



Evaluating Critical Infrastructure Resilience: proposed Methodology and Guidelines

Sandro Bologna

AIIC Working Group on Critical Infrastructure Resilience

s.bologna@infrastrutturecritiche.it

ERNCIP-IMPROVER

Operators Workshop

27-28 April 2016, Ispra

Sandro Bologna

- ❖ Graduated in Physics at Rome University
- ❖ 35+ years experience at the Italian National Agency for New Technologies, Energy and Sustainable Economic Development in the position of Head of Research and Project Manager in the field of Safety and Security of Computer Based Industrial Control Systems and Critical Infrastructures Protection
- ❖ Past President of the Italian Association of Critical Infrastructure Experts and current Board Member
- ❖ Independent researcher and expert in the participation to National and International Research Projects in the fields of Critical Infrastructures Protection, Cyber Security and Resilience

Adopted Infrastructure Resilience definition

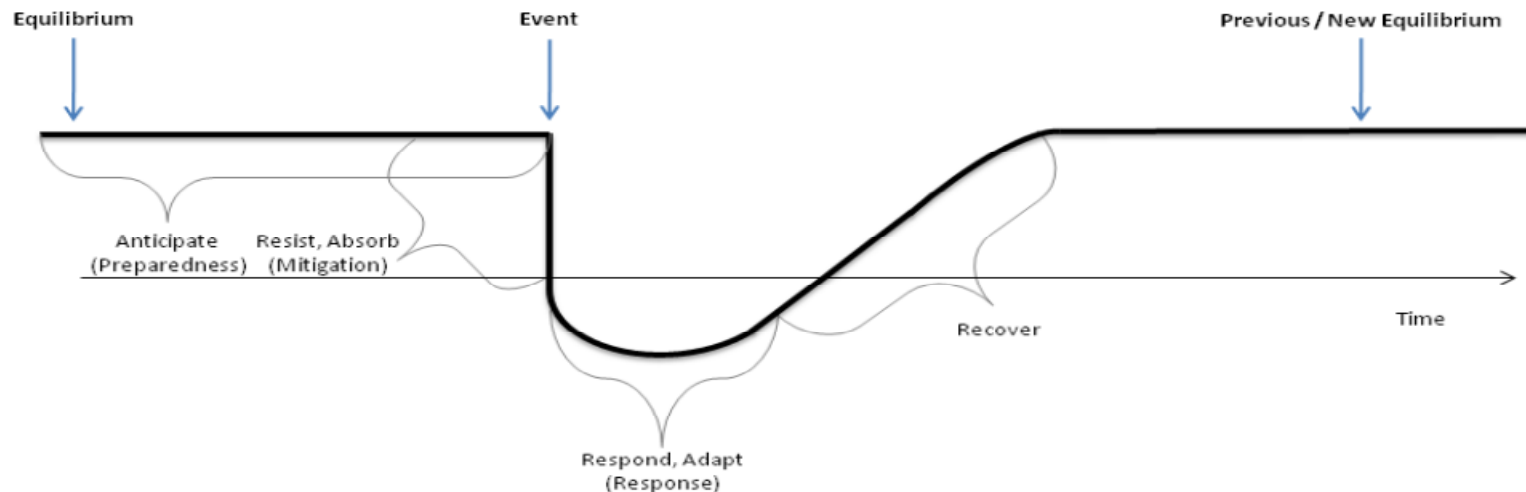
*“**Infrastructure resilience** is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event.”*

*(NIAC 2009 Critical Infrastructure Resilience:
Final Report and Recommendations)*

http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf

Graphical Representation of Resilience

- A negative event occurs (i.e. a threat exploits the vulnerability of a given component)
- The system detects the occurrence of negative event
- The system reacts to the negative event and tries to recover its state

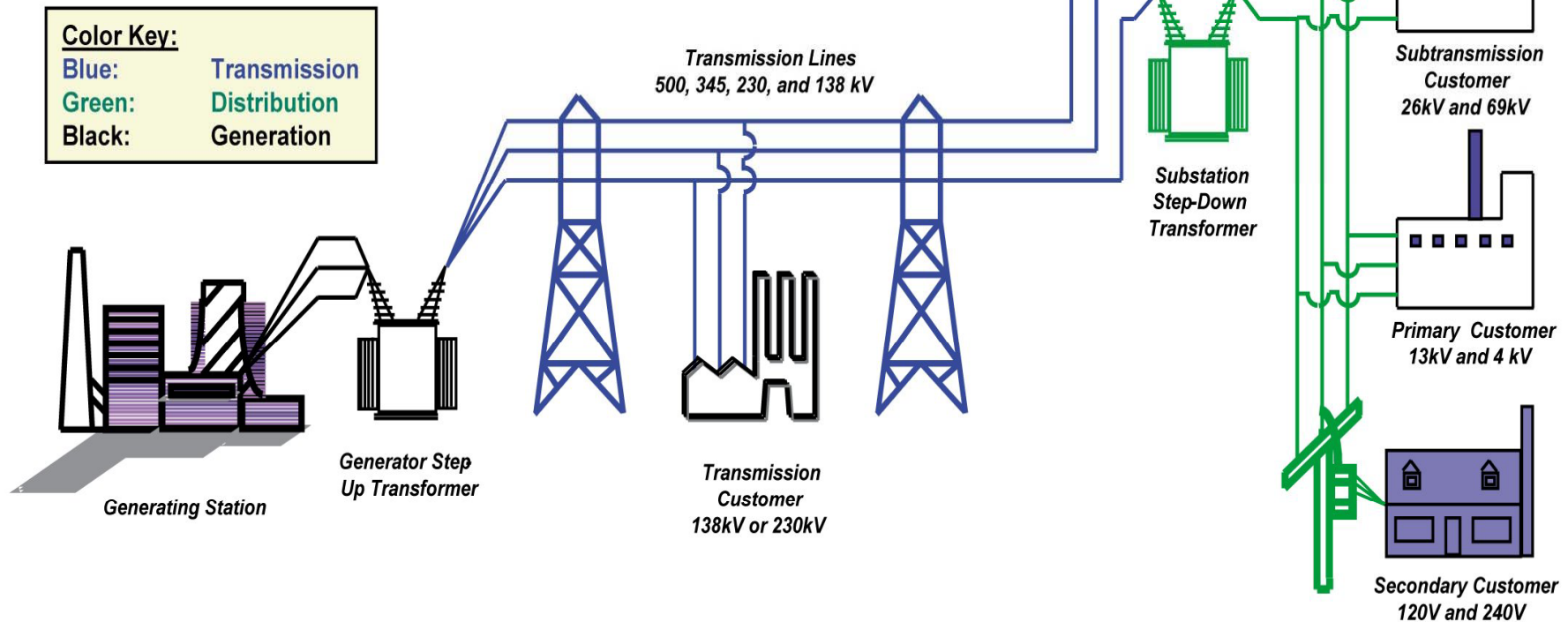


Source: ANL/DIS-12-1 Resilience: Theory and Applications



Resilience: a Multifaceted Problem

Basic Structure of the Electric System



Question: Resilience of what, to what and for whom?

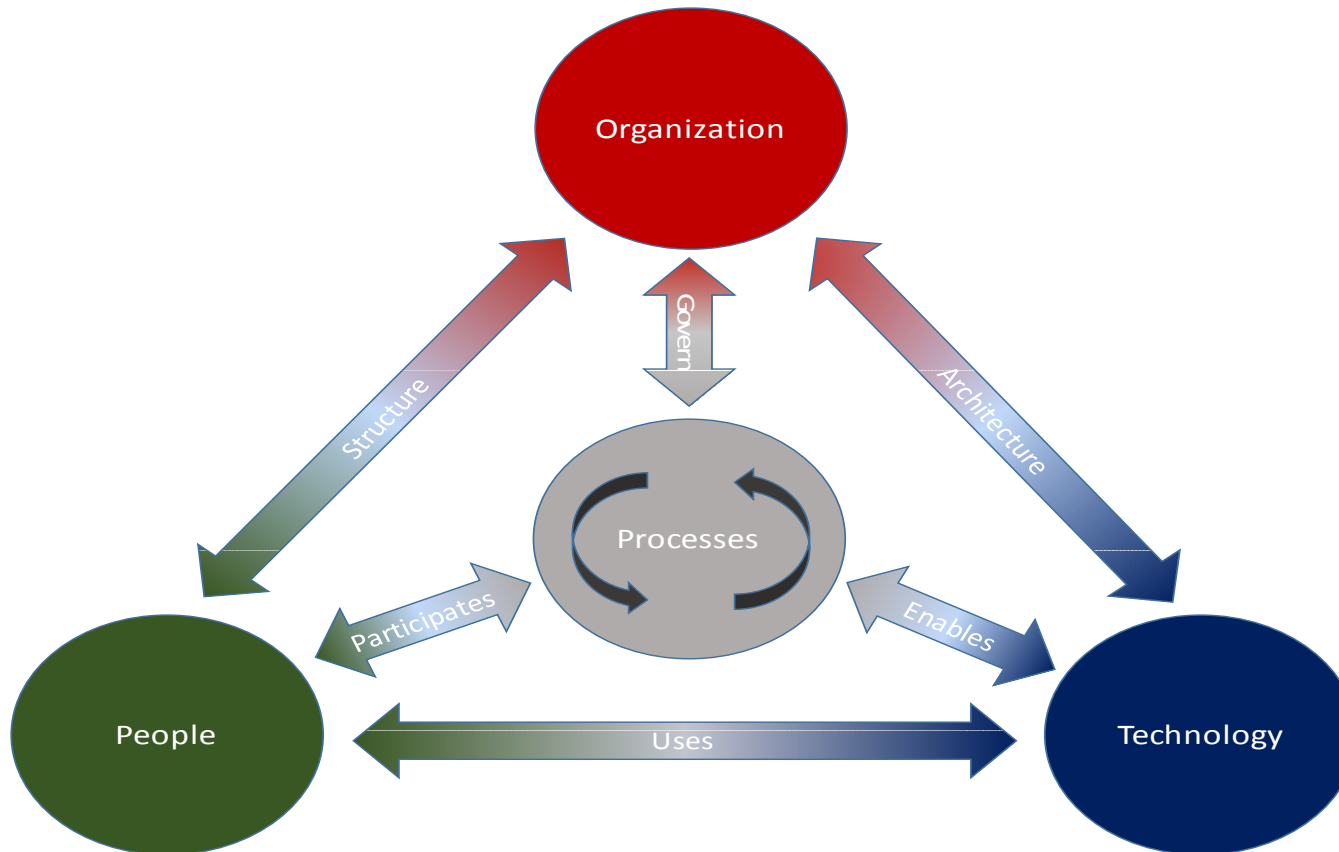
To assess a system's resilience, one must specify which system configuration and which disturbances are of interest



Question: Resilience of what, to what and for whom?

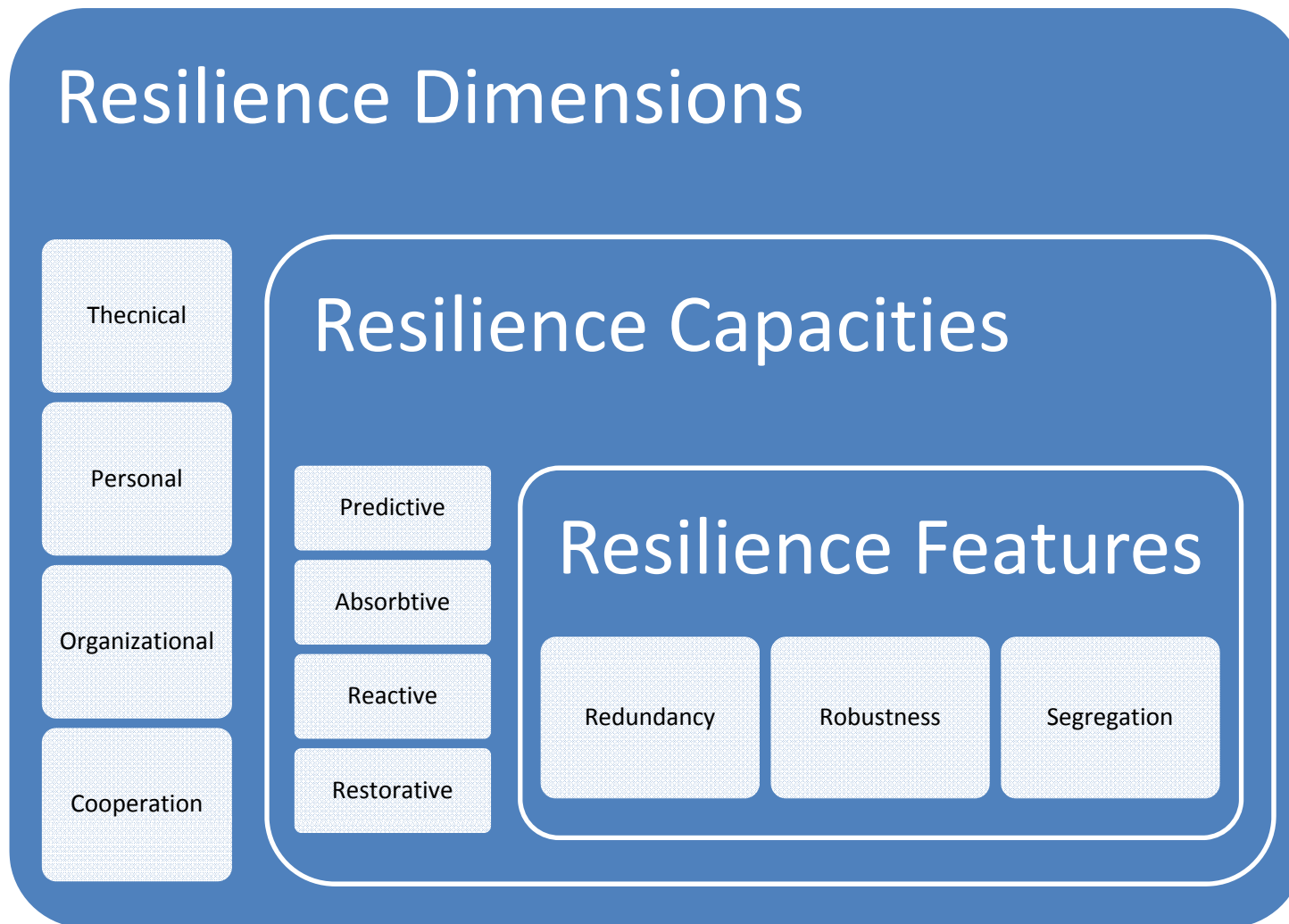
To assess a system's resilience, one must specify which system configuration and which disturbances are of interest

A Critical Infrastructure is not only made of technologies but especially of people, processes and organizations. Resilience must take in consideration all these components, plus cultural background, to be complete and successful.



**Source: Adapted from the USC Marshall School of Business
Institute for Critical Information Infrastructure Protection**

Resilience Dimensions



Hierarchical Representation of the Infrastructure Resilience Model

Four Dimensions of Resilience

Cooperative Resilience



Organizational Resilience



Personal Resilience



Technical (Logical & Physical) Resilience

PLC

RTU

CCTV

LAN

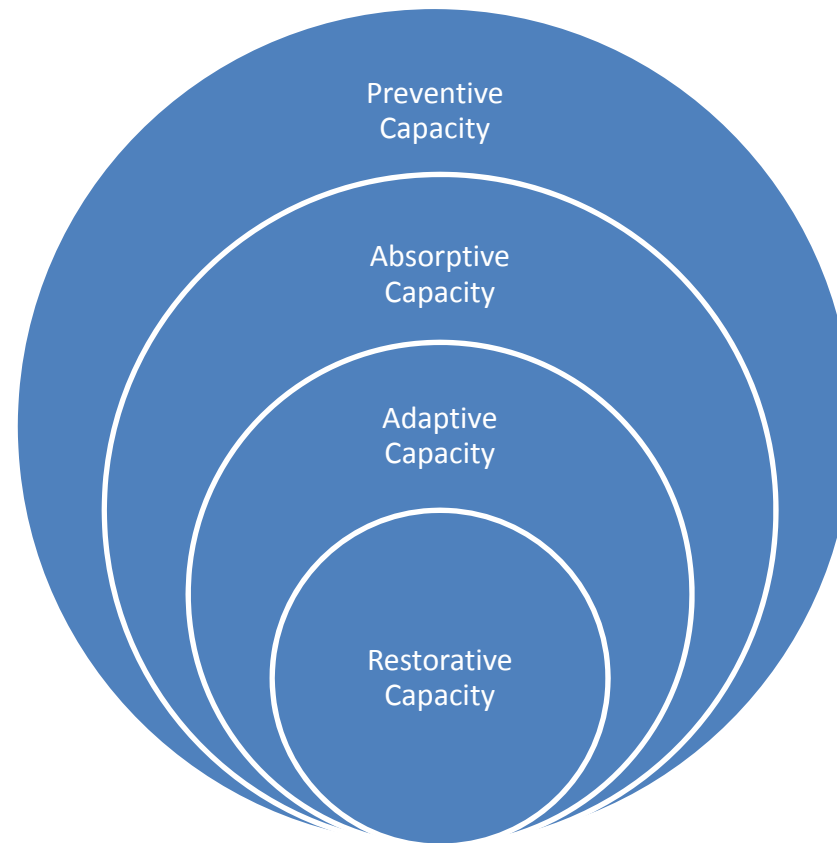
SCADA

TOUCH ID

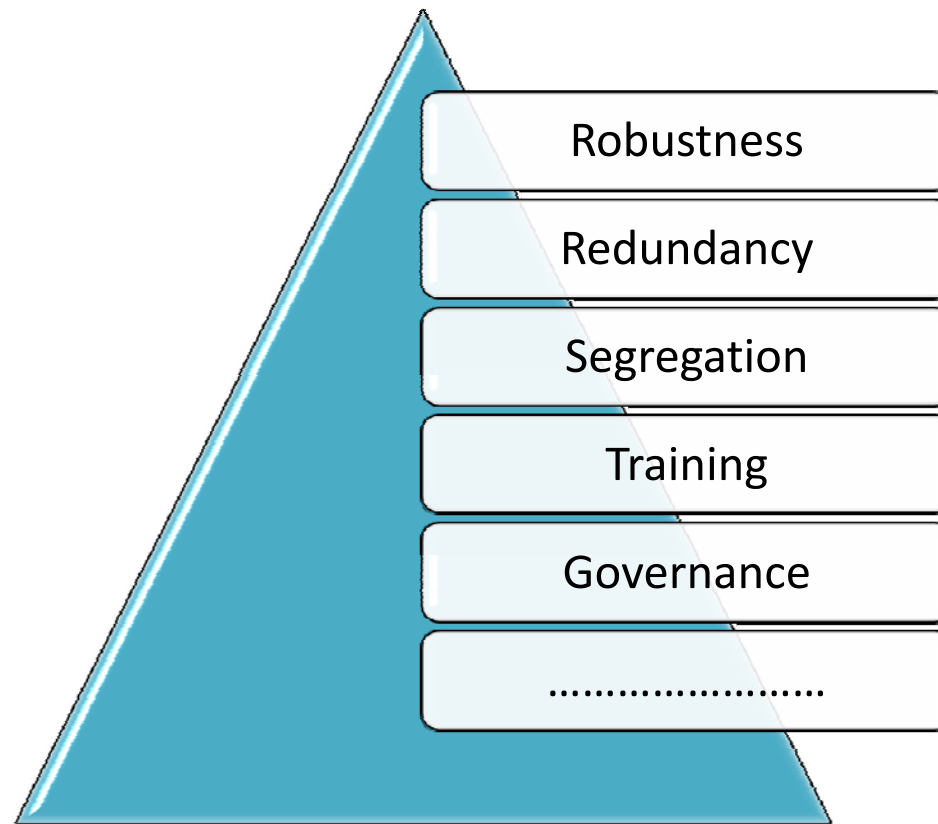
BIOMETRIC ID

DATABASE

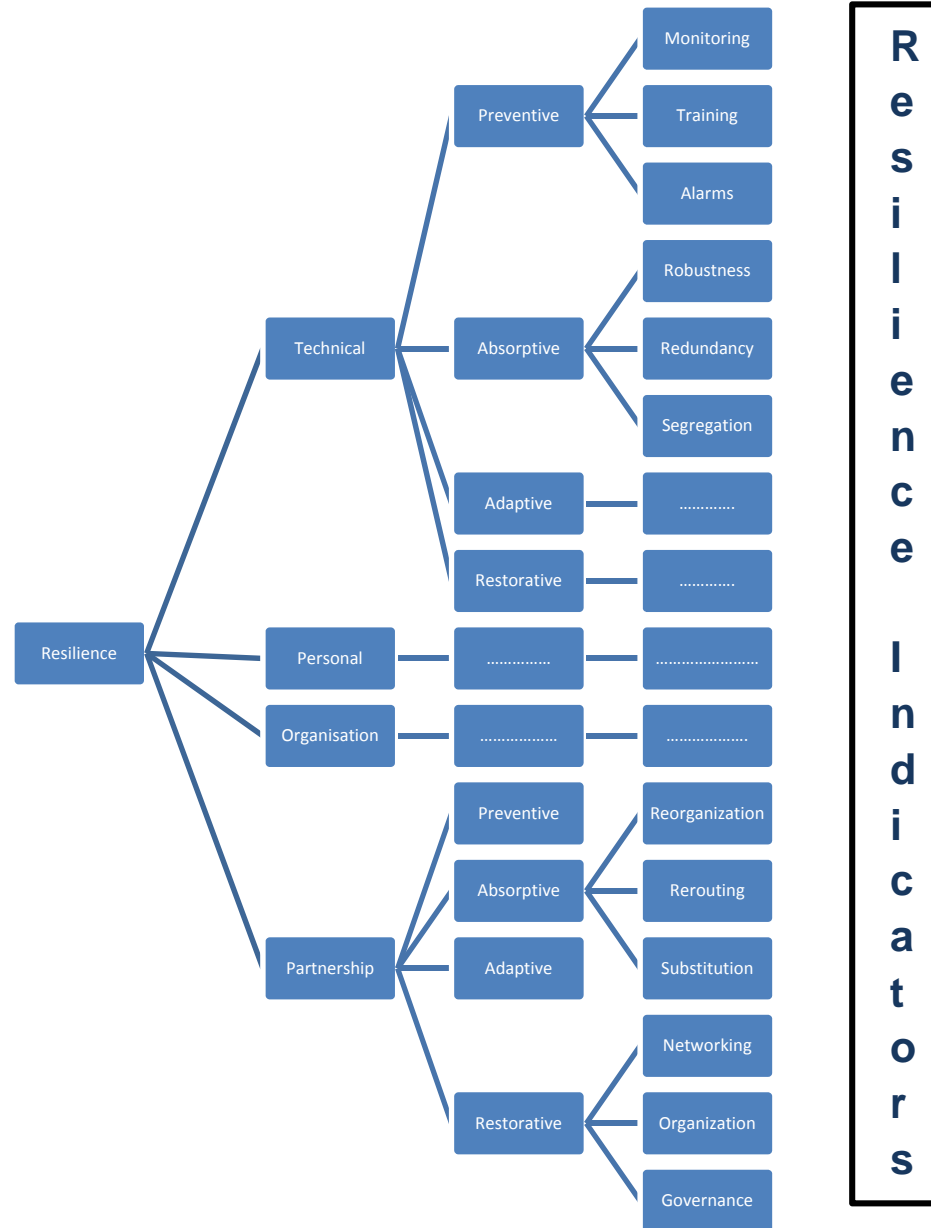
In building and evaluating resilience the contribution made by each of these four dimensions needs to be considered



System resilience capacities that contribute to the ability of a system to prevent, absorb, adapt to, and/or rapidly recover from a potentially disruptive event



**System features (capabilities) that may contribute to the system resilience:
in building and evaluating resilience the contribution made by each of these
Features (capabilities) needs to be considered and evaluated**



Resilience Tree representing the resilience components that contribute to the system resilience

Resilience Indicator NAME	
Description	Description of the specific Resilience Indicator of the component subject to assessment
Sub-system/system Dimension/capacity	To which sub-system/system and dimension/capacity it applies: component/feature subject to assessment
Sector Applicability Relevance	Relevance for the specific CI sector under evaluation
Evaluation method(s)	Method used for ranking the specific resilience indicator
Sources / References	For more details and information

Template for Resilience Indicators Description

Lo3 - DATABASE SCANNING	
Description	Database Scanners are a specialized tool used specifically to identify vulnerabilities in database applications. In addition to performing some external functions like password cracking, the tools also examine the internal configuration of the database for possible exploitable vulnerabilities.
Dimension(s)	Technical logical
Sector Applicability Relevance	Very important for CI sectors with large DB, e.g. financial sector
Evaluation method(s)	Database vulnerabilities
Sources / References	http://samate.nist.gov/index.php/Database Scanning Tools.html http://www.mcafee.com/us/products/security-scanner-for-databases.aspx

Example for Resilience Indicator description for Technical-Logical dimension

2015 Italian Cyber Security Report

Un Framework Nazionale per
la Cyber Security

Roberto Baldoni
@robertobaldoni

CYBER INTELLIGENCE
AND INFORMATION
SECURITY CENTER



SAPIENZA
UNIVERSITÀ DI ROMA



cini

Cyber Security National Lab

Ph4 - PERIMETER OR LOCATION SURVEILLANCE SYSTEMS	
Description	The latest generation of computer vision technology is revolutionizing concepts, applications, and products in video surveillance and CCTV. This is of prime relevance to security for large outdoor facilities such as commercial airfields, refineries, power plants, and office/industrial campuses. Most airfields, for example, have open (unfenced) perimeters, high volume heterogeneous traffic, are easily accessed on foot or by water, and exist in areas where regulations providing a safety buffer are difficult to legislate or enforce. And all airfields require 24x7 outdoor monitoring – snow, fog, rain or shine. Likewise, most high-value facilities appealing to criminals and terrorists are in close proximity to public areas (roads, residences, city, etc.).
Dimensions	Technical physical
Sector Applicability Relevance	To be estimated by the sector specific experts
Evaluation methods	Degree of implementation
Sources/References	http://www.sitepitalia.it/products/security/surveillance-and-perimeter-monitoring-system http://www.objectvideo.com/rad-services/publications.html

Example for Resilience Indicator description for Technical-Physical dimension

PE1 - Employees are trained and made aware of resilience requirements	
Description	Employees receive standard training and, further to that, are introduced to the basic concepts of resilience.
Dimensions	Personal and organizational
Sector Applicability Relevance	To be estimated by the sector specific experts . Human Resources Department should have a significant role in this evaluation
Evaluation methods	Presence/absence
Sources / References	M. Mullen <i>"On Total Force Fitness in War and Peace"</i> – MILITARY MEDECINE, 175, 8:1, 2010 Carlin Leslie, Air Force Public Affairs Agency OL-P <i>"Comprehensive Airman Fitness: A Lifestyle and Culture"</i> , August 19, 2014.

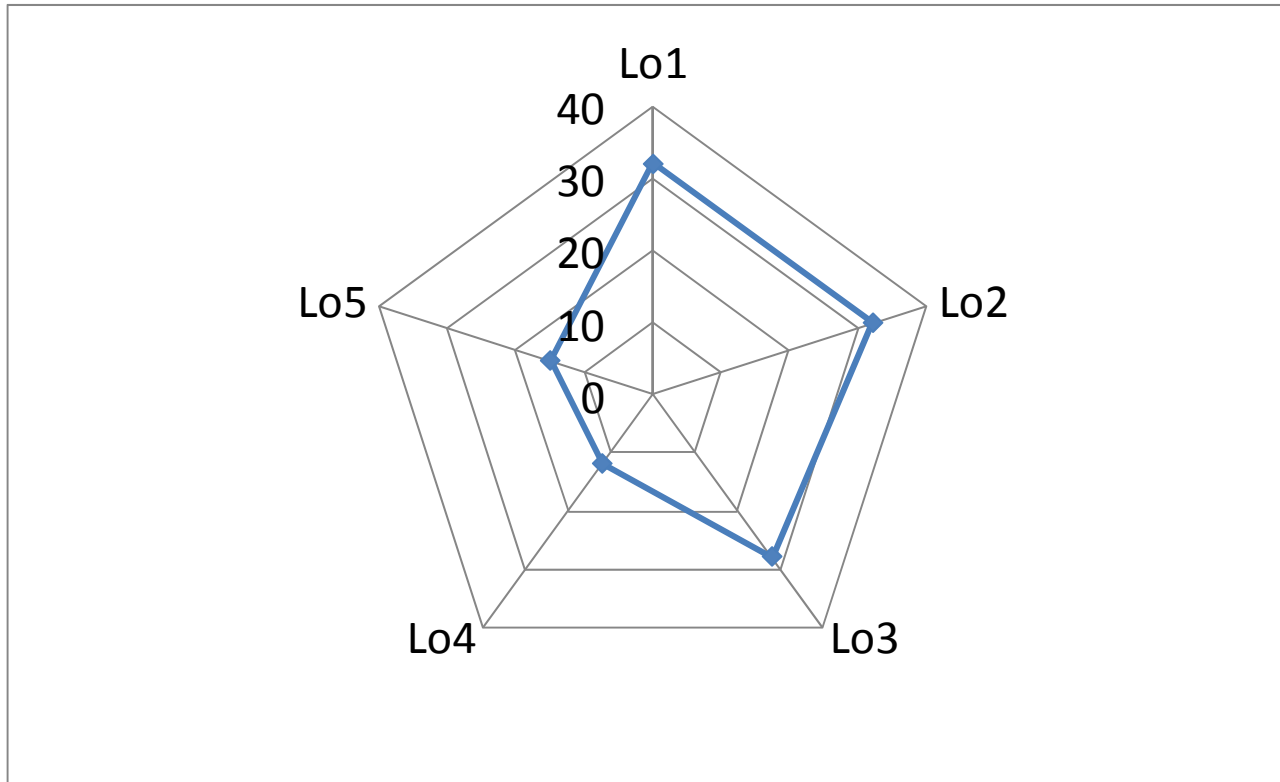
Example for Resilience Indicator description for Personal dimension

Or5 – Governance Framework - Role and responsibilities definition for Resilience	
Description	Provide the organizational model to enable the resilience coordination, command and control within organizations such as the roles and responsibilities assumed by institutions and other business or governmental entities to face national interest incidents. For example within organizations role and responsibilities of designated personnel responsible for managing crisis procedures, performing risk management process or responding security threats and emergencies are to be identified and explained. At national level for the US Department of Homeland Security manages a bottom-up network of entities from local first responders to nationwide threat analysis and emergency response centers like the National Cybersecurity and Communications Integration Center (NCCIC).
Dimensions	Organizational
Sector Applicability Relevance	To be estimated by the sector specific experts
Evaluation methods	Presence & Maturity level of Adoption by the Organization
Sources / References	www.cosla.gov.uk/system/files/private/cw130219item12annex.pdf https://www.hsdl.org/?view&did=733614 http://www.cio.ca.gov/ois/government/documents/pdf/iso_roles_respon_guide.pdf

Example for Resilience Indicator description for Organizational dimension

Co1 - Organization's relationship with business partners	
Description	<p>A partnership is where two or more people need to work together to accomplish a goal while building trust and a mutually beneficial relationship. This means the partnership is voluntarily agreed upon, built on the desire to have trust, and based on agreed-upon mutual benefits.</p> <p>Relationships impact every aspect of business operations. Collaboration may occur as individual one-to-one partnerships or it may involve multiple parties working together such as external alliance partners, suppliers, internal divisions and customers. An organization must therefore take a structured approach to partnering and be confident that the relationship will complement and enhance existing business activities.</p>
Dimensions	Cooperative
Sector Applicability Relevance	To be estimated by the sector specific experts
Evaluation methods	Degree of implementation
Sources / References	http://www.bsigroup.com/LocalFiles/en-GB/bs-11000/resources/BSI-BS-11000-implementation-guide-UK-EN.pdf

Example for Resilience Indicator description for Cooperational dimension



**Radar Chart is suggested to represent ALL Indicators for the same DIMENSION
(Technical Physical, Technical Logical, Personel, Organizational, Cooperation)**

KEY ROLES IN THE ORGANISATION

RESILIENCE INDICATORS	Chief Executive Officer	Chief Information Officer	Chief Security Officer	Chief Information and Security Officer	Human Resources Director	Security Liason Officer	Business continuity manager	Supply chain manager	Other
	CEO	CIO	CSO	CISO	HR Director	SLO	BCM	SCM
Lo01									
Lo02									
Lo03									
....									
Ph01									
Ph02									
Ph03									
....									
Pe01									
Pe02									
Pe03									
.....									
Or01									
Or02									
Or03									
...									
Co01									
Co02									
Co03									
...									

The general matrix with resilience indicators by row and possible key role in the organisation by column that should be customized for each specific CI operator/owner.

CONSTRUCTING COMPOSITE INDICATORS

Critical Infrastructure Resilience cannot be assessed by examining indicators in isolation. These indicators are strongly interconnected, and a quantification of CI resilience requires an indexed calculation, based on the weighted importance of each indicator. Drawing these indicators together into a meaningful composite indicator is not a simple task. It requires a sophisticated modeling approach not covered yet by the methodology.

RESILIENCE: How to Construct Composite Resilience Index at different levels of abstraction

$$R_{SYSTEM} = f(R_{TECH}, R_{PERS}, R_{ORG}, R_{PART})$$

The Challenge

Data emanating from the four dimensions have to be correlated and a composed value of resilience for the overall CI inferred using tailored aggregation algorithm account for the dependency level between the resilience of the different dimensions and layers.

2016 AIIC Working Group on “Guidelines for Community Resilience Evaluation”



Aim of the Working Group is to propose Community Resilience Metrics, answering to the following questions:

- How can community leaders know how resilient their community is?
- How can they know if their decisions and investments to improve resilience are making a significant difference?

The Working Group will start from the results of the previous Working Group “Guidelines for Critical Infrastructures Resilience Evaluation”, by introducing the concepts of “**Dependencies, Interdependencies and Cascading effects**” aimed at identifying dependencies and potential cascading failures among the Infrastructures serving the Community, through the implementation of combinations of societal, organisational and technological resilience concepts

The Working Group will refer to the Official Reports NIST SP 1190 (Vol. I & II) and NIST SP 1197

Thank you for your attention

for any further information

Sandro Bologna
AllC Working Group on Critical Infrastructure Resilience
s.bologna@infrastrutturecritiche.it

[*http://www.infrastrutturecritiche.it/new/*](http://www.infrastrutturecritiche.it/new/)