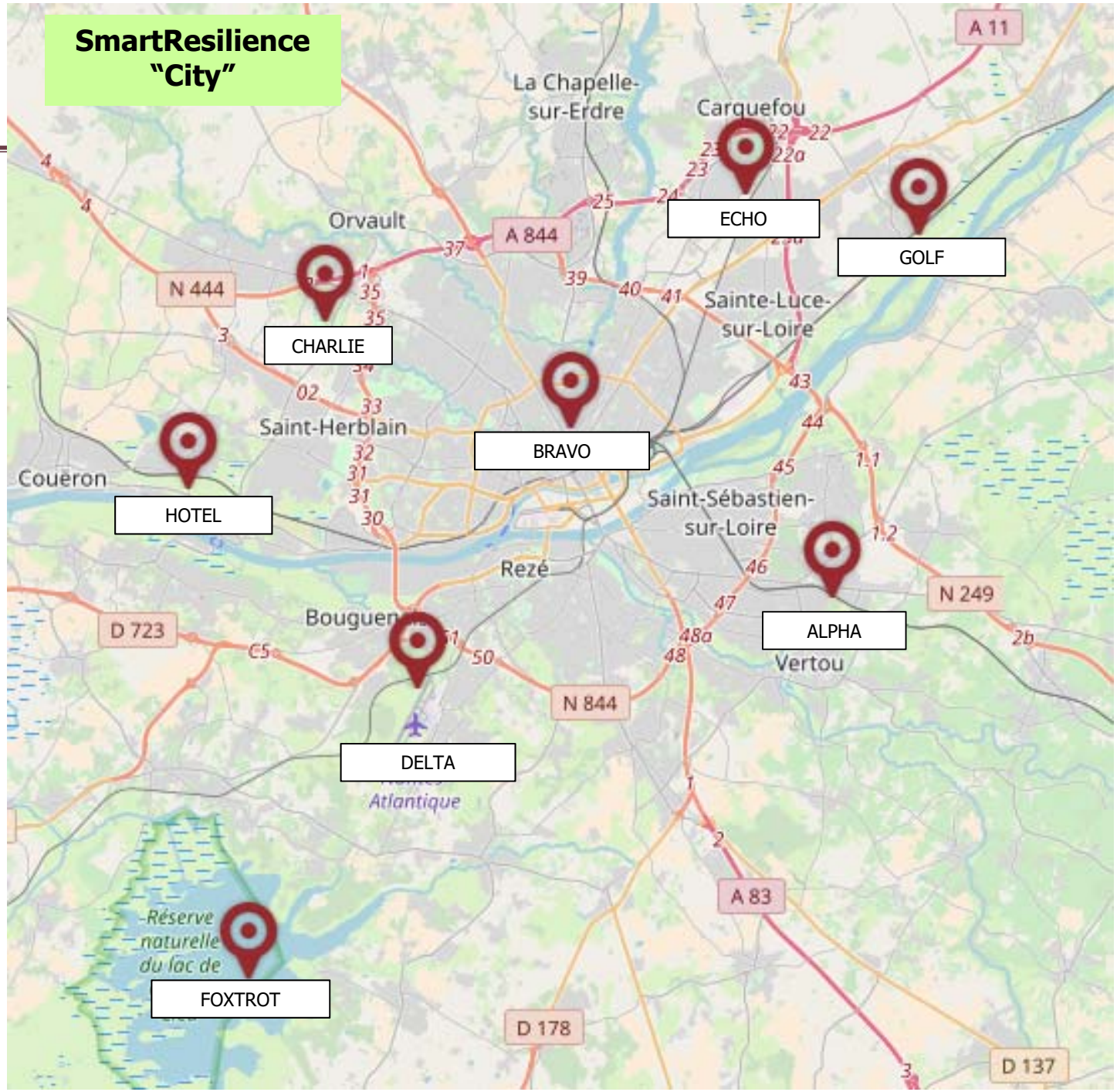
DELTA:
Transportation (airport)

ECHO:
Industrial site (refinery)

FOXTROT:
Water supply

GOLF:
Fire brigade / flood experts

HOTEL:
Power supply

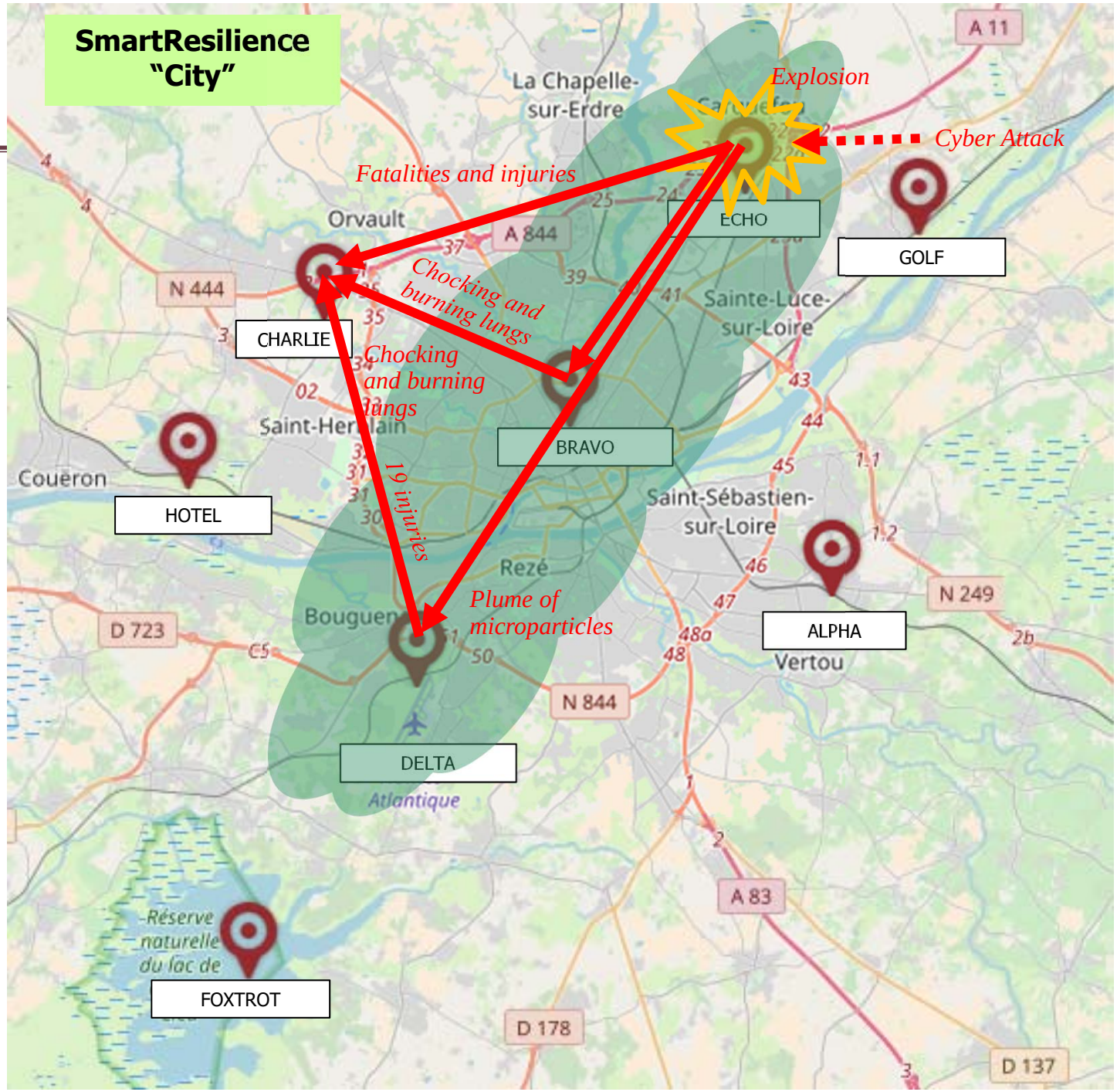


Imagine an event
(the “INDIA” event in SmartResilience project)

Time	Event description (announcement)
Day 1 05:00	explosion in the ECHO industrial production complex within BRAVO city.
Day 1 05:24	DELTA Air Traffic Control issues NOTAM due to lack of visibility and the aggressive chemical nature of the fog arising from explosion
Day 1 05:30	Certain districts of BRAVO city must be evacuated
Day 3 16:00	CHARLIE health service providers report that they have no more capacity at local service providers.
Day 5	Heavy rainfall hits BRAVO city (more than 100 mm in one day with a very intensive period), causing pluvial flood, immediately followed by a tidal flood.
Day 12	Financial systems report extended spear-phishing attempts on customers of banking and insurance services.
Day 8	FOXTROT waterworks report that the flood had contaminated the FOXTROT drinking water reservoir
Day 10	HOTEL underground storage plant reports that it has been successfully sealed off and prevented flooding of coal reserves,
Day 12	CHARLIE: bacteria in the drinking water system is resistant to carbapenems and the last line antibiotic colistin as well. Through the damage of an antibiotic storage caused by the recent incidents, both antibiotics are release into the water, killing non-resistant bacteria and facilitating overspread of resistant strands.

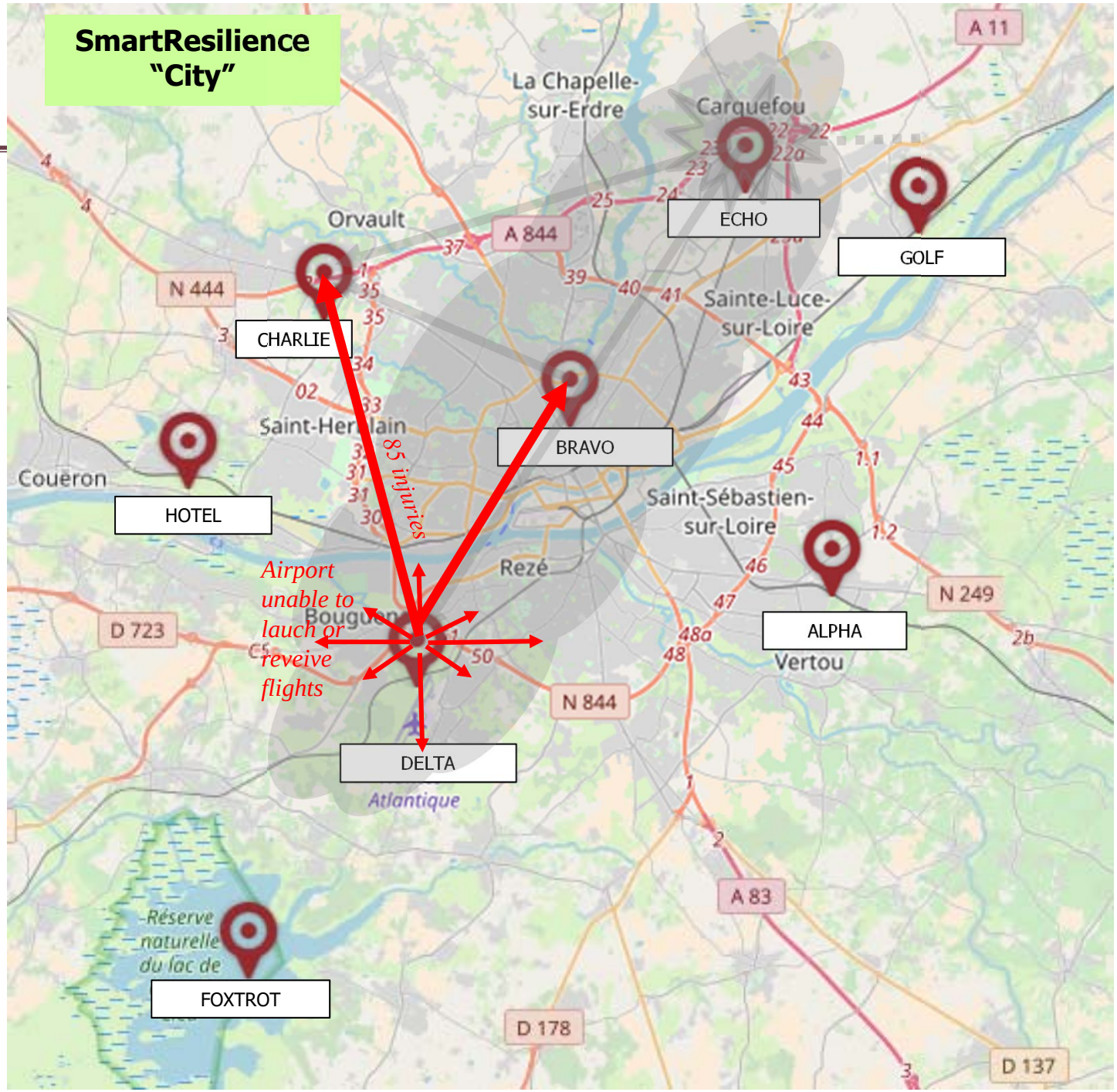
Day 1
5:00 AM

A cyberattack causes ***explosion in the ECHO industrial production complex within BRAVO city.*** *The attack releases a large fog of microparticles. Lots of casualties, the fog is choking and burning lungs of people inhaling it. The wind blows the plume across the river towards densely inhabitated area of BRAVO city and towards the airport DELTA. 19 fatalities and 19 injured (38 casualties).*



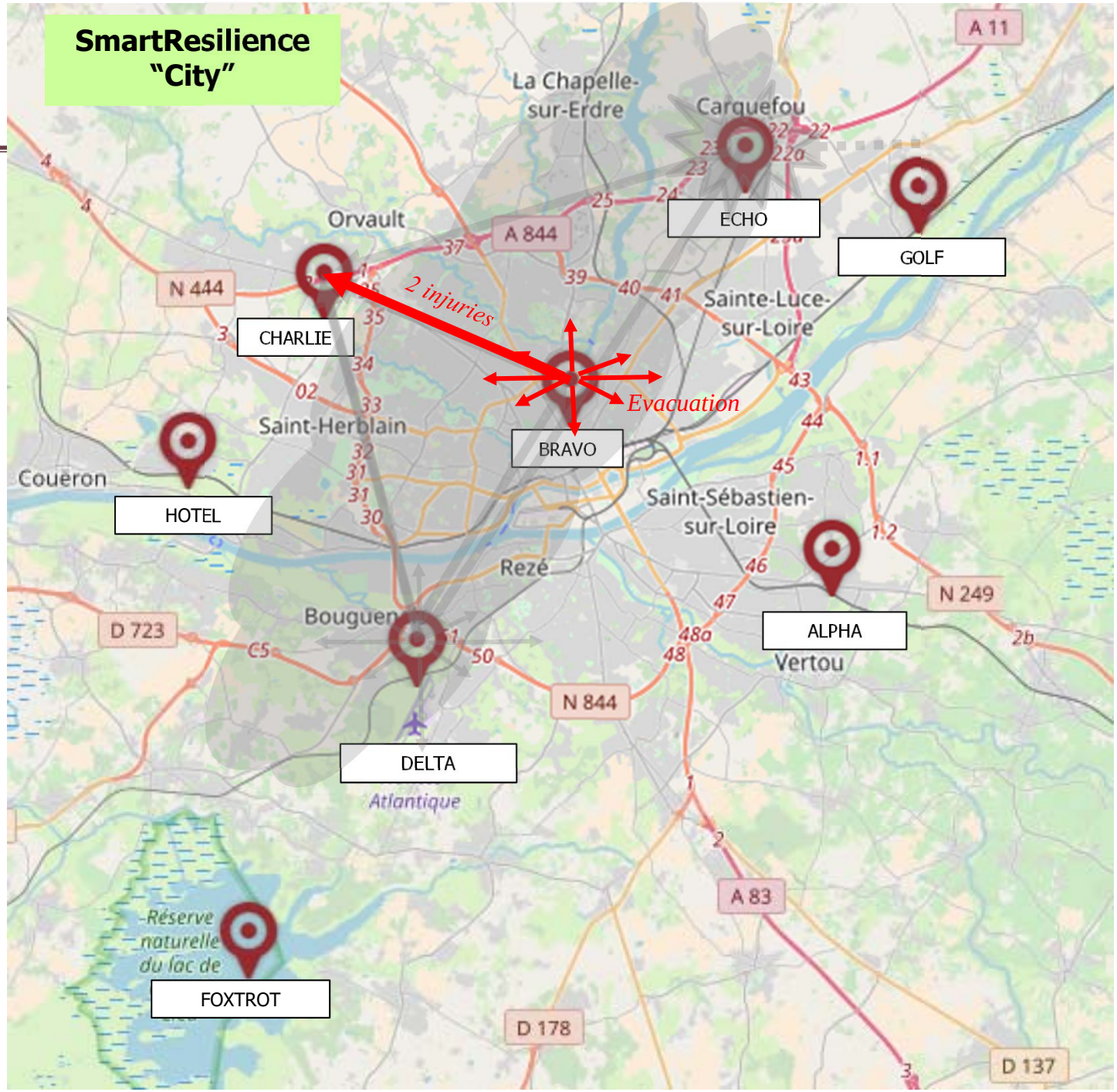
Day 1
5:24 AM

DELTA Air Traffic Control issues NOTAM due to lack of visibility and the aggressive chemical nature of the fog arising from explosion and declares DELTA airport unable to launch or receive flights. All airplanes are grounded. Passengers were sheltered inside the terminal as the fog covers the passenger terminal as well. Another 34 fatalities and 85 injured (157 casualties).



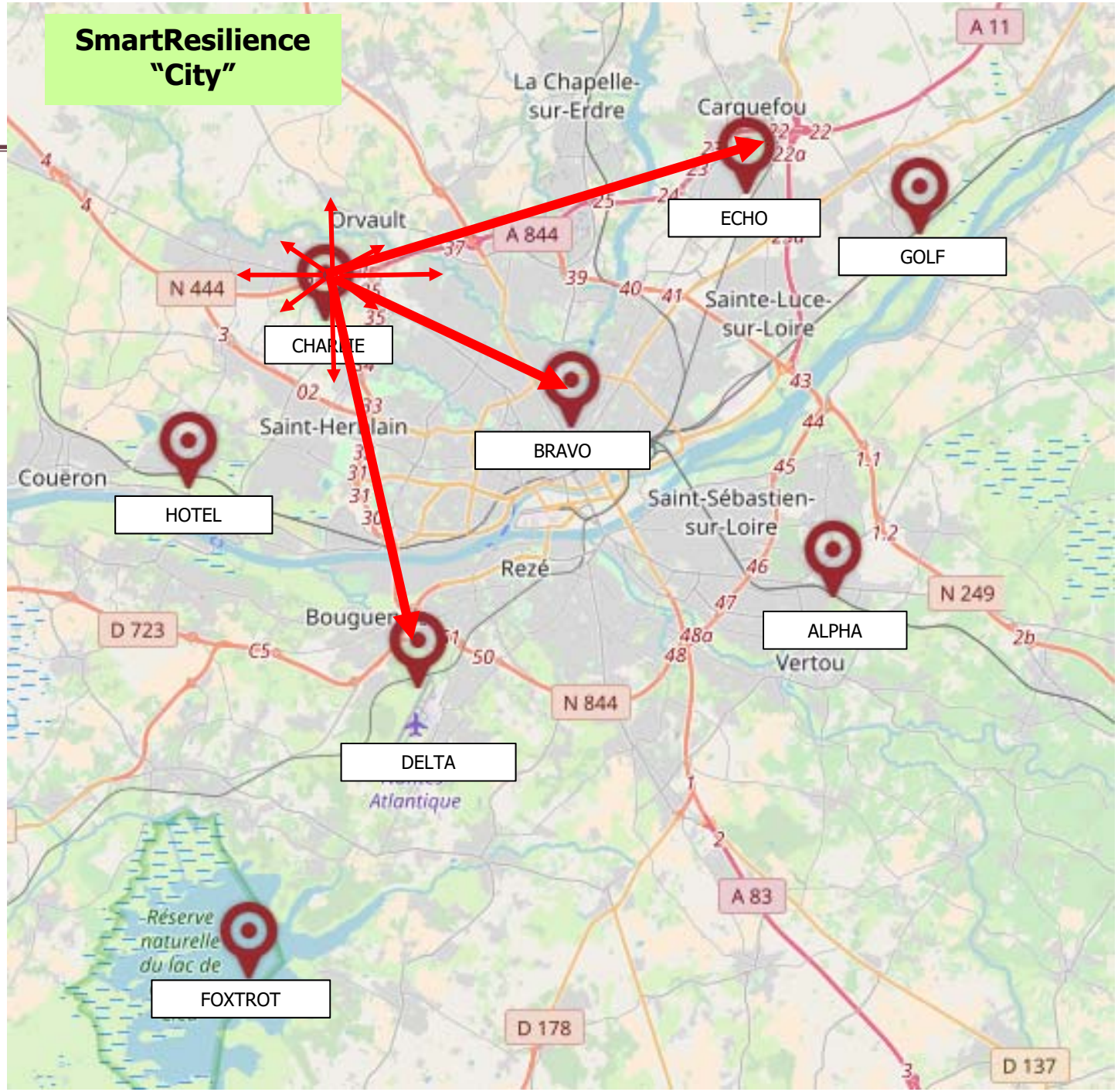
Day 1
5:30 AM

Certain districts of BRAVO city must be evacuated, in the other parts residents are advised to keep shut all doors and windows. Some citizens decide to self-evacuate. Roads get overcrowded. Another 83 fatalities and 2 injured (242 casualties).



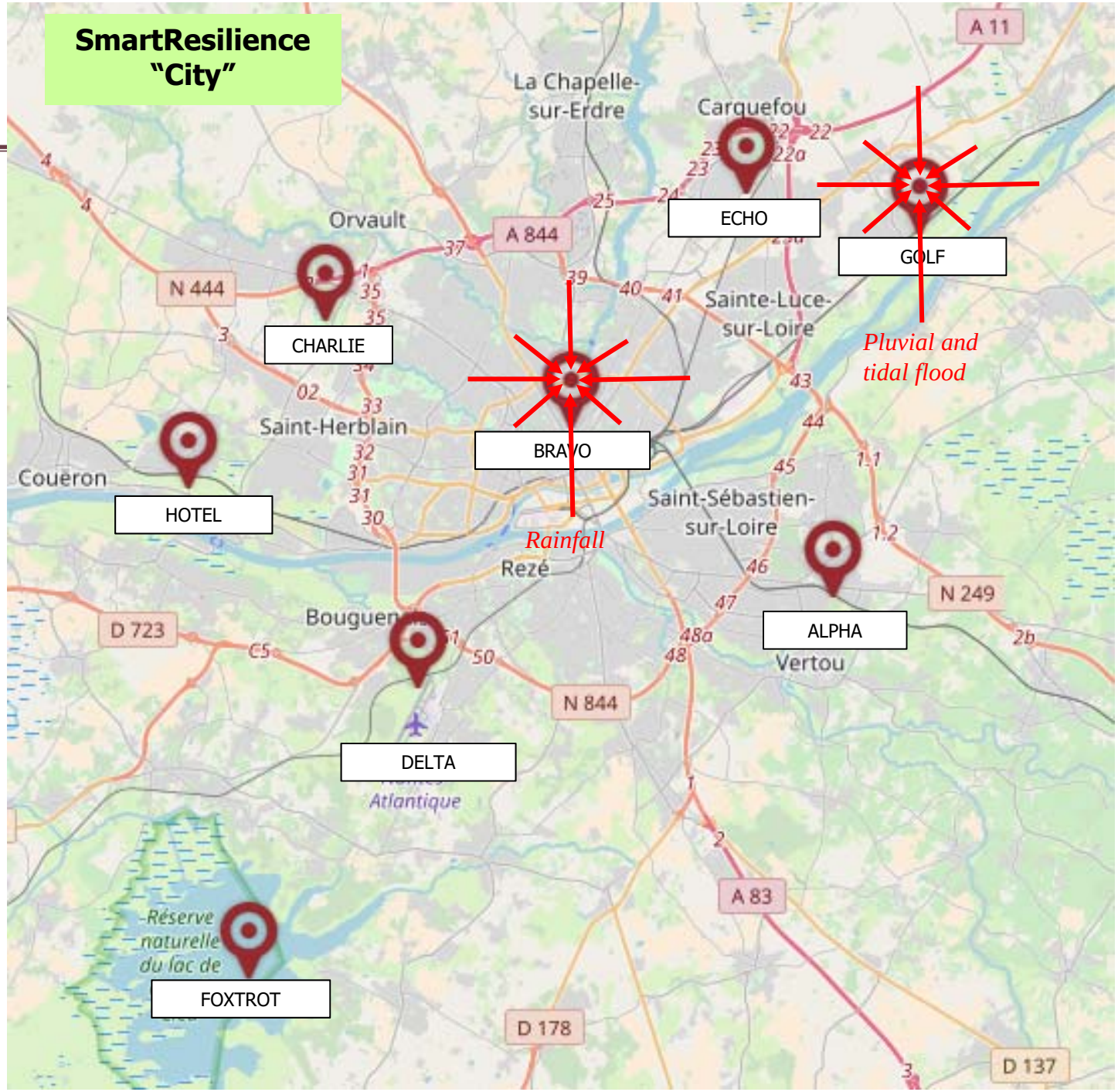
Day 3
16:00 PM

CHARLIE health service providers report that they have no more capacity at local service providers. During first medical response, 21 employees get injured and can not continue their work, in spite of efforts of health service staff, 51 more fatalities and 64 more injuries occur during decontamination efforts and aftermath. (378 casualties).



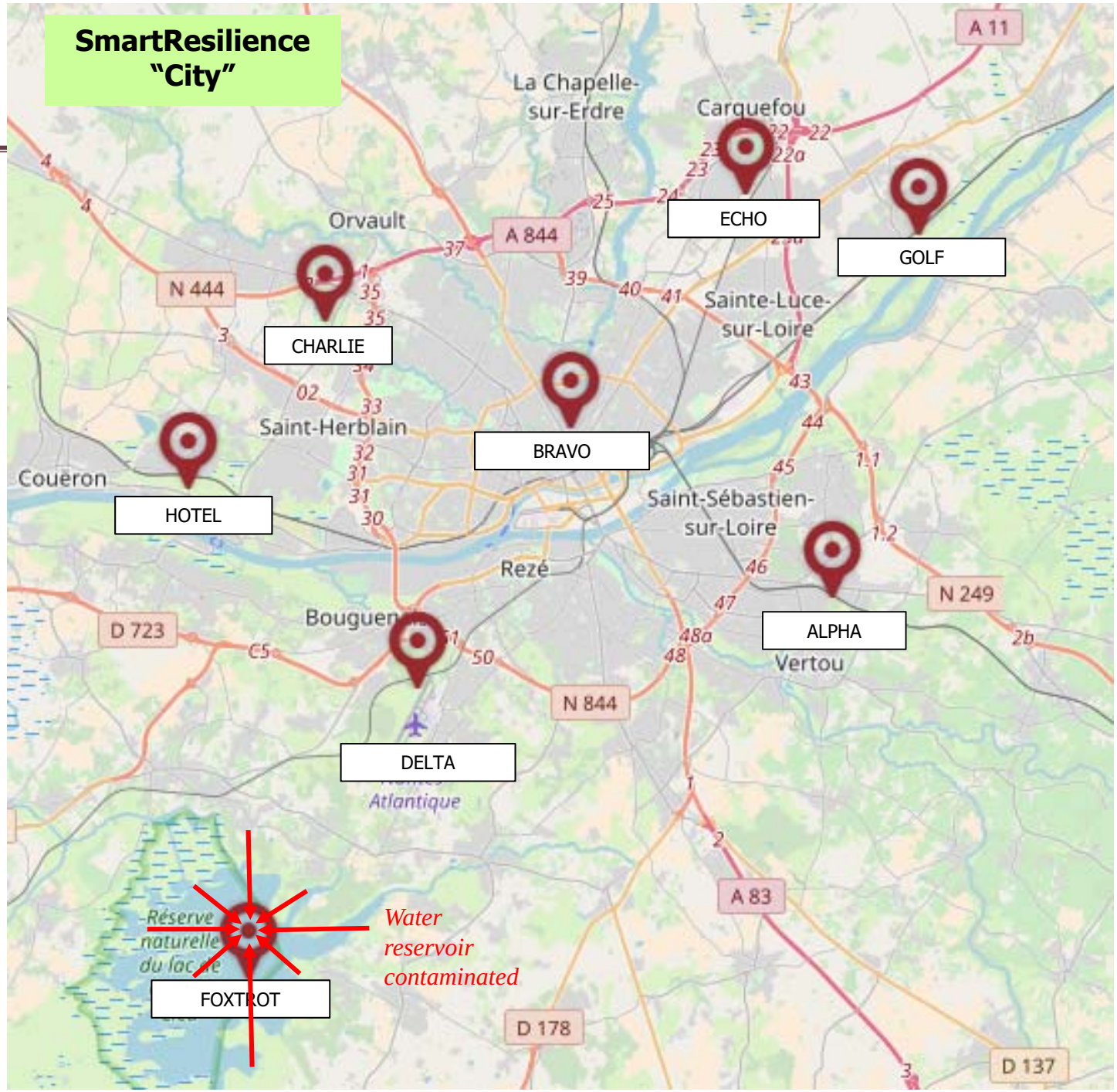
Day 5

Heavy rainfall hits BRAVO city (more than 100 mm in one day with a very intensive period), causing pluvial flood, immediately followed by a tidal flood. GOLF flood protection facilities are not able to prevent water rising on the streets. 59 dead, 2 injured (439 casualties).



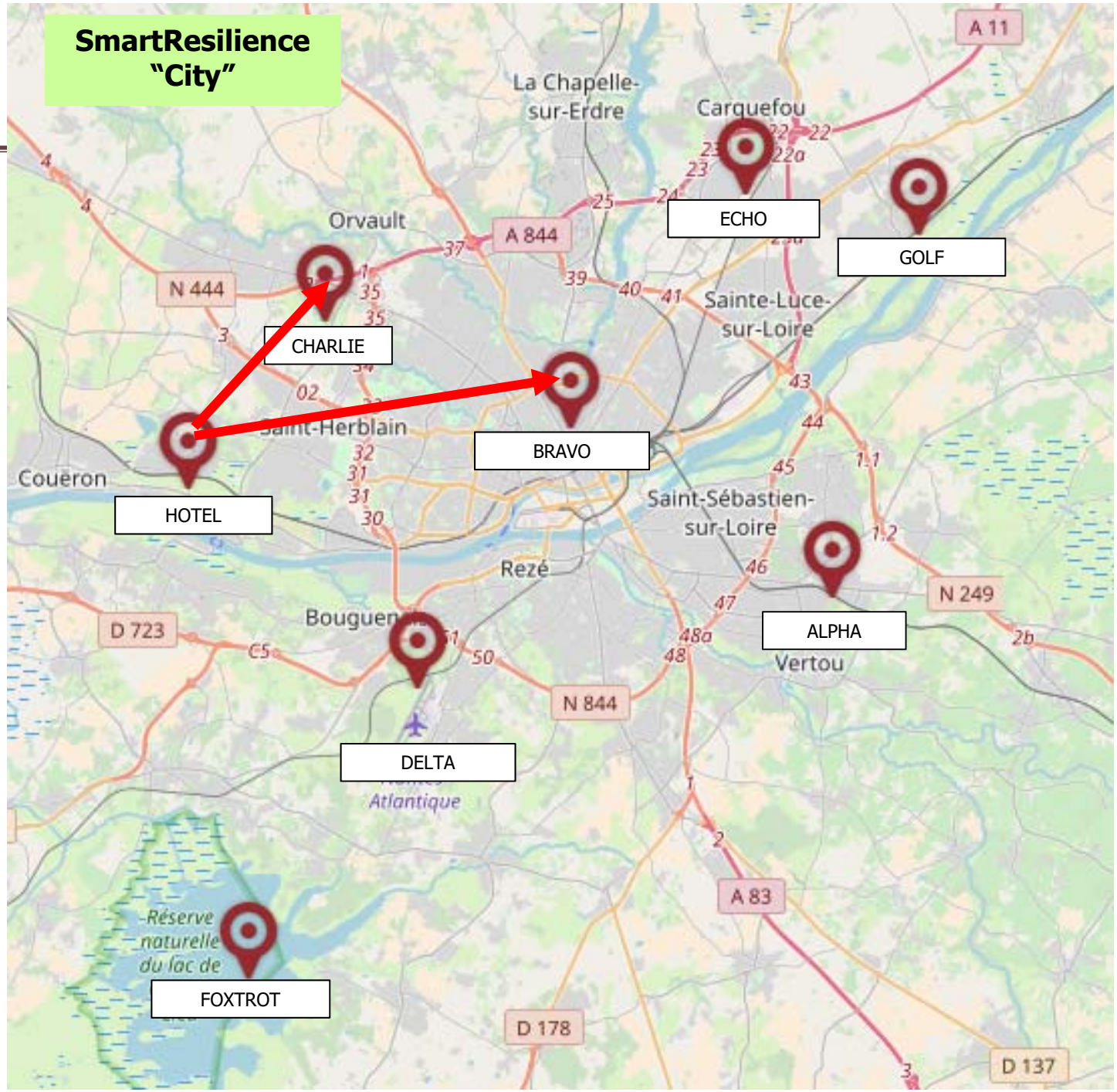
Day 8

FOXTROT waterworks report that the flood had contaminated the FOXTROT drinking water reservoir by washing water from the on-site wastewater treatment plant of ECHO production site into the river and from the river to the lake. They detected large amount of antibiotics-resistant bacteria multiplying rapidly in the drinking water. The bacteria are resistant to carbapenems and the last line antibiotic colistin as well, both antibiotics are also present in the contaminated water.



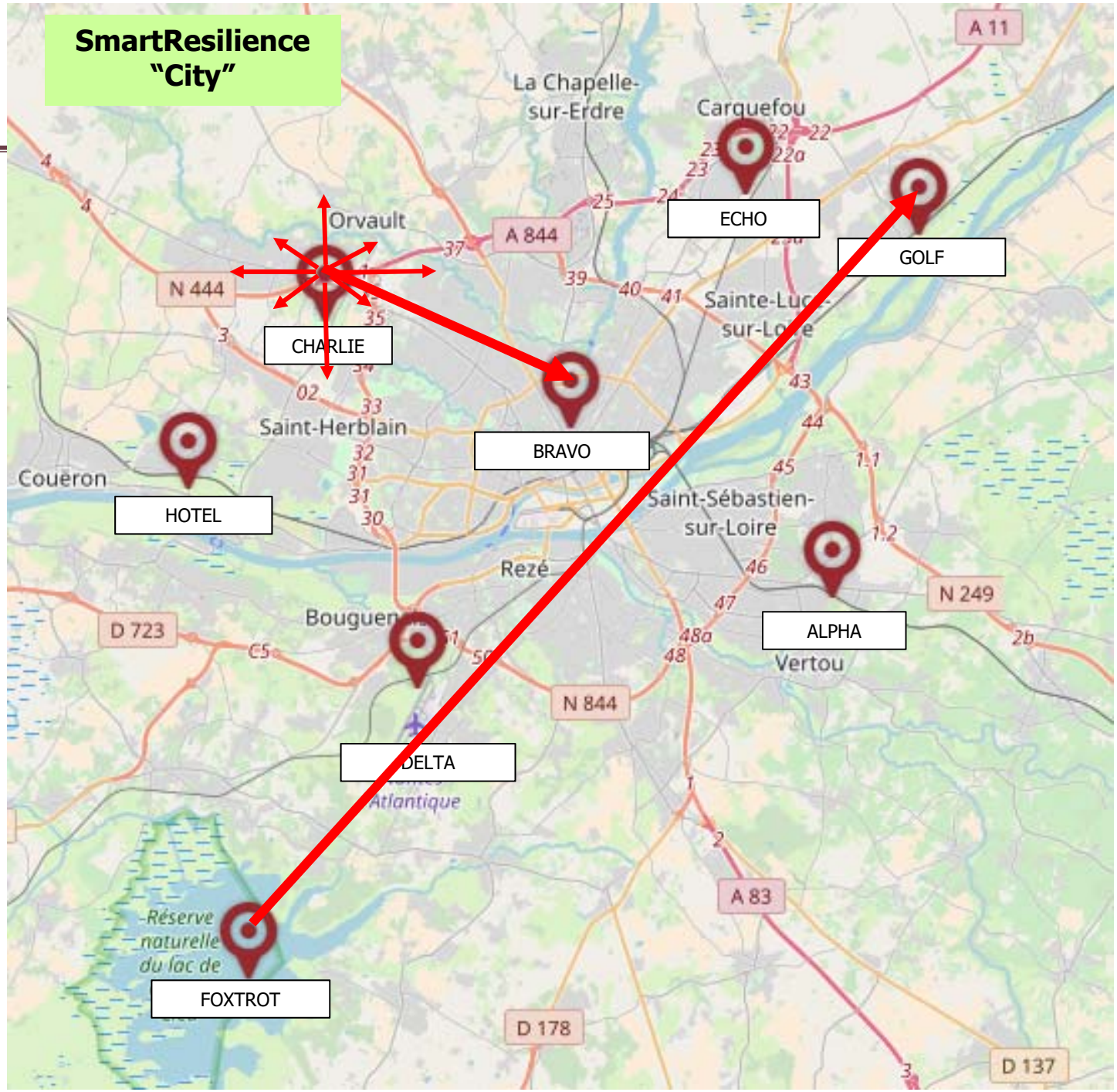
Day 10

HOTEL underground storage plant reports that it has been successfully sealed off and prevented flooding of coal reserves, but one out of the four storages is suffering a self-ignition. 2 fatalities and 2 injured (441 casualties)



Day 12

A given percent of the ***bacteria in the drinking water system is resistant to carbapenems and the last line antibiotic colistin as well. Through the damage of an antibiotic storage caused by the recent incidents, both antibiotics are release into the water, killing non-resistant bacteria and facilitating overspread of resistant strands.*** *CHARLIE health system is not able to cure infected patients. 810 people got infected and there is no available remedy for them (1251 casualties).*



SMART RESILIENCE

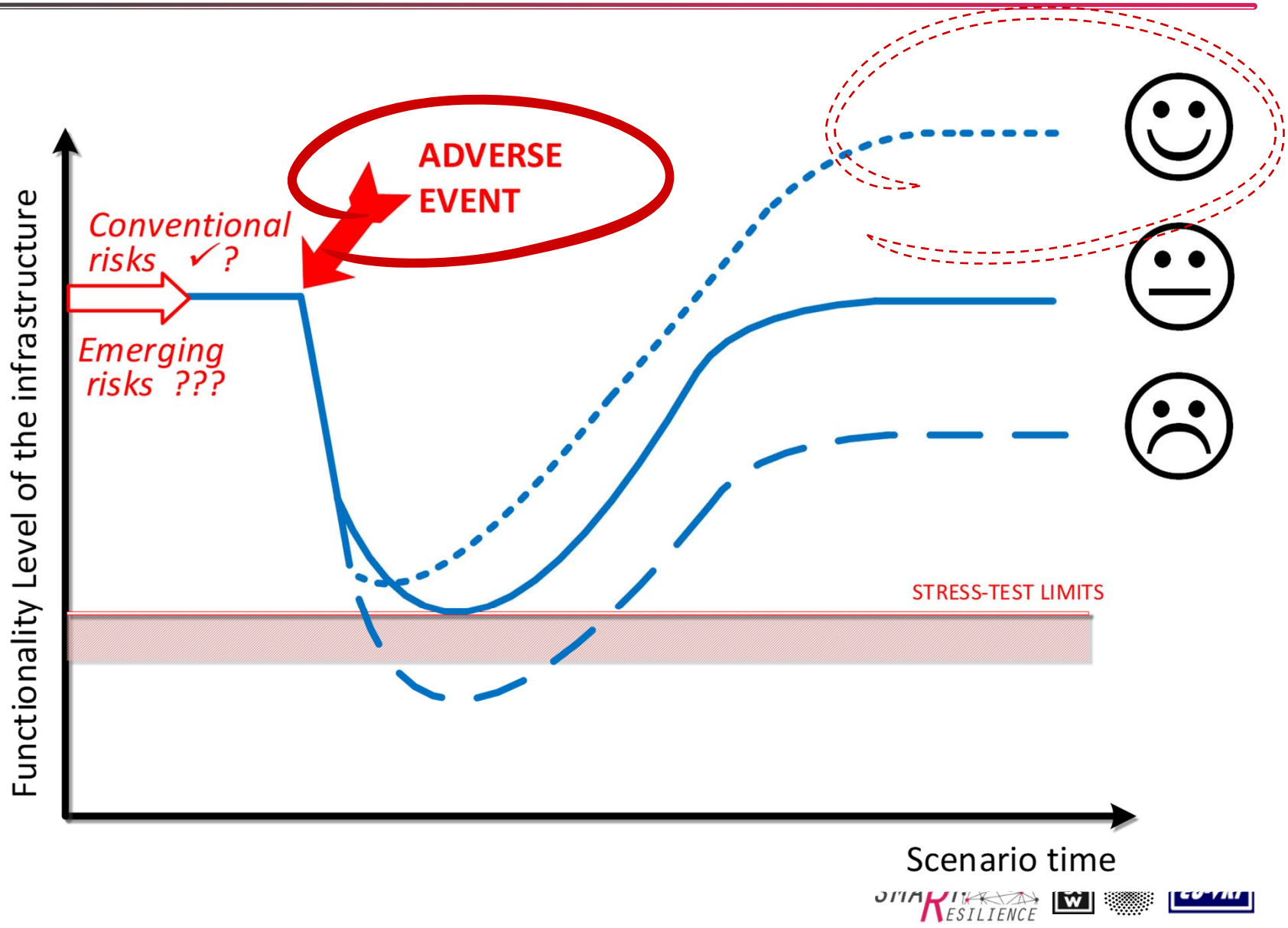
Smart Resilience Indicators for Smart Critical Infrastructures

Key questions

1. Do we need indicators? Do we need indicator-based resilience assessment?
2. If yes, how to do it? How to MEASURE resilience of critical infrastructures and systems… in the age of information overload?
3. How to deal with unknown or poorly known threats?
4. If we do it, how to do it in a globally agreed way?
5. Who's concern is the "resilience of the world"?

SMART RESILIENCE EU-VRi

… manage risks to enhance resilience:



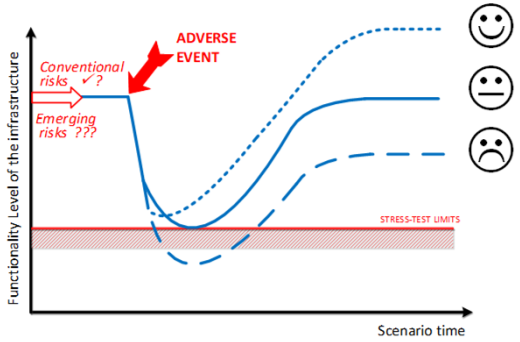
SMART RESILIENCE

Smart Resilience Indicators for Smart Critical Infrastructures

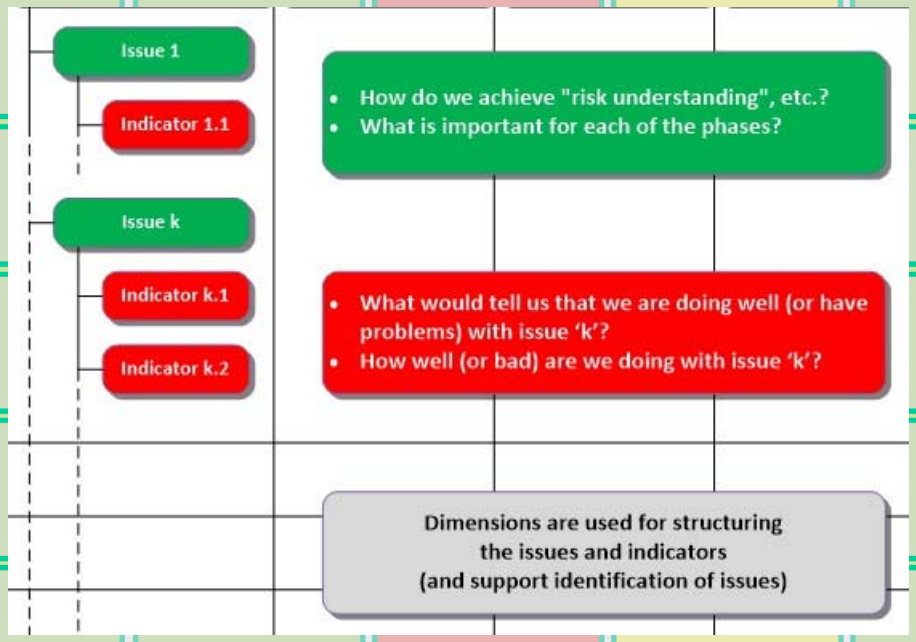
Indicators-based resilience assessment?

We need a METHOD

ISO 31050 – new way, the 5x5 matrix:
… manage emerging risks to enhance resilience



	Understand (emerging) Risks	Anticipate / Prepare	Absorb / Withstand	Respond / Recover	Adapt / Transform
System / Physical					
Information / Data / Smartness					
Societal / Political					
Cognitive / Decision Making					
Organization / Business					

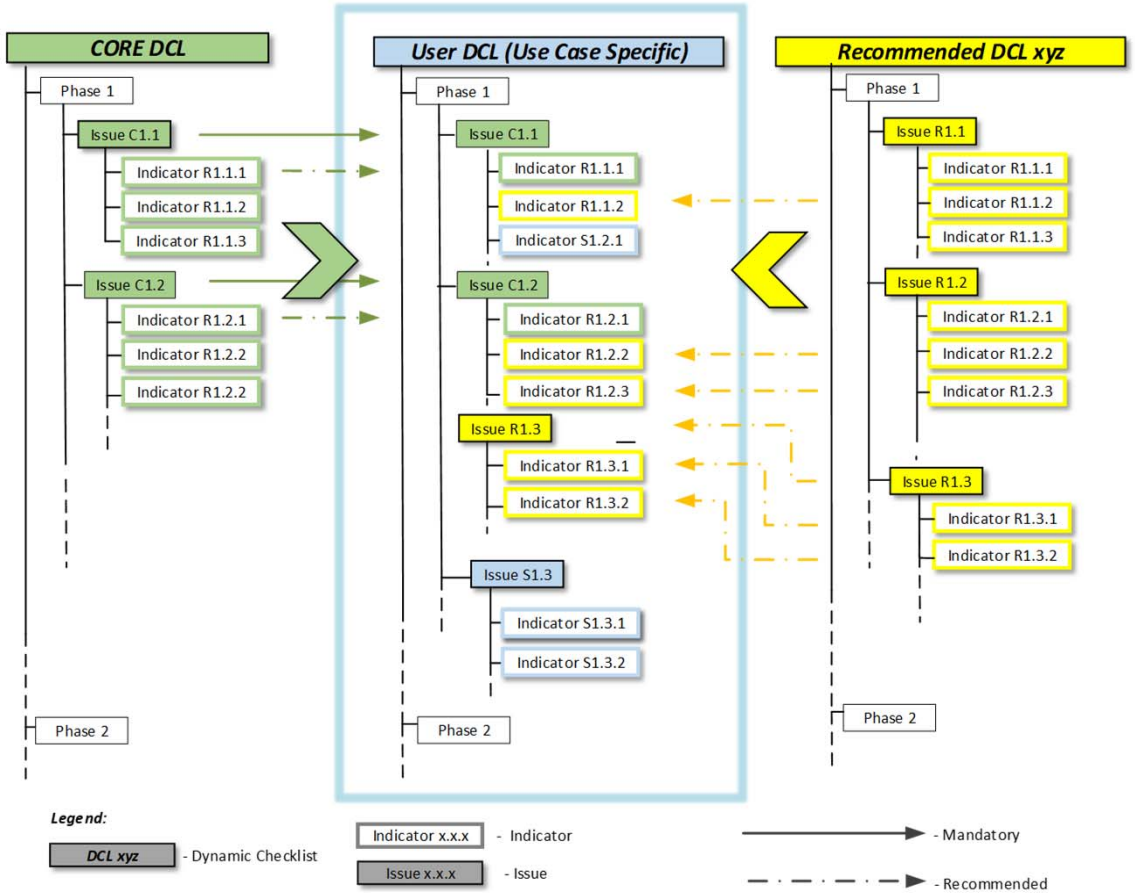


Create (customized, but still comparable) checklists of indicators

Same for all ("CORE")…

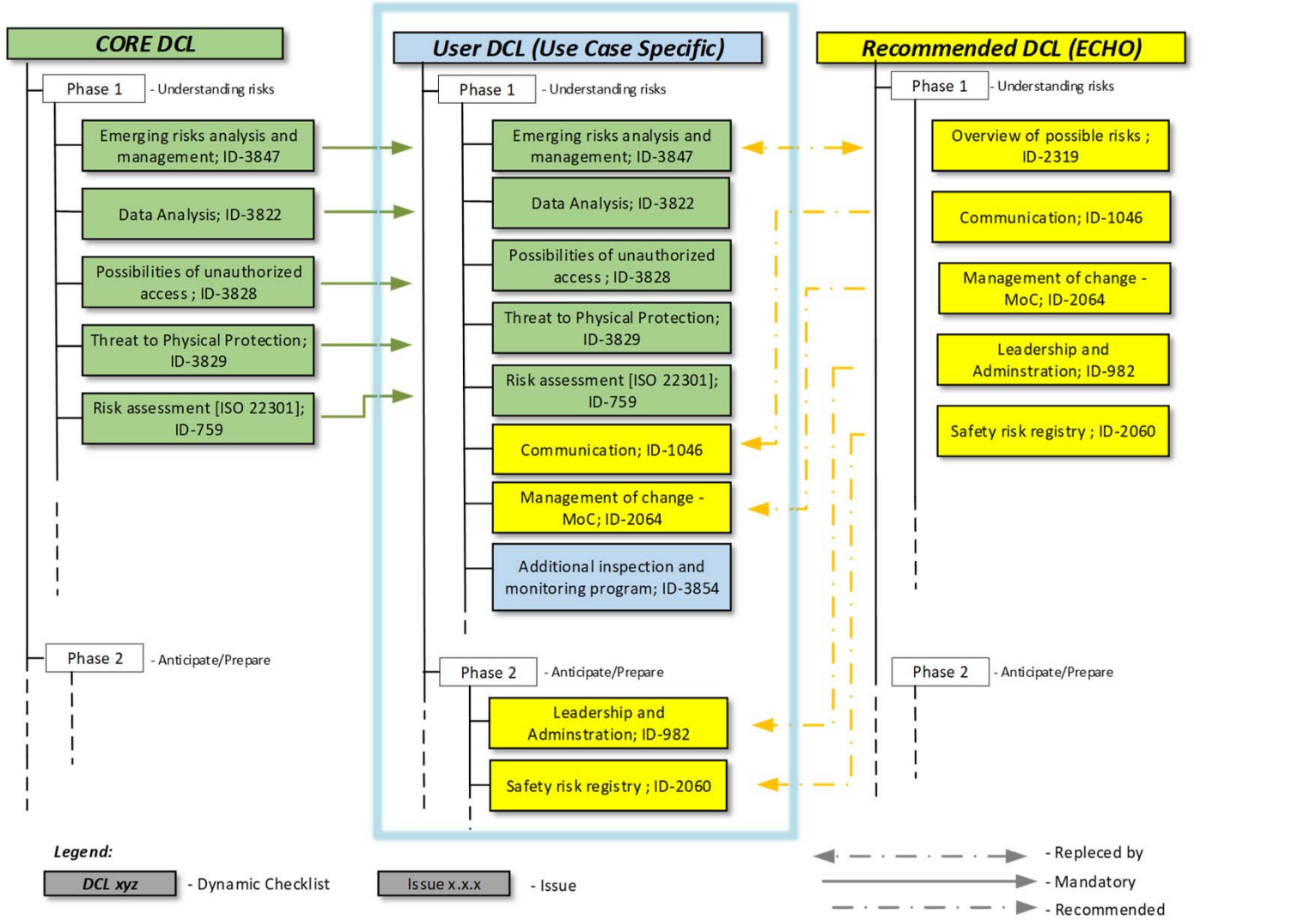
User's customized list…

Recommended for a sector…

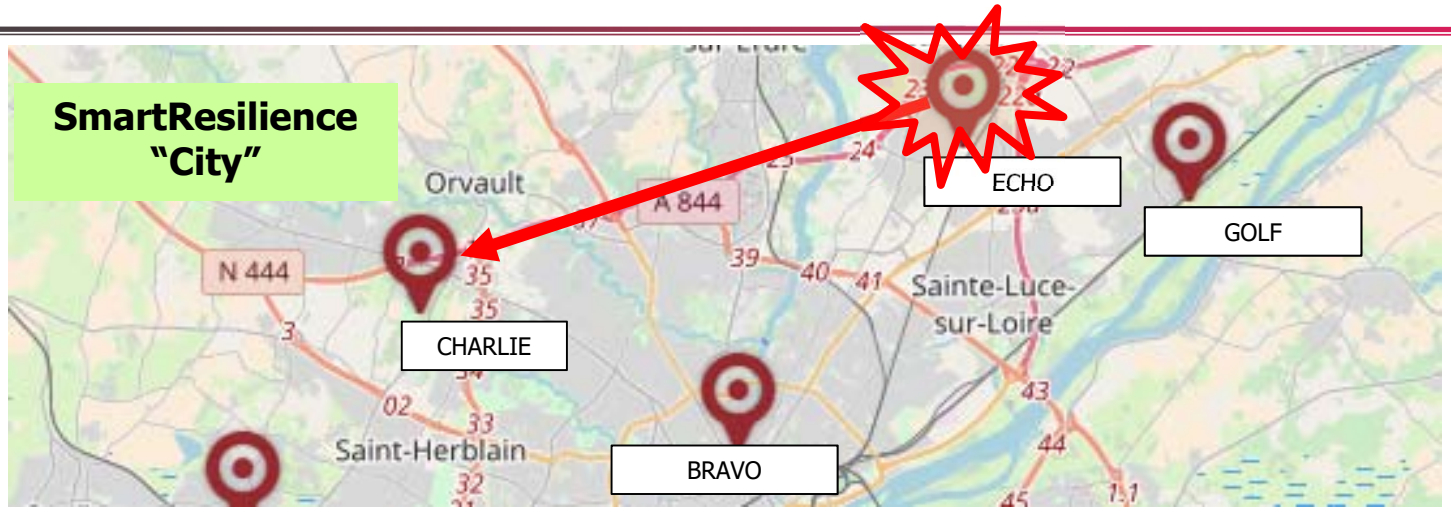


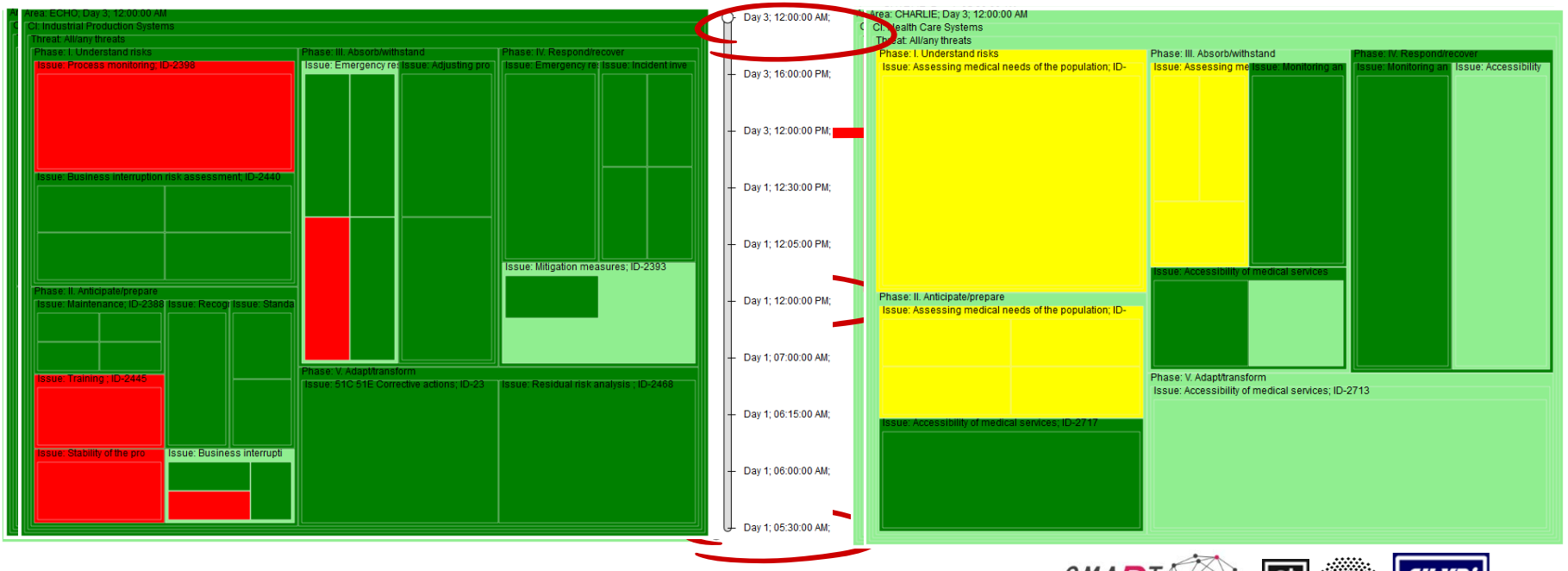
- **I. UNDERSTAND RISKS**
  - Risk assessment [ISO 22301]; ID-759
  - Data Analysis; ID-3822
  - Possibilities of unauthorized access ; ID-3828
  - Threat to Physical Protection; ID-3829
  - Emerging risks analysis and management; ID-3847
  - New types of ICT attack to smart Infrastructure; ID-3863
- **II. ANTICIPATE/PREPARE**
  - Training ; ID-988
  - Business continuity plan [ISO 22301]; ID-1031
  - Use of smart technologies and devices for safety and security; ID-3517
  - 51C Emergency management/planning; ID-2258
  - Management of information and knowledge relevant for resilience; ID-3823
  - Physical Protection; ID-3812
  - Cyber operation continuity plan; ID-3833
  - ICT Attacks monitoring; ID-3865
- **III. ABSORB/WITHSTAND**
  - Business continuity plan [ISO 22301]; ID-1031
  - Physical Protection; ID-3824
  - Cyber operation continuity plan; ID-3833
  - 51C Emergency management/planning; ID-2258
  - Offsite/external capabilities and resources available; ID-3834
  - Command/Coordination structures availability and effectiveness; ID-3837
  - First Preventer/Responder available and effective; ID-3836
  - Proper use of smart CI related procedures and protocols ; ID-3866
- **IV. RESPOND/RECOVER**
  - Emergency response; ID-996
  - Incident management plans and procedures effectiveness; ID-3825
  - Management of information and knowledge relevant for resilience; ID-3823
  - Impact of dependencies on resilience; ID-3835
  - Proper use of smart CI related software; ID-3867
- **V. ADAPT/TRANSFORM**
  - Business continuity plan [ISO 22301]; ID-1031
  - Incident investigation; ID-1004
  - Emergency response reporting including lessons learned ; ID-3826
  - Availability of adequate human resources; ID-3827
  - Management of information and knowledge relevant for resilience; ID-3823
  - Organizational learning and continual improvement; ID-3848
  - Measuring adaptation/trasformation; ID-3860
  - Improving smart IC related protection capacity; ID-3869

How to create a DCL needed for a particular case?

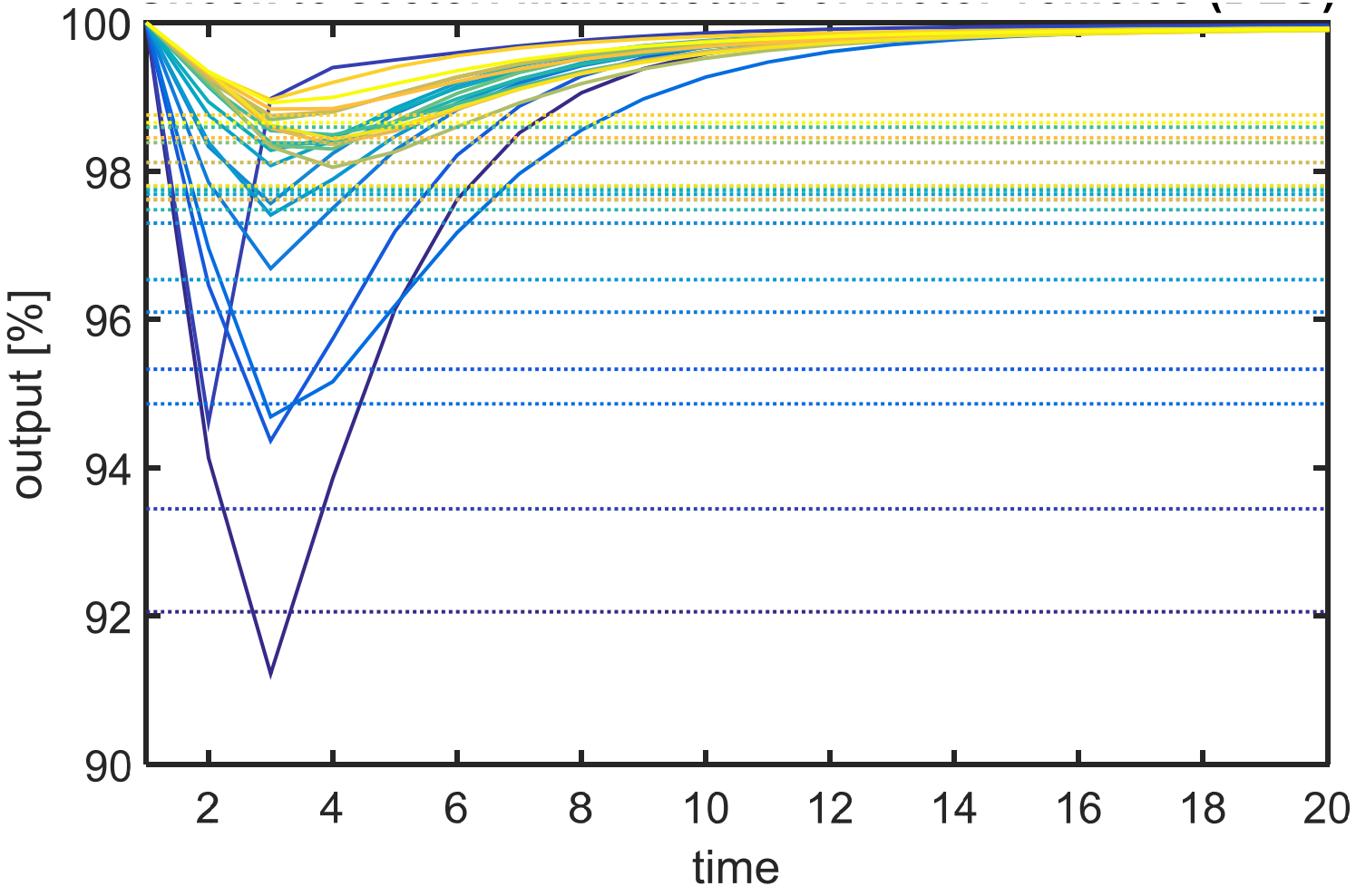


Indicators telling what happens in an “infrastructure-of-critical-infrastructures”:

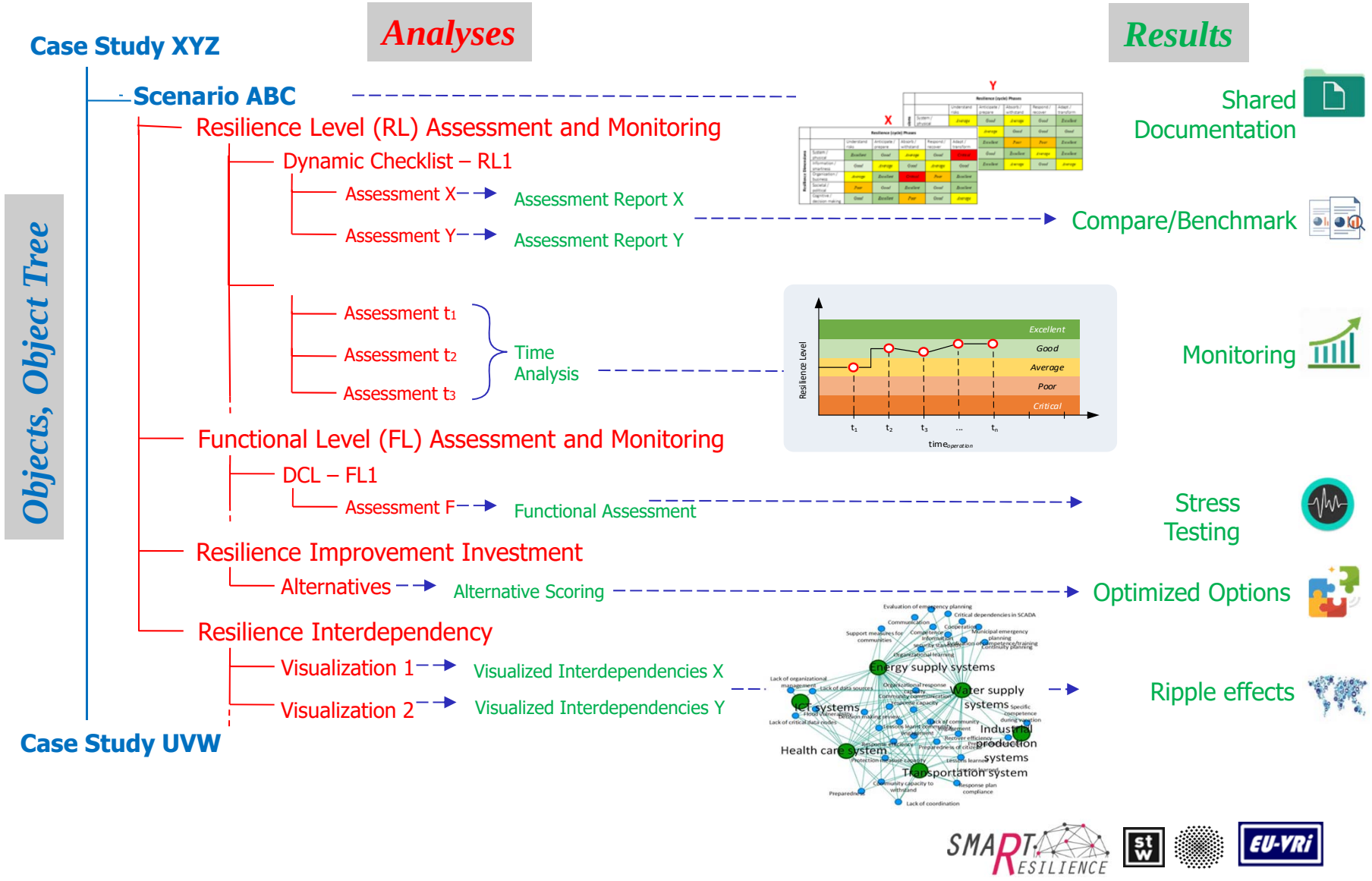




… manage risks to enhance resilience: also in infrastructure-of-infrastructures



Integrated, indicator-based, resilience analysis: resilience level, functionality loss, interdependency…



SMART RESILIENCE

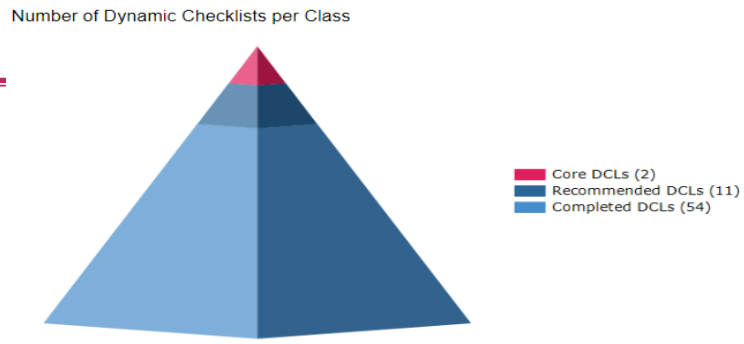
Smart Resilience Indicators for Smart Critical Infrastructures

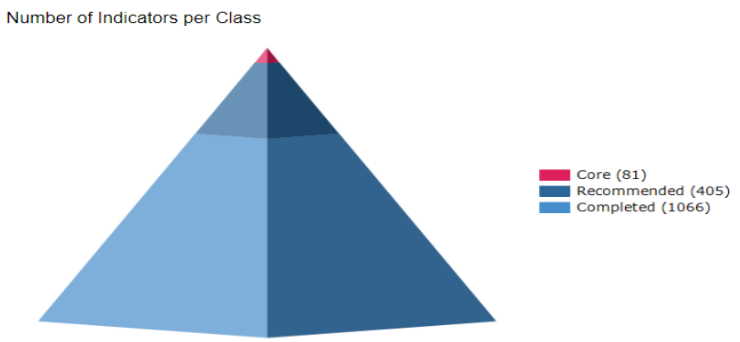
Indicators-based resilience assessment?

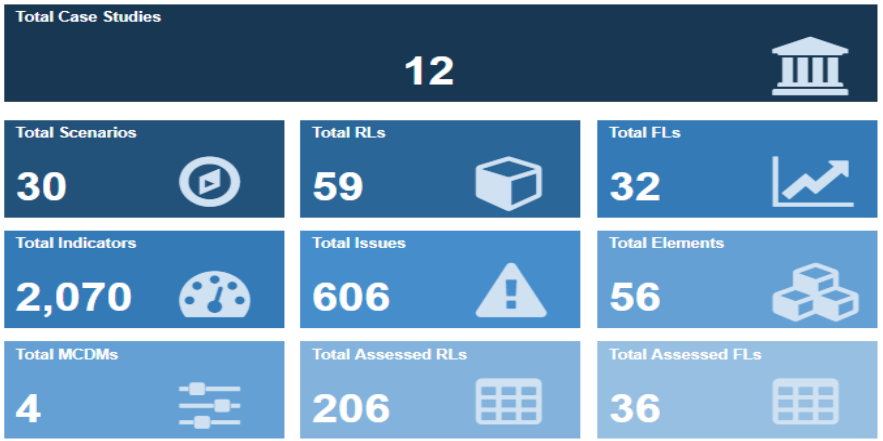
We need INDICATORS

Implementation

User dashboard







SMART RESILIENCE

Smart Resilience Indicators for Smart Critical Infrastructures

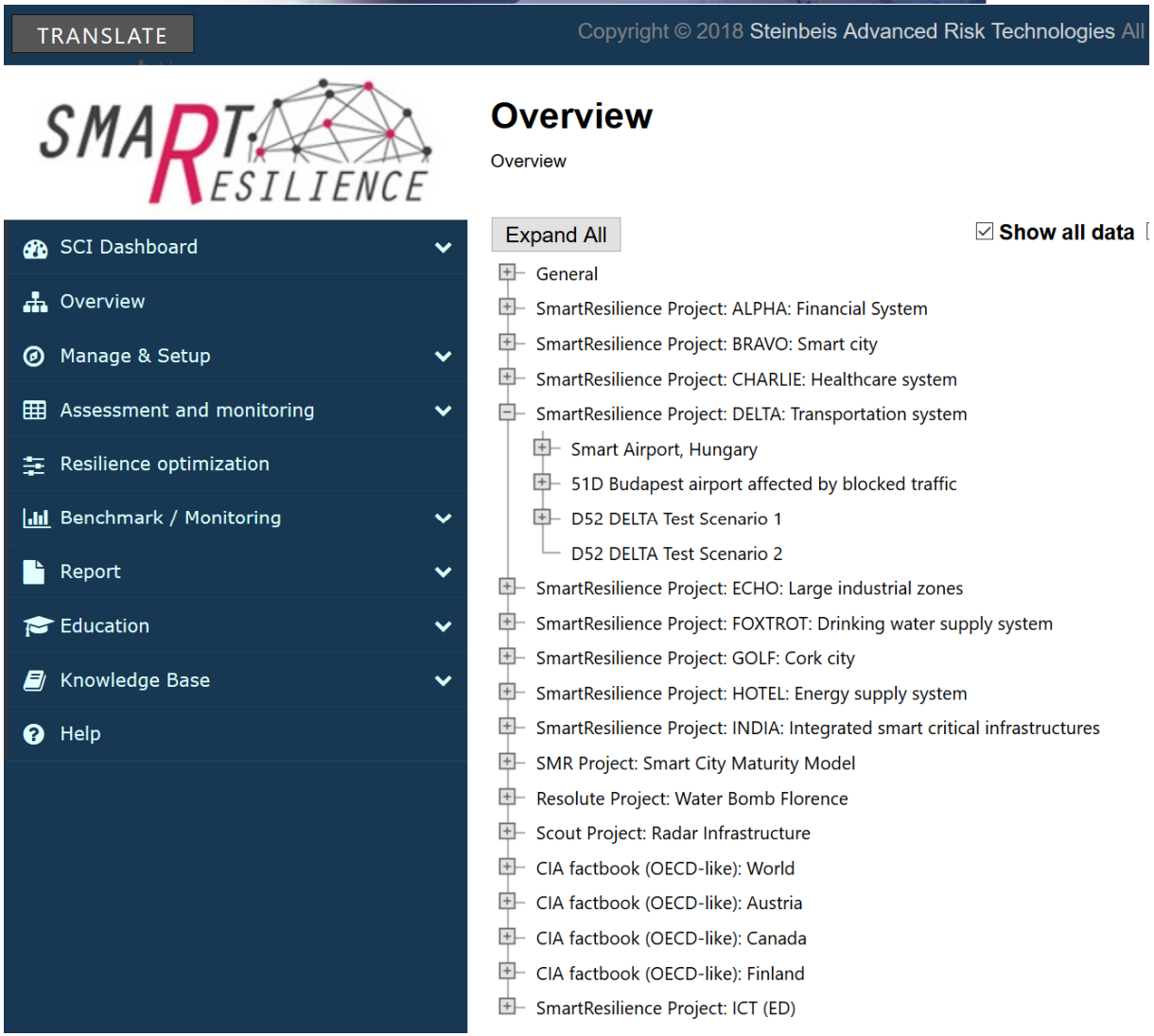
Indicators-based resilience assessment?

We need a SYSTEM

Smart Resilience Indicators for Smart Critical Infrastructures

SmartResilience:

System



"Infrastructure of Critical Infrastructures" (e.g. a Smart City)

Scenario: Infrastructure(s), Threat(s)

Analysis: Phases, Issues, Indicators

SMART RESILIENCE

OUTCOME OF A DISRUPTIVE EVENT? *Functionality level*

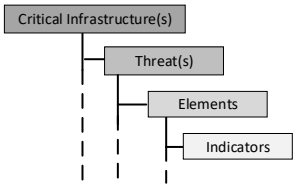
RESILIENCE OF AN INFRASTRUCTURE? *Resilience level*

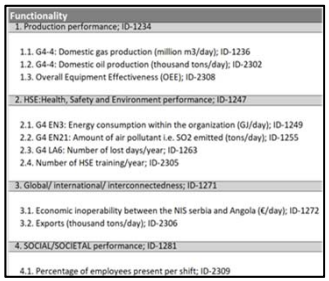
INFLUENCE OF INTERCONNECTEDNES? *Analysis of interdependencies*

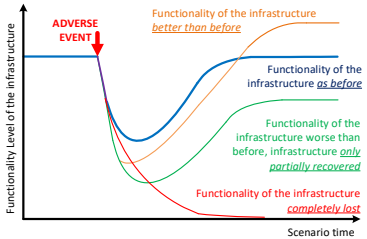
INVESTMENT IN RESILIENCE OPTIMIZATION? *Decision optimization*

TANGIBLE RESULTS / OUTPUTS

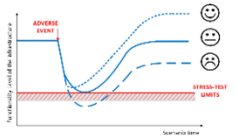
time$_{scenario}$



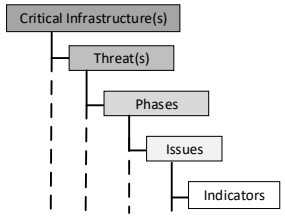


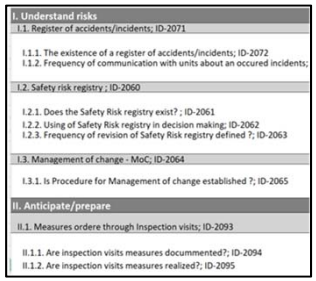


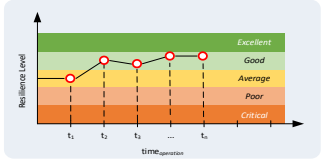
STRESS-TEST OK?



time$_{operation}$

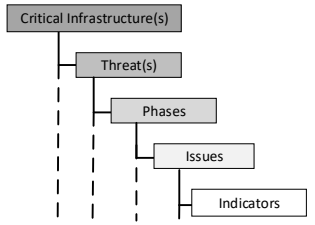


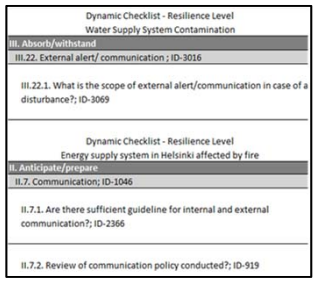




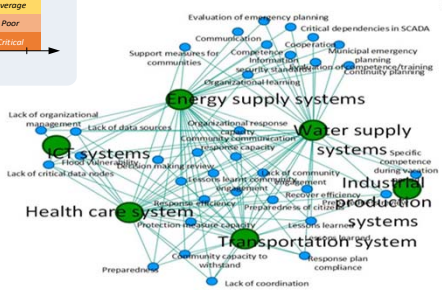
RESILIENCE LEVEL OK?

time$_{operation\ OR\ scenario}$

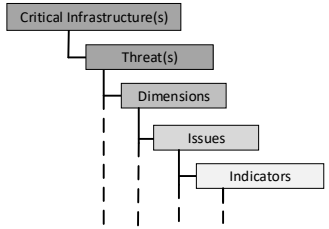


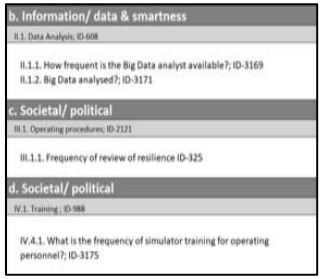


UNEXPECTED CASCADING EFFECTS?



time$_{operation\ OR\ implementation}$





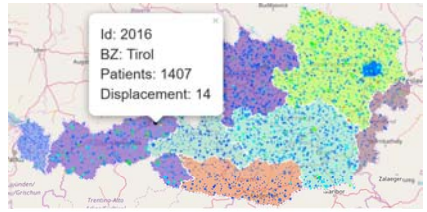
INVESTMENT IN RESILIENCE IMPROVEMENT OPTIMAL?

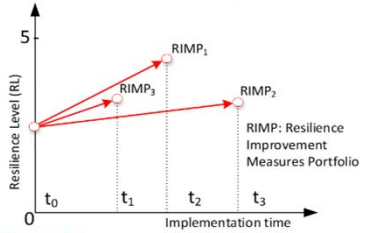
time$_{operation\ OR\ scenario}$

RESILIENCE ASSESSMENT OF A SINGLE INFRASTRUCTURE OR A CITY

Resilience Dimensions	Resilience (cycle) Phases	Understand risks	Anticipate / prepare	Absorb / withstand	Respond / recover	Adapt / transform
	System / physical	Average	Good	Average	Good	Excellent
	Information / smartness	Good	Average	Good	Good	Good
	Organization / business	Excellent	Excellent	Poor	Poor	Excellent
	Societal / political	Poor	Good	Excellent	Average	Excellent
	Cognitive / decision making	Critical	Excellent	Average	Good	Average

RESILIENCE ASSESSMENT OF A COUNTRY OR REGION

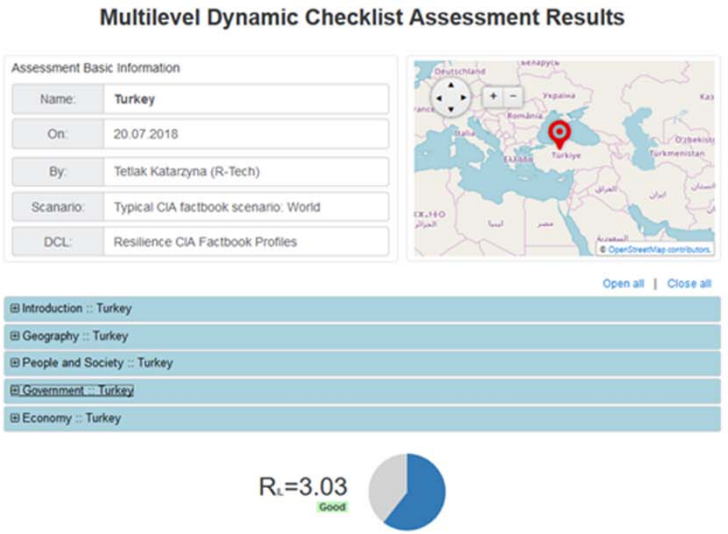


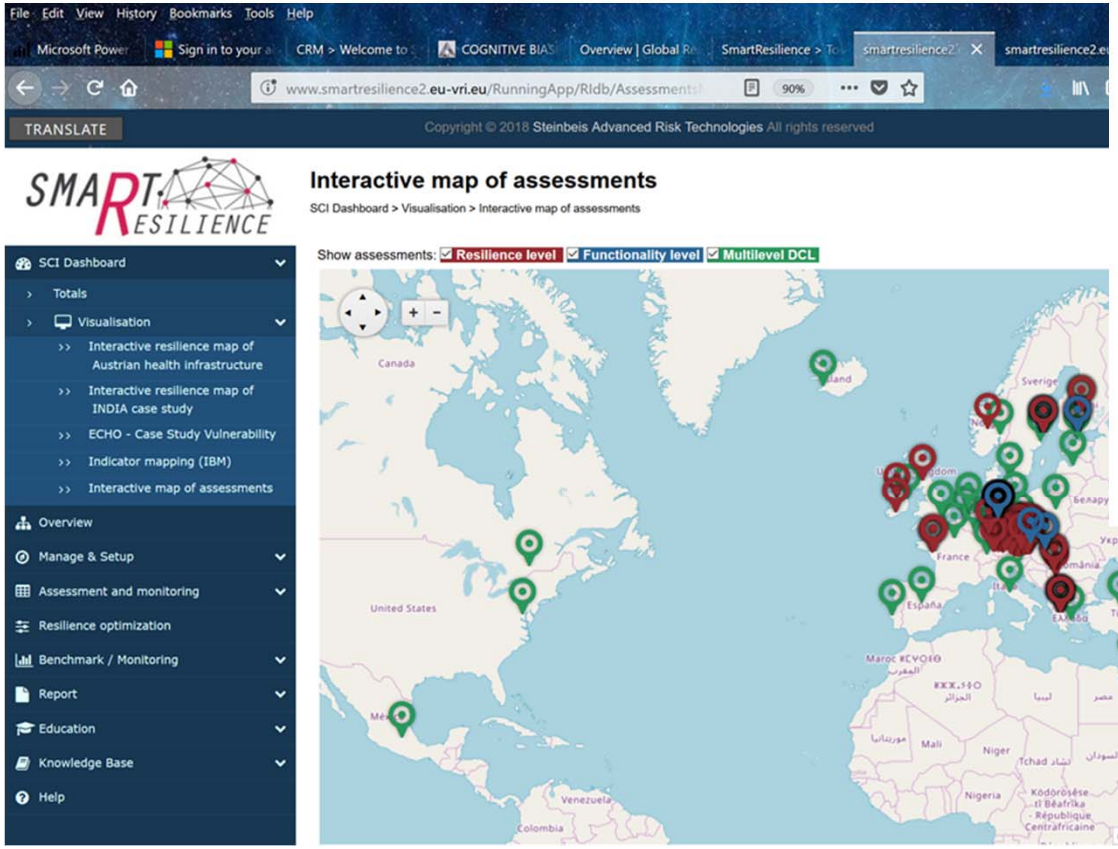


TOOL:

Case Studies, Scenarios, Dynamic Checklists (DCLs), Assessments

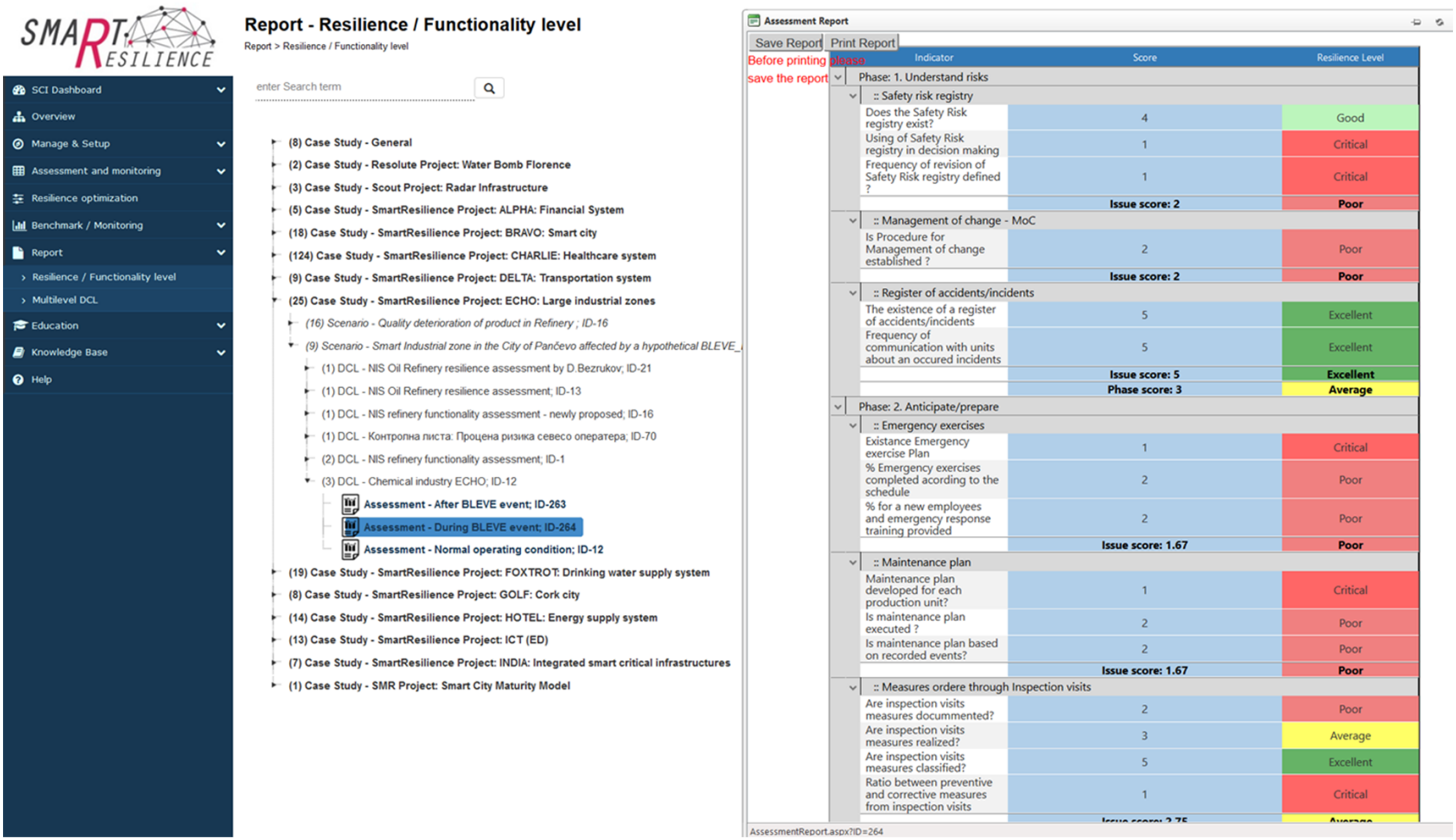
Country resilience



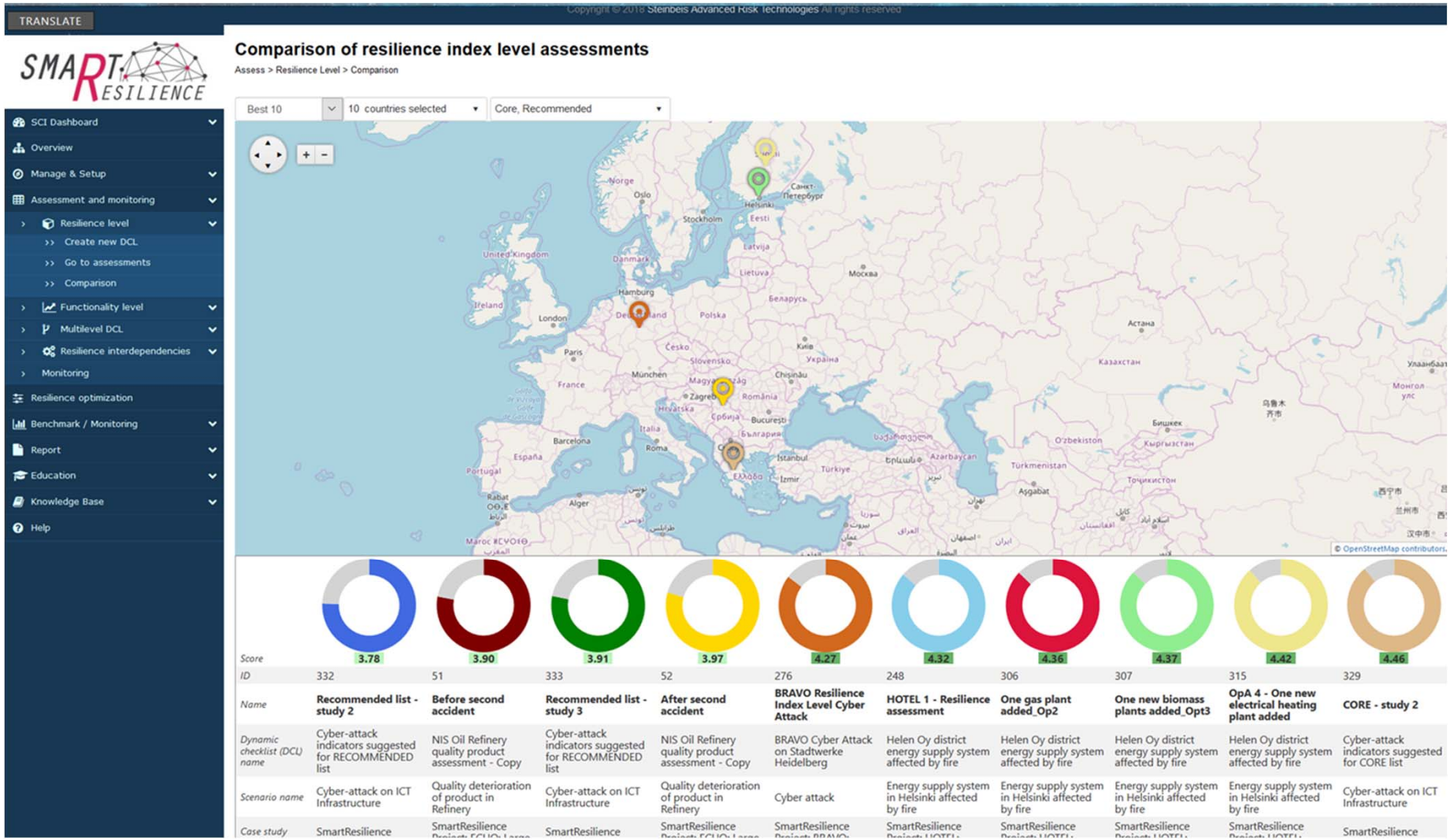


Name	Level	ID	Type	Score	Resilience Level
Turkey	0	1	Root	3.03	Good
1. Disaster impact	1	3752	Issue	4.06	Excellent
1.1. Average number of disasters per year (1980-2016)	2	3751	Indicator	3.78	Good
1.2. Average damages due to disasters (1980-2016)	2	3755	Indicator	4.63	Excellent
1.3. Average damages due to disasters as a percentage of GDP (1995-2015)	2	3756	Indicator	3.76	Good
2. Health Care	1	3757	Issue	1.02	Poor
2.1. Total hospital beds per 1000 population	2	3758	Indicator	1.02	Poor
3. ICT Technology	1	3779	Issue	2.97	Average
3.1. ICT Access and Usage by Households and Individuals	2	3783	Indicator	2.97	Average
4. Well-being	1	3781	Issue	2.74	Average
4.1. Life expectancy at birth	2	3801	Indicator	4.77	Excellent
4.2. Employees working very long hours	2	3802	Indicator	0	Critical
4.3. Self-evaluation of life satisfaction	2	3803	Indicator	3.45	Good
5. ENVIRONMENT	1	3782	Issue	3.06	Good
5.1. Air pollution, level of PM2.5	2	3804	Indicator	3.06	Good
6. Economy	1	3780	Issue	3.52	Good
6.1. Disposable household income per capita	2	3798	Indicator	2.81	Average
6.2. Employment rate	2	3799	Indicator	3.65	Good
6.3. Share of labour force with at least secondary education	2	3800	Indicator	4.09	Excellent
7. Sense of security	1	3810	Issue	3.88	Good
7.1. Feeling safe walking alone at night	2	3805	Indicator	3.02	Good
7.2. Homicide rate	2	3806	Indicator	4.74	Excellent
8. Civic engagement	1	3809	Issue	2.96	Average
8.1. Stakeholder engagement for developing regulations	2	3807	Indicator	2.62	Average

Critical infrastructure resilience

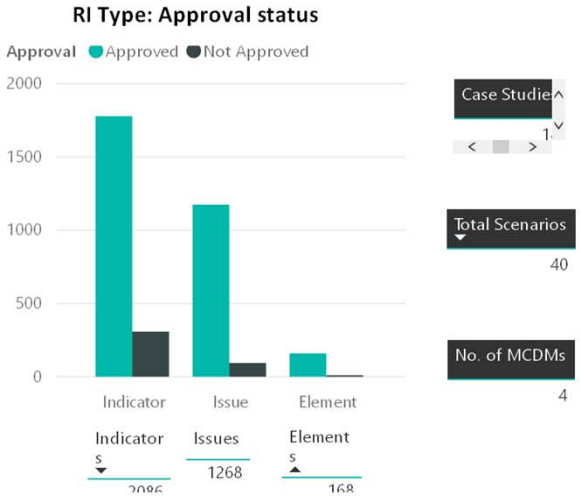


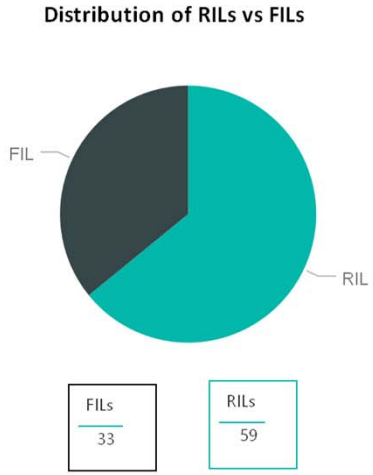
Critical infrastructure resilience

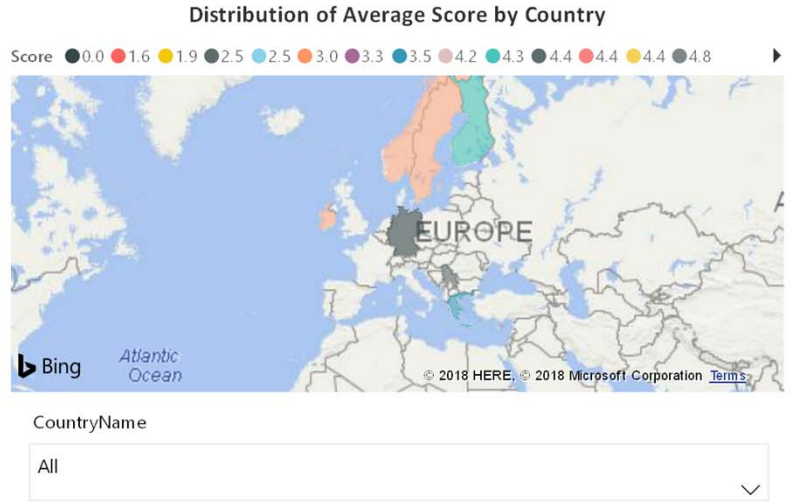


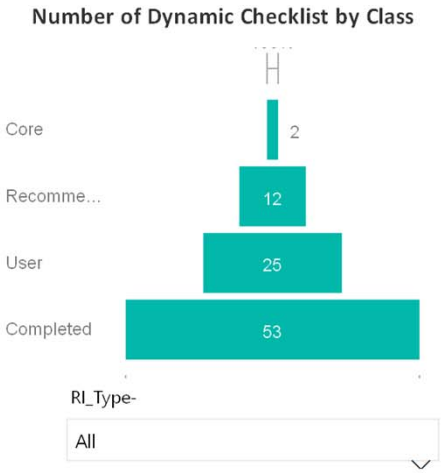
Score	3.78	3.90	3.91	3.97	4.27	4.32	4.36	4.37	4.42	4.46
ID	332	51	333	52	276	248	306	307	315	329
Name	**Recommended list - study 2**	**Before second accident**	**Recommended list - study 3**	**After second accident**	**BRAVO Resilience Index Level Cyber Attack**	**HOTEL 1 - Resilience assessment**	**One gas plant added_Op2**	**One new biomass plants added_Opt3**	**OpA 4 - One new electrical heating plant added**	**CORE - study 2**
Dynamic checklist (DCL) name	Cyber-attack indicators suggested for RECOMMENDED list	NIS Oil Refinery quality product assessment - Copy	Cyber-attack indicators suggested for RECOMMENDED list	NIS Oil Refinery quality product assessment - Copy	BRAVO Cyber Attack on Stadtwerke Heidelberg	Helen Oy district energy supply system affected by fire	Helen Oy district energy supply system affected by fire	Helen Oy district energy supply system affected by fire	Helen Oy district energy supply system affected by fire	Cyber-attack indicators suggested for CORE list
Scenario name	Cyber-attack on ICT Infrastructure	Quality deterioration of product in Refinery	Cyber-attack on ICT Infrastructure	Quality deterioration of product in Refinery	Cyber attack	Energy supply system in Helsinki affected by fire	Energy supply system in Helsinki affected by fire	Energy supply system in Helsinki affected by fire	Energy supply system in Helsinki affected by fire	Cyber-attack on ICT Infrastructure
Case study	SmartResilience	SmartResilience	SmartResilience	SmartResilience	SmartResilience	SmartResilience	SmartResilience	SmartResilience	SmartResilience	SmartResilience

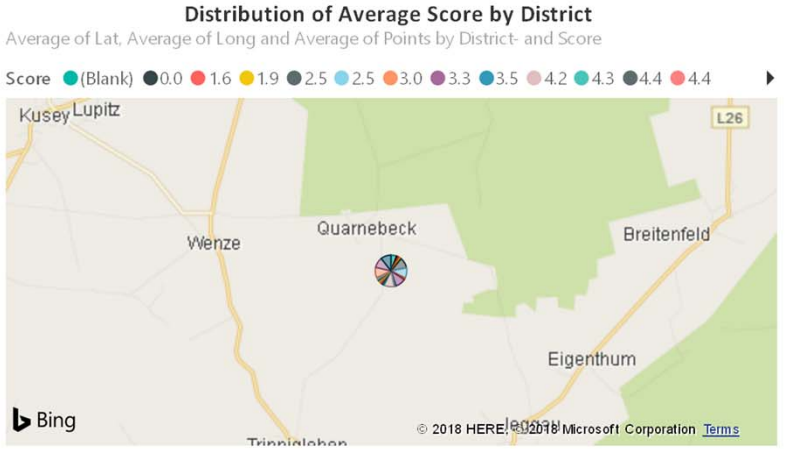
How to manage 2,000 indicators?
Resilience intelligence (based on BI)











Last update on: 14 September 2…

Last entry on

RESILIENCE ASSESSMENT EXERCISE REPORT

The template is proposed in the EU funded project: SmartResilience (the Grant Agreement No. 700621)
http://smartresilience.eu-vri.eu/

Infrastructure assessed:
Scenario name & ID:
DCL name & ID:
Assessment name & ID:
Date:

Executive summary of the exercise:

Historical data/ situational reporting of the similar events (real or simulated):
Main objectives and challenges of the exercise:
Description of the conducted exercise:
⚠ *Expected length of this section is the following:* *½ page in case of discussion-based exercises (seminar, workshop, table-top or game)* *1 page in case of operation-based exercises (drill, functional exercise or full-scale exercise)*
Measurements:
Main findings after the exercise:
⚠ *Can be copied from section: 1.5 Results*

Part A: Basic info

I.	Resilience assessment/stress-test team[1] member's information: Requestor		
I.1	Requestor's initials & last name[2]:	I.2 Requestor's organization:	I.3 Requestor's position:
I.4	Requestor's phone number:	I.5 Requestor's email address:	

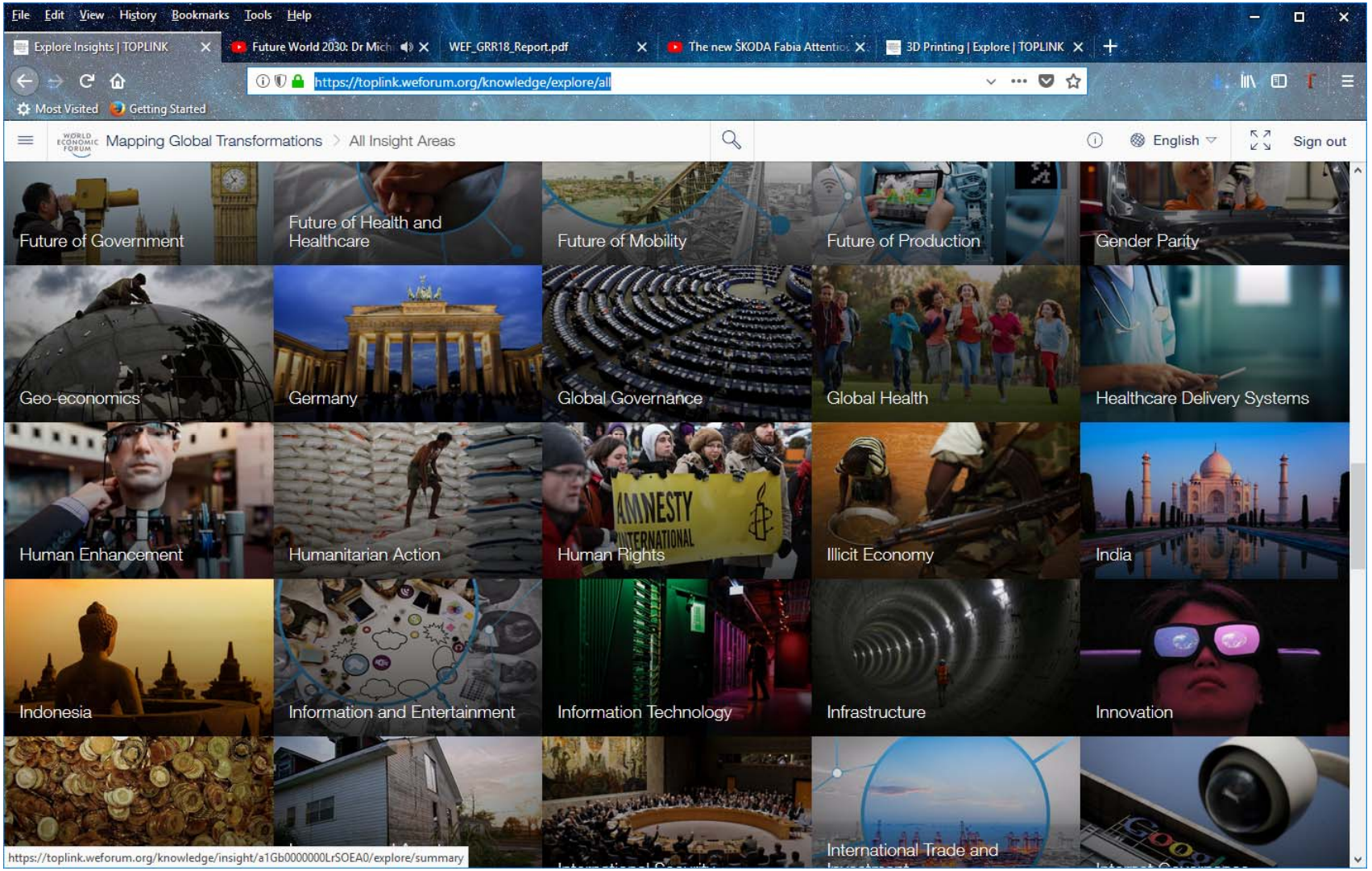
[1] The Resilience Assessment Exercise structure is shown on the Figure 2 (see: below).
[2] The requestor can be EC/local authorities/company authorities/individual person.

SMART RESILIENCE

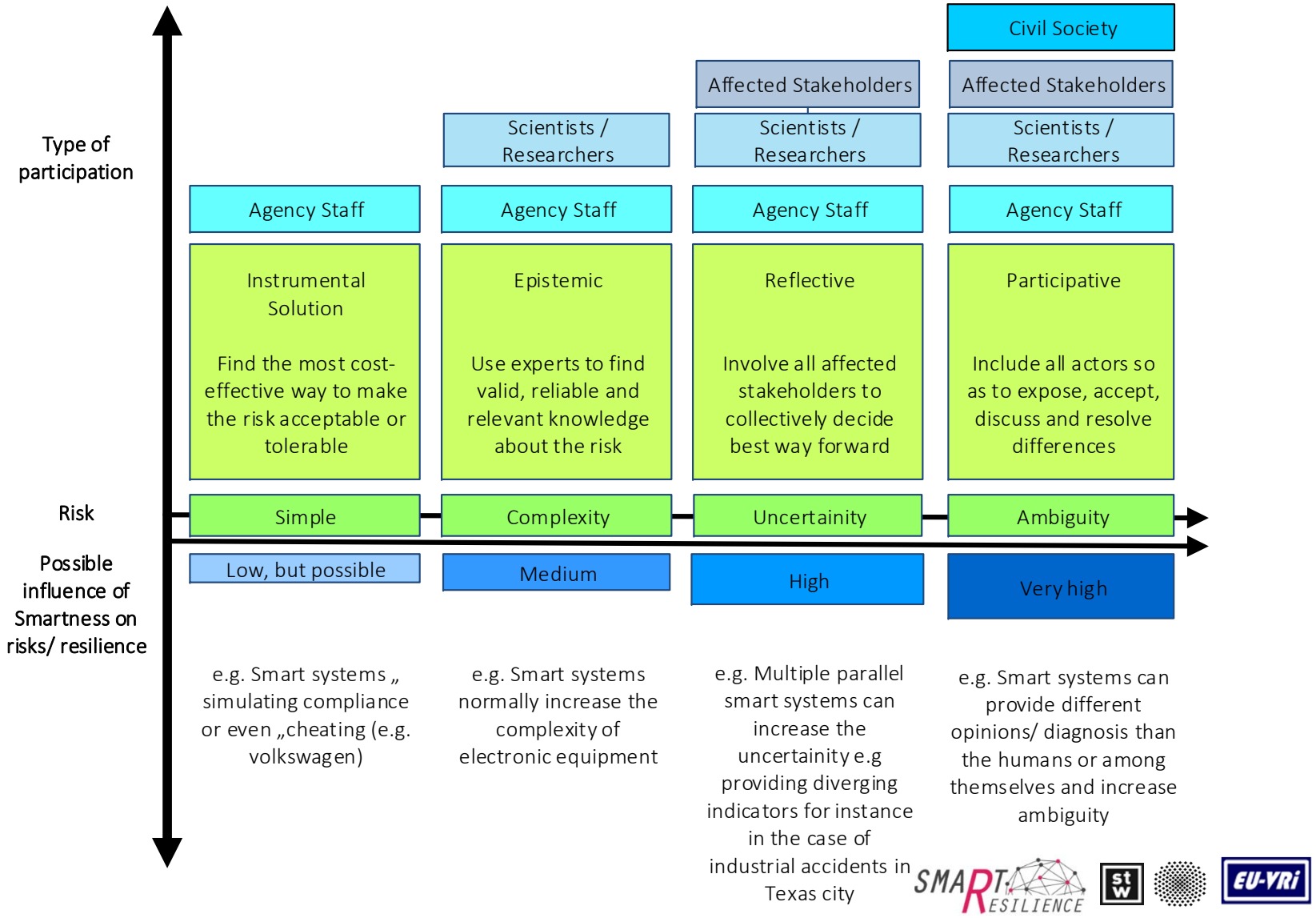
Smart Resilience Indicators for Smart Critical Infrastructures

Conclusions

Problem #1:
The world is (very) complex ☹…



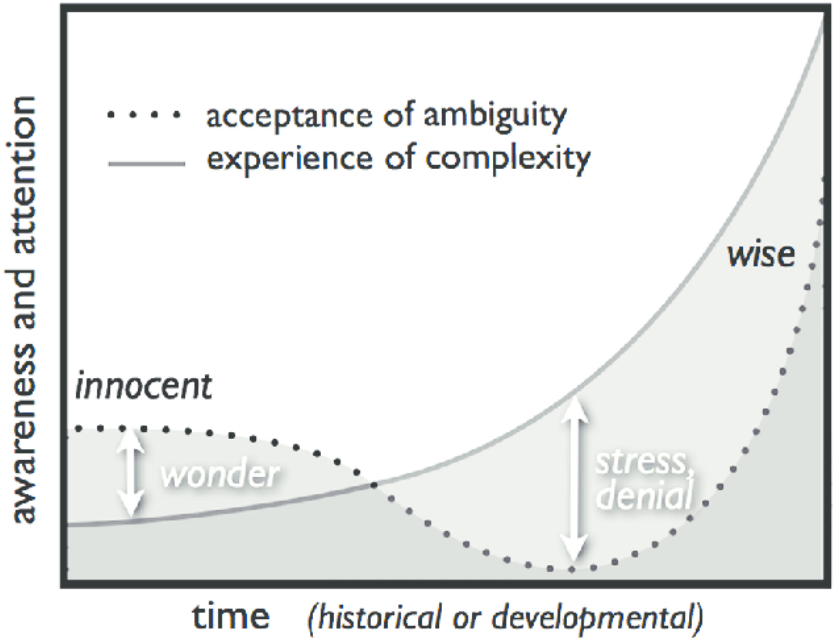
Problem #2:
Our institutions!

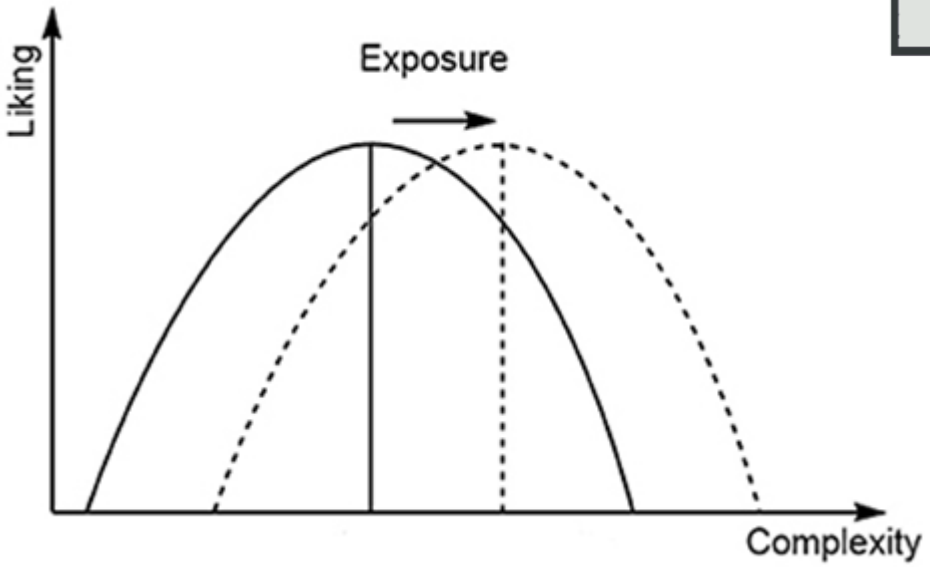


Problem #3:
We think and act in silos!

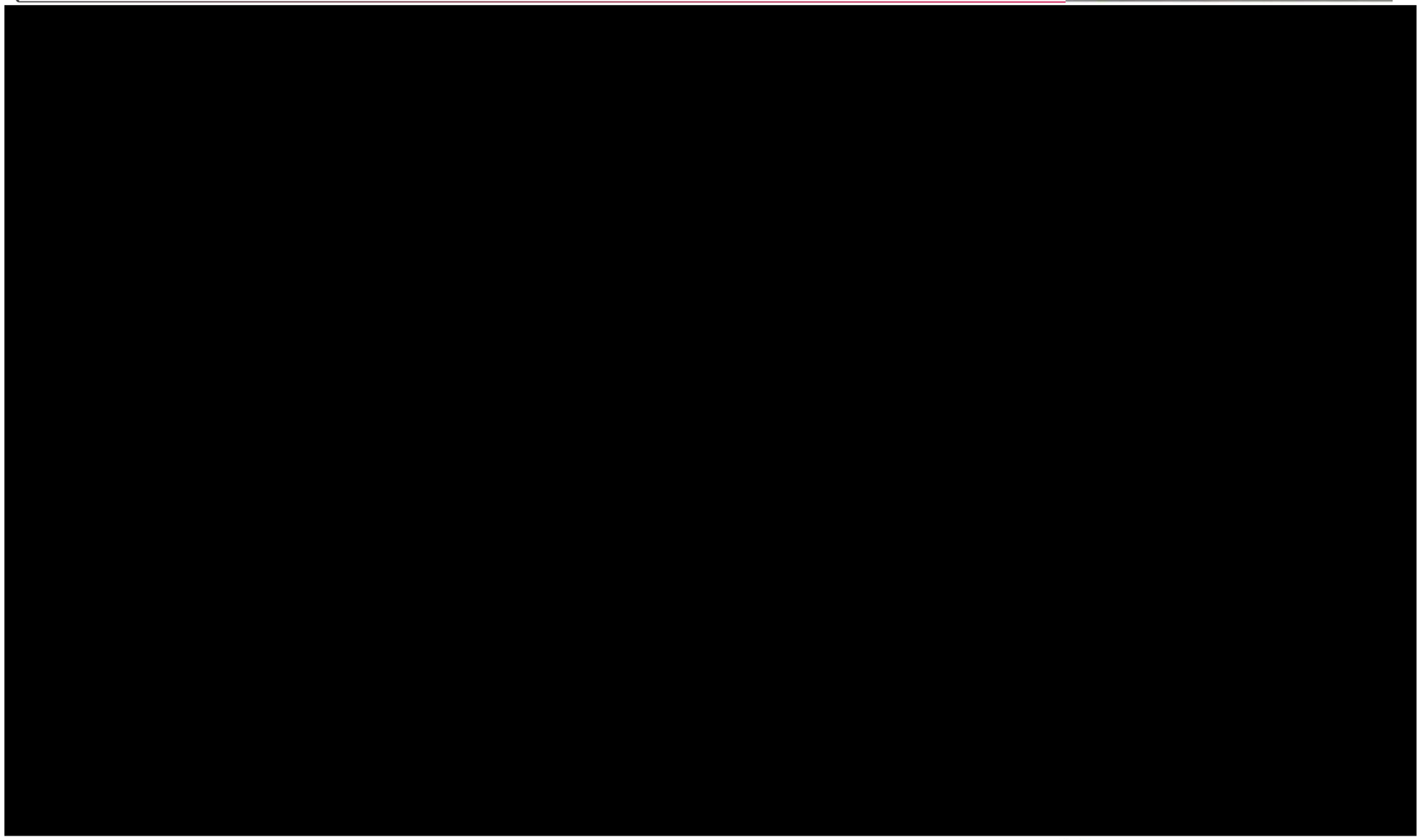
- Interdependent infrastructures!
  … often analyzed independently!!!

Problem #4:
The world is (very) complex ☹… and we do not like it!





Problem #5:
We are bad at seeing unexpected things!



Further research and applications

New technologies (also soft ones!):

- Open intelligent systems of n^{th} generation
- Smart/interactive/intuitive/3D/serious-gaming-based education
- Full-scale exploitation of big/open data (self-feeding systems!)

New direct applications for real outreach:

- Resilience mapping
- GRI-like resilience (voluntary) bottom-up reporting (**European Risk and Resilience Assessment & Rating Agency ?**)
- Global alignment/agreement (**ISO 31050!**)

SMART RESILIENCE

Smart Resilience Indicators f
Critical Infrastructures

Challenge(s)? Emerging risks!

ISO 31000 https://www.iso.org/iso-31000-risk-management.html
TC262 Risk Management – WG8 https://www.iso.org/committee/629121.html

ISO 31050

Guidance for Managing Emerging Risks to Enhance Resilience: Thriving in a World Growing in Uncertainty

"Emerging" risks are emerging daily... Example: Foreign Affairs June 2018

(on June 12, 2018, ISO voted for 31050!)

Why ISO 31050?

At the current pace of change, the world in the 21st century will experience 20,000 years of advancements, in just one 100 years (WEF, 2016). This is changing the risk landscape and bringing in an avalanche of new uncertainties and new emerging risks the management of which is essential for the society.

The new ISO 31050 standard will provide the much needed foresight and insight to deal with these risks. It will also provide new ways for enhancement of organizational resilience and new capabilities to deal with new challenges, helping, at the same time, to increase the level of trust in management of risk.

ISO 31000:2018 as a "generic standard"

The newly revised and published International Standard on Risk Management ISO 31000:2018 is created, monitored and supplemented (with supporting documents) by ISO Technical Committee TC262.
ISO 31000 standard is one of the few ISO Standards (of the several thousand promulgated by top experts in their fields) that is qualified as a "generic ISO standard" – this means that all other standards must accommodate and align to its provisions.

Therefore, it is mission critical for every entity utilizing ISO Standards, to address and strategically approach risk management and, when doing so, to follow ISO 31000.

New ("emerging") risks

ISO 31050:
A new member of ISO 31000 family

Starting from the ISO 31000 definition of risk ("effect of uncertainty on objectives") and understanding risk management as significant contributor to value creation and preservation, the new

"ISO 31050 Guidance for Managing Emerging Risks to Enhance Resilience"

will contribute to the further development of integrated management processes that provide insight into how risk may affect the achievement of organization objectives. The development of the standard is assigned to the Work Group 8 (WG8) of the Technical Committee TC262. The work started in June 2018, taking DIN SPEC 91299 (CWA 1664), the work of the ISO TC292 (ISO 223xx standards) and the works of organizations such as OECD, SRA, WEF and EU (projects iNTeg-Risk and SmartResilience project, ResiStand) as its main reference.

The main calling is to provide universal, yet meaningful guidance on developing new competencies and business models to create relevant and realistic recommendations in an ever-changing uncertain world, to facilitate best practices, enhance resilience, promote agility, assist transformation, deliver insight, insure foresight, establish value and integrate resources.

With ISO 31050, the decision makers in organizations will be better equipped to manage both known (ISO 31000) and emerging risks (ISO 31050) with confidence. To this aim, ISO 31050 will, deliver:

Final conclusion:
INTEGRATE & ALIGN resources GLOBALLY!

(IIC-like) TESTBED

Technology: ledger-technology (BlockChain)

A European AGENCY, Assessment-as-a-Service

Organization: a network of approved assessors/auditors (companies)

ERRA RISK & RESILIENCE RATING AGENCY

DYNAMIC RISK & RESILIENCE ASSESSMENT

Methodology & tools: The dynamic checklists, risk and resilience indicator based methodology and the open www-tool from the EU project SmartResilience