IFIP 10.4 WG – 29 Gennaio 2020

Situational picture for integrated cyber-physical Critical Infrastructure Protection

Gabriele Giunta

Head of the Smart Transport and Infrastructure Unit

Industry and Security Technologies, Research and Innovation (IS3) Lab

ENGINEERING Research & Development

ENGINEERING IS3 Lab cini consorzio interuniversitario nazionale per l'informatica

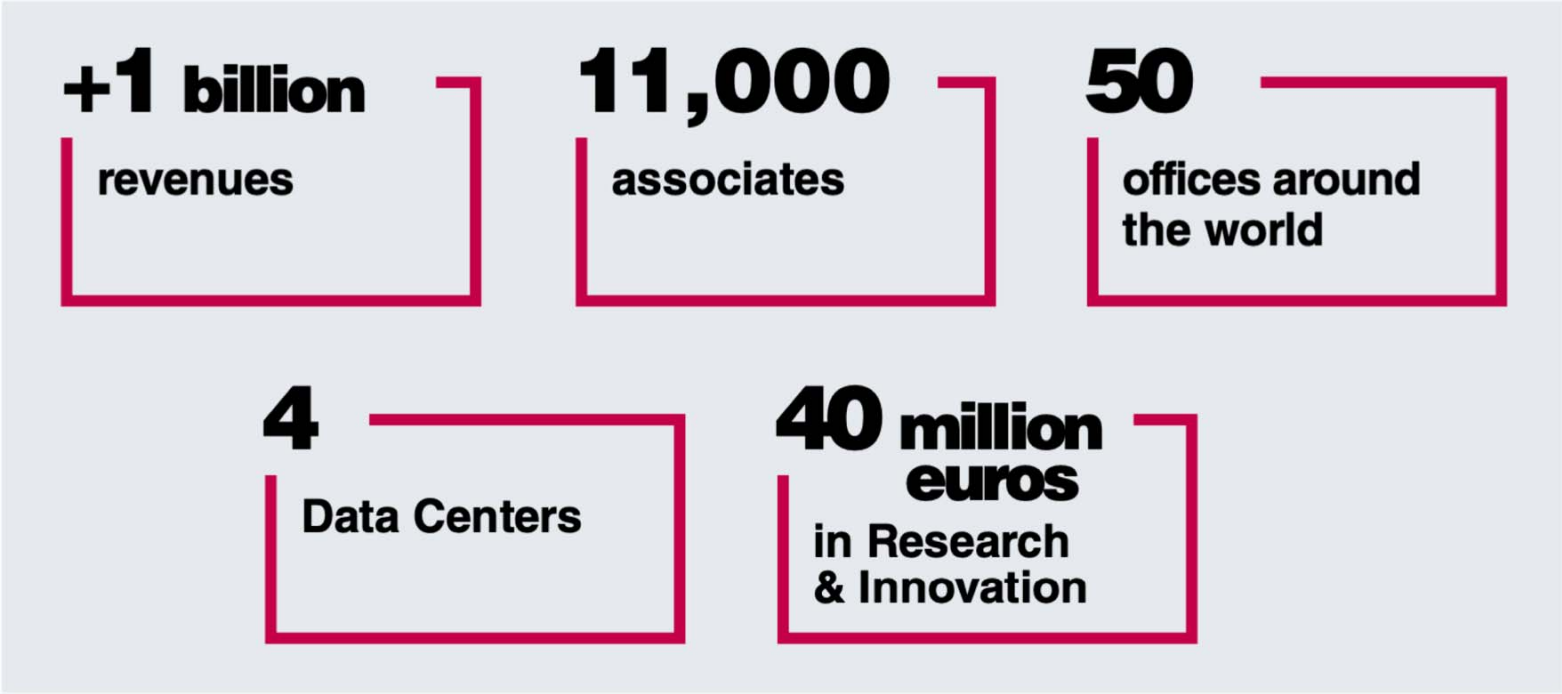
Overview

- ENGINEERING Corporate Profile
- CIP Reference and Logical Architecture
- Data and Information Flow
- Data Processing Chain
- Identification and Event Processing
- Situation Perception and Comprehension
- Situational Visualisation (situational picture)
- Related Research Projects

ENGINEERING

Corporate Profile

LEADER IN DIGITAL TRANSFORMATION



OUR PORTFOLIO

THE WORLD WE LIVE IN

- AUGMENTED CITY
- SMART TRANSPORTATION
- SMART ENERGY & UTILITIES
- DIGITAL MEDIA & COMMUNICATION

THE WORLD WE WORK IN

- DIGITAL INDUSTRY
- DIGITAL FINANCE
- DIGITAL RETAIL & FASHION
- SMART AGRICULTURE

THE WORLD THAT TAKES CARE OF US

- SMART GOVERNMENT
- E-HEALTH
- DIGITAL DEFENSE, AEROSPACE & HOMELAND SECURITY

RESEARCH AND INNOVATION

€ 40 Million
in annual investments

80
ongoing research projects

420
researchers and data scientists

4
development laboratories

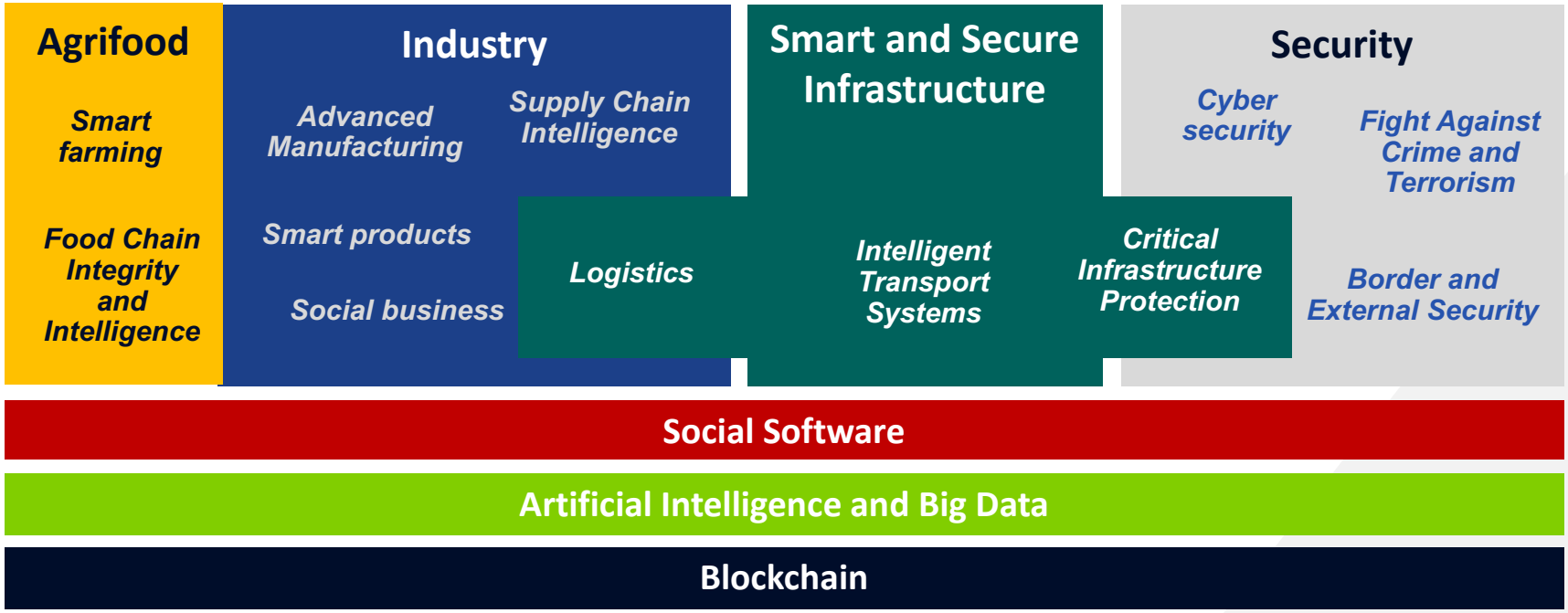
The core of the ecosystem consists of a **network of over 200 innovators** selected not only from within all company structures, but also universities, research centers, start-ups, SMEs and industrial partners.

- ARTIFICIAL INTELLIGENCE
- AUGMENTED REALITY
- BLOCKCHAIN
- CLOUD
- CYBERSECURITY
- DATA
- DIGITAL PLATFORMS
- INTERNET OF THINGS
- ROBOTICS

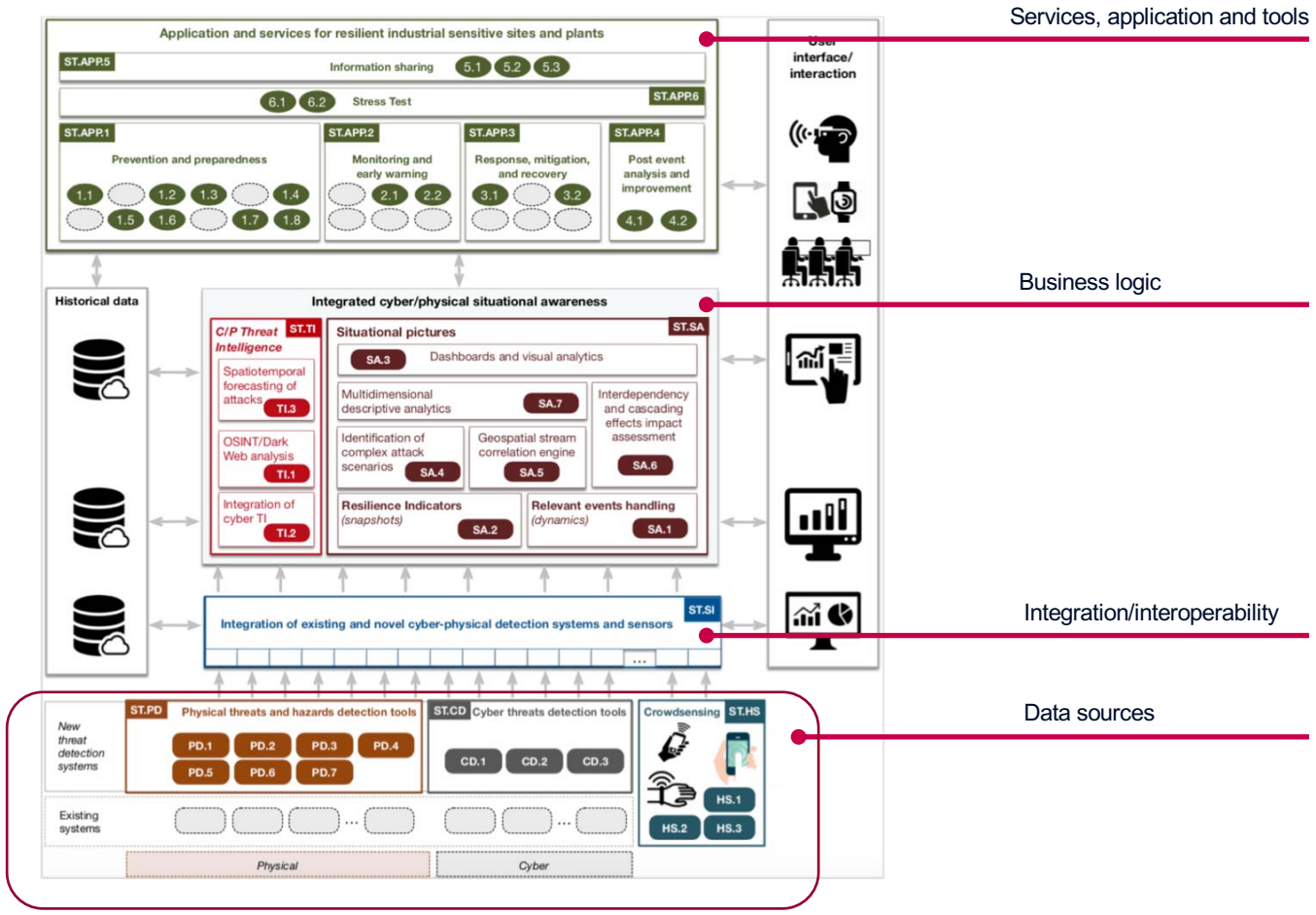
Industry and Security Technologies Research and Innovation ... in a nutshell

Mission: to **conceive, design, develop, and demonstrate** innovative **concepts and solutions** in the **industry, agrifood, transport, security and defense** sectors.

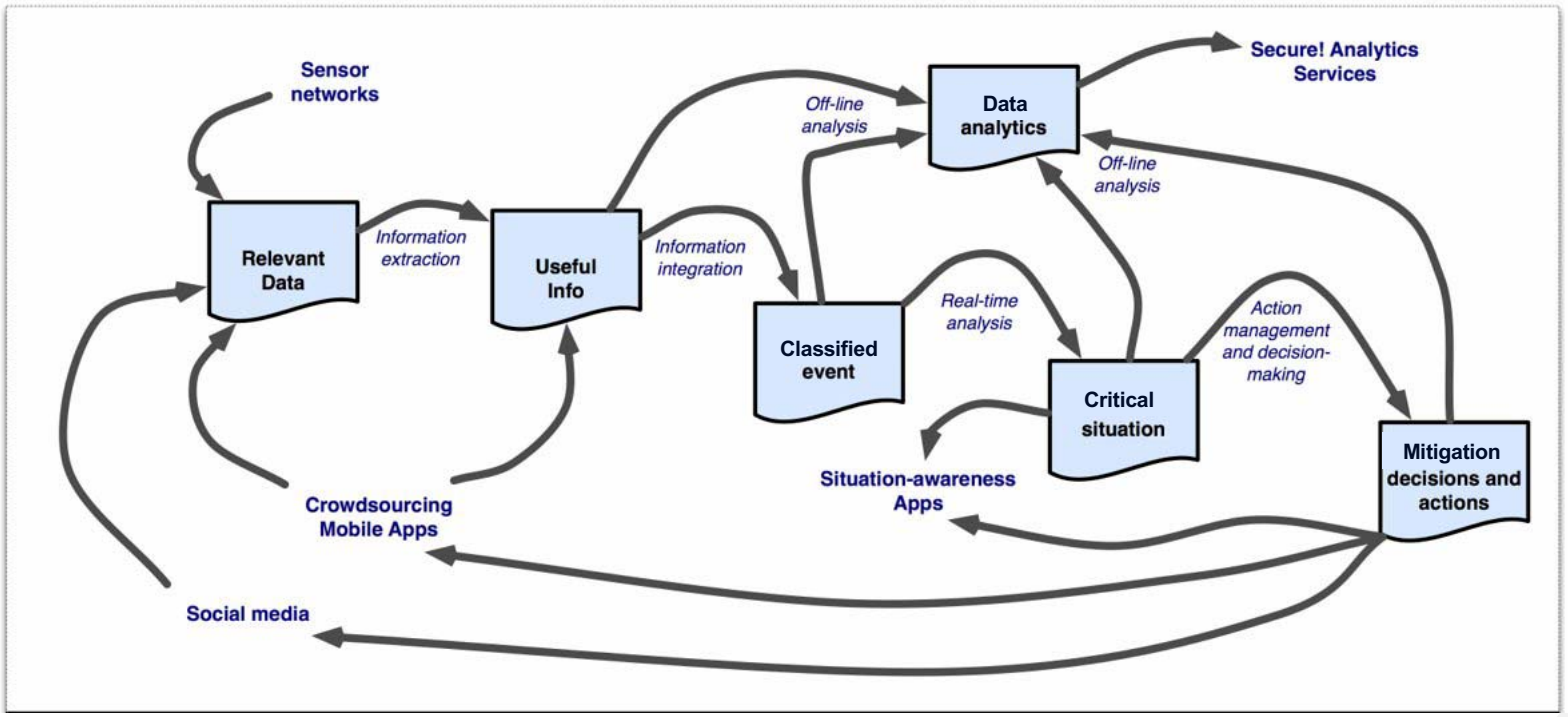
42 running projects



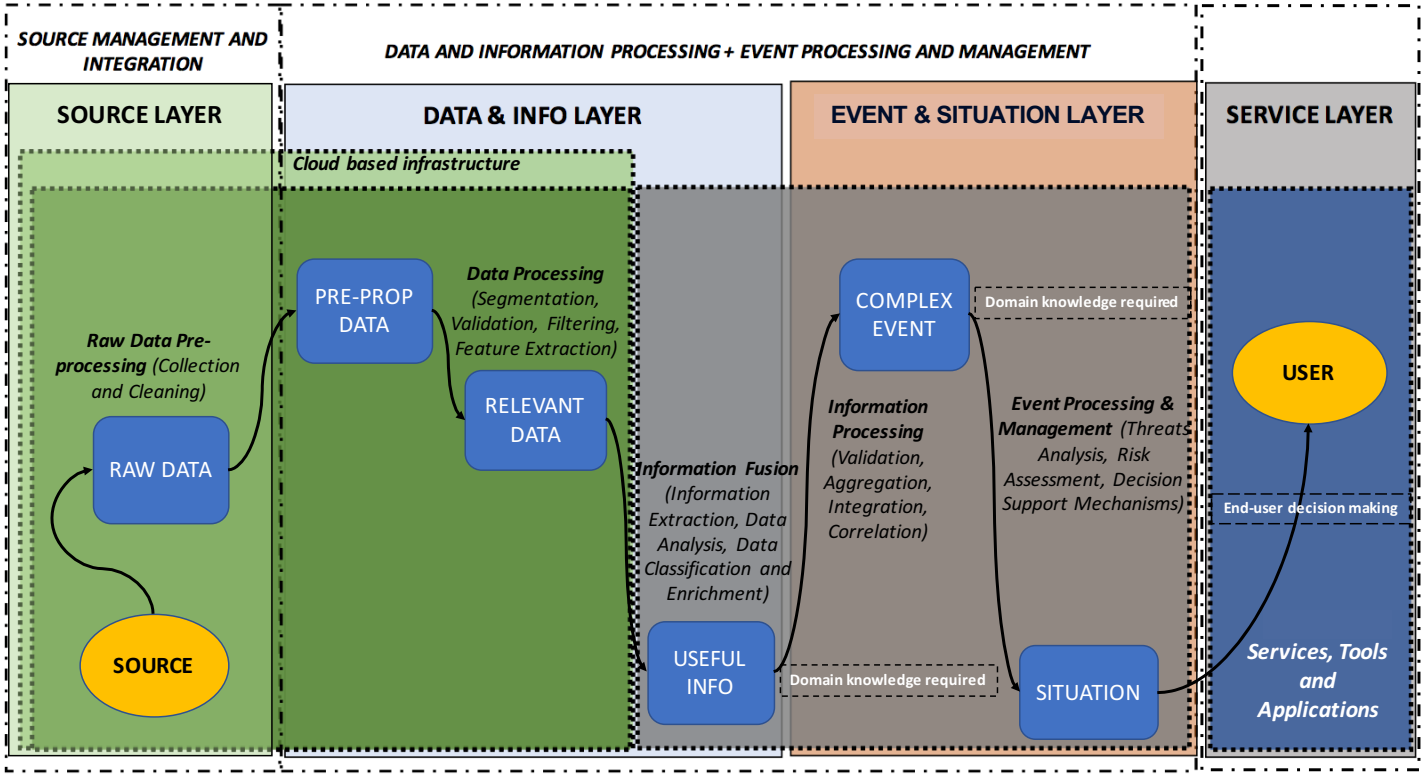
CIP Reference Architecture



Data and Information Flow (1/2)



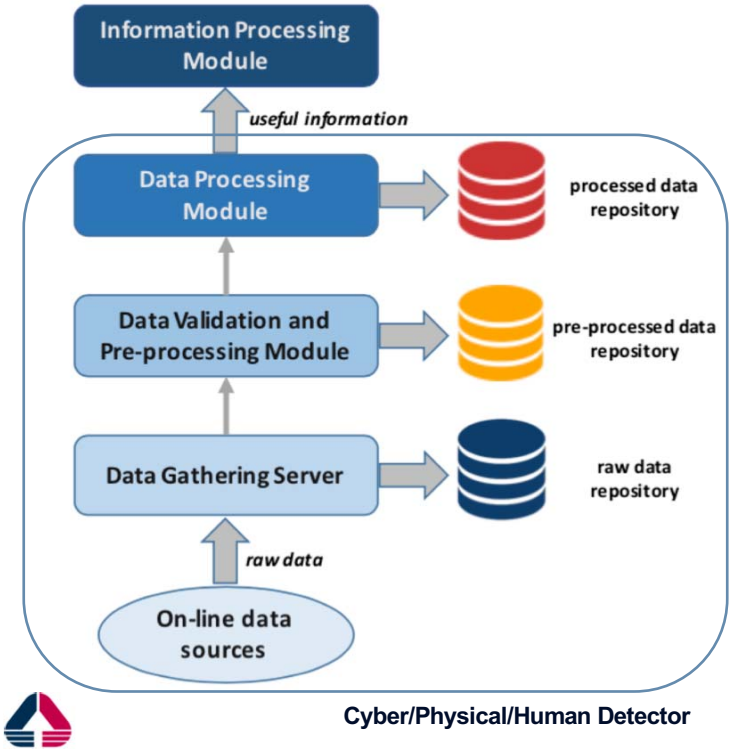
Data and Information Flow (2/2)



Data and Information Sources

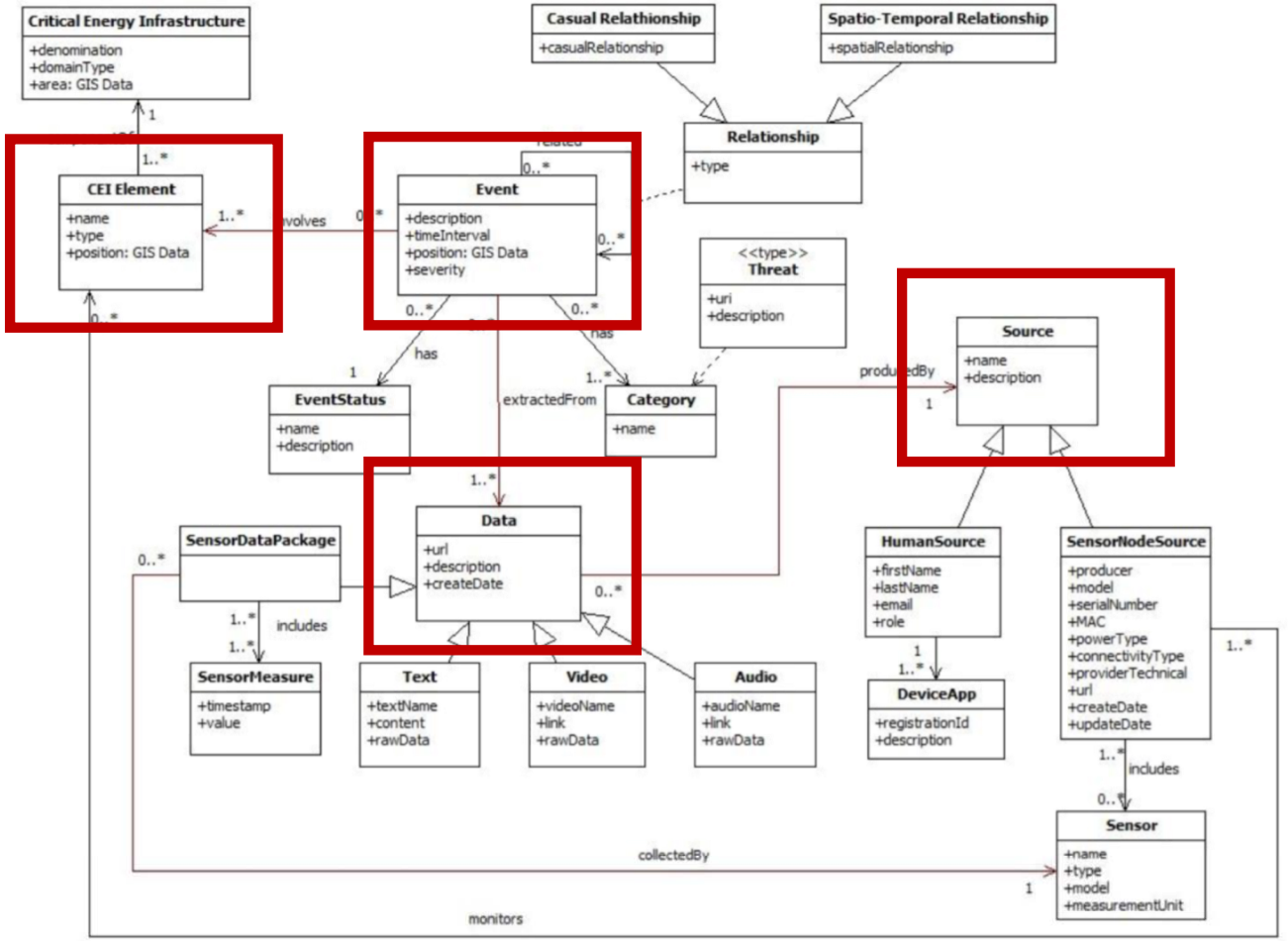
- Integration of heterogeneous and distributed source
  - **Cyber Sensors:** SCADA, communication network elements, smart meters, information system elements, operation procedure elements, business procedure elements, …
  - **Physical Sensors:** vibration (IR, strain, fiber, etc.), geophone, Lidar, PMZ camera, Thermal camera, RF radar, camera equipped UxVs, …
  - **Human Sensors:** (as know as “Human-In-The-Loop”) for innovative, trusted, traceable and bidirectional information flows, enabling efficient communication from/to the Control Centre.
  - **WEB and Social media**
  - **External (already existing) Systems:** CCTV, Remote Video Surveillance, …

Data Processing Chain



- **Data Gathering Server:** responsible to store the received raw and processed data and notify the presence of new incoming data to the other modules (interoperability layer, P&S mechanism, standard APIs, …)
- **Data Pre-processing:** cleaning, filtering, integration, transformation, normalisation, reduction, …
- **Data Validation** (mainly for crowdsourcing apps): crowdsensing mobile apps can be used by restricted (i.e. skilled/expert) and unrestricted set of users, different level of validation on the data collected from “human sensors” should be considered (filtering based on statistical approaches or on-site check performed by skilled users)
- **Data Processing/Analysis:** feature and information extraction via pattern recognition/classification (e.g., supervised machine learning method) and probabilistic modelling (e.g., Bayesian Networks).

Event Model

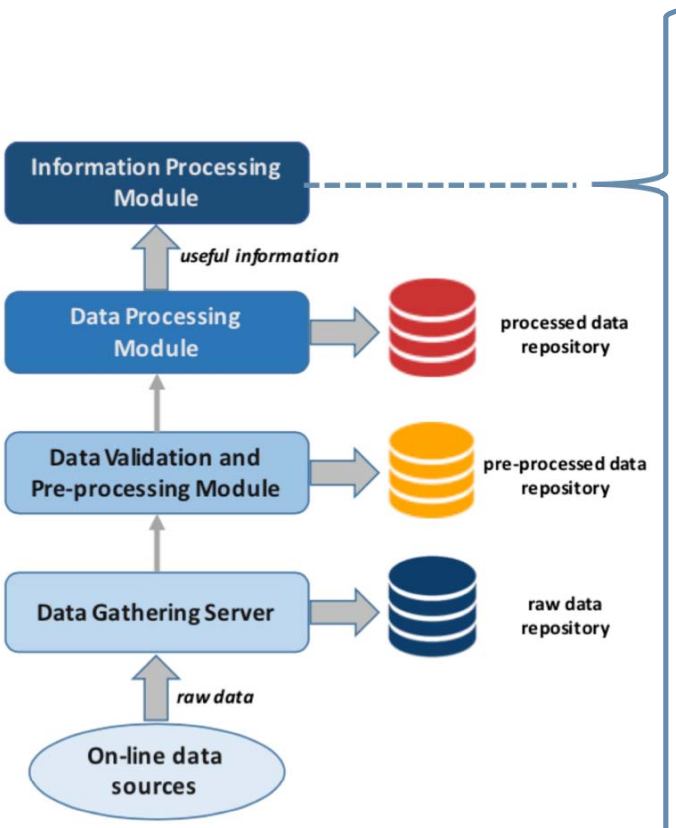

Critical Energy Infrastructure
+denomination
+domainType
+area: GIS Data
Casual Relathionship
+casualRelationship
Spatio-Temporal Relationship
+spatialRelationship
Relationship
+type
CEI Element
+name
+type
+position: GIS Data
Event
+description
+timeInterval
+position: GIS Data
+severity
<<type>>
Threat
+uri
+description
Source
+name
+description
EventStatus
+name
+description
Category
+name
Data
+url
+description
+createDate
SensorDataPackage
HumanSource
+firstName
+lastName
+email
+role
SensorNodeSource
+producer
+model
+serialNumber
+MAC
+powerType
+connectivityType
+providerTechnical
+url
+createDate
+updateDate
SensorMeasure
+timestamp
+value
Text
+textName
+content
+rawData
Video
+videoName
+link
+rawData
Audio
+audioName
+link
+rawData
DeviceApp
+registrationId
+description
Sensor
+name
+type
+model
+measurementUnit
involves
has
extractedFrom
includes
collectedBy
monitors

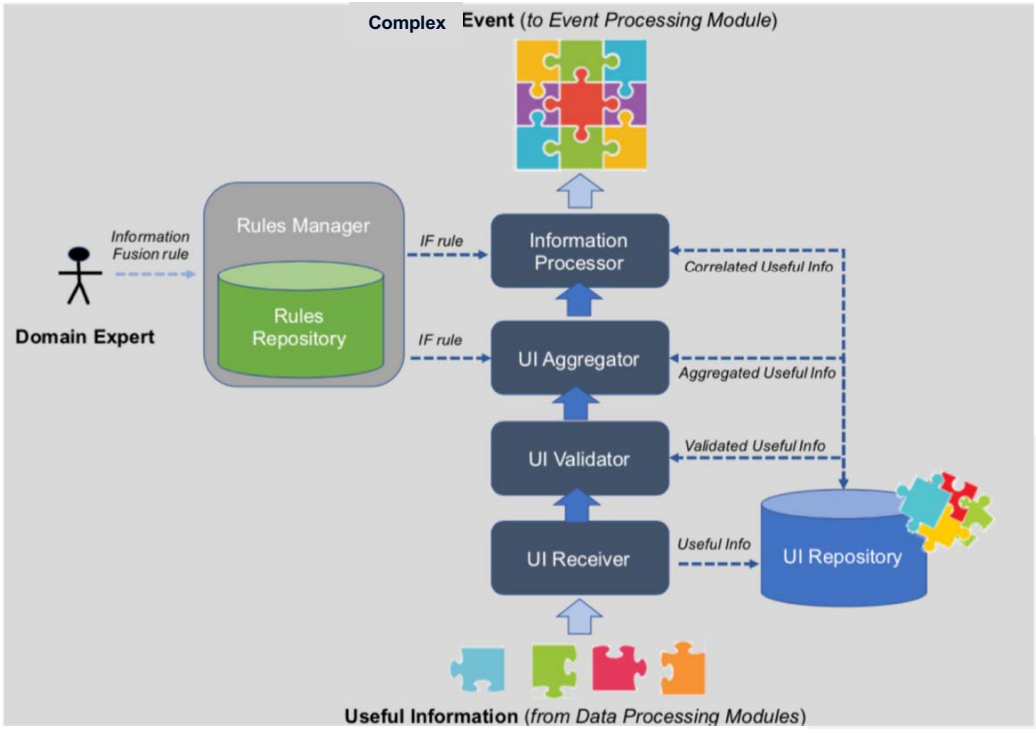
Information Processing (1/4)

DEFINITION

- **Simple Event (or Useful Info):** any event refers to an **abnormal** or **anomaly behaviour** detected in one or more CI subsystems (e.g. SCADA system, network, secondary substation, etc.) by any Cyber or Physical Detector. Each ***detector*** is specialized in the analysis of a specific type of data, so a *simple event* is always related to the processing of a specific type of data;
- **Complex Event:** it is an event that refers to the identification of the occurrence of a specific threat belong to a ***threat classification***. A *complex event* is identified by applying several *CEP techniques* to each detected simple event (e.g. spatio-temporal and causal correlation and the pattern recognition).
- **State of the environment:** consists of a set of complex events. It can potentially represent a threat or not. It has to be deeply understood and perceived (***situation comprehension and perception***).

Information Processing (2/4)





Information Processing (3/4)

- **Simple Event Receiver:** whenever a new simple event (NSE) is received, the Simple Event Receiver (SER) checks its syntax, the presence of every mandatory field and the correctness of values assigned to every field.
- **Simple Event Validation:** (temporal, spatial) **consistency** and **coherence** (e.g. contrasting information) of simple event data are checked and evaluated;

Temporal: when the creation timestamp of any data included in the simple event are not included in its time interval

Spatial: when the location of the simple event is very far to the position of the data source that has produced the data from which it was identified or of the involved CEI Element.

```
Given a pair of Simple Event SE1,SE2
When categories of SE1,SE2 are equals AND
     category of SE1 is "People Recognition" AND
     the recognised person in SE1,SE2 is the same AND
     distance of the SE1,SE2 time intervals is less than "2 minutes" AND
     distance of the SE1,SE2 positions is greater than "1000 meters"
Then mark SE1,SE2 as "incoherent"
```

https://cucumber.io/docs/gherkin/reference/

Information Processing (4/4)

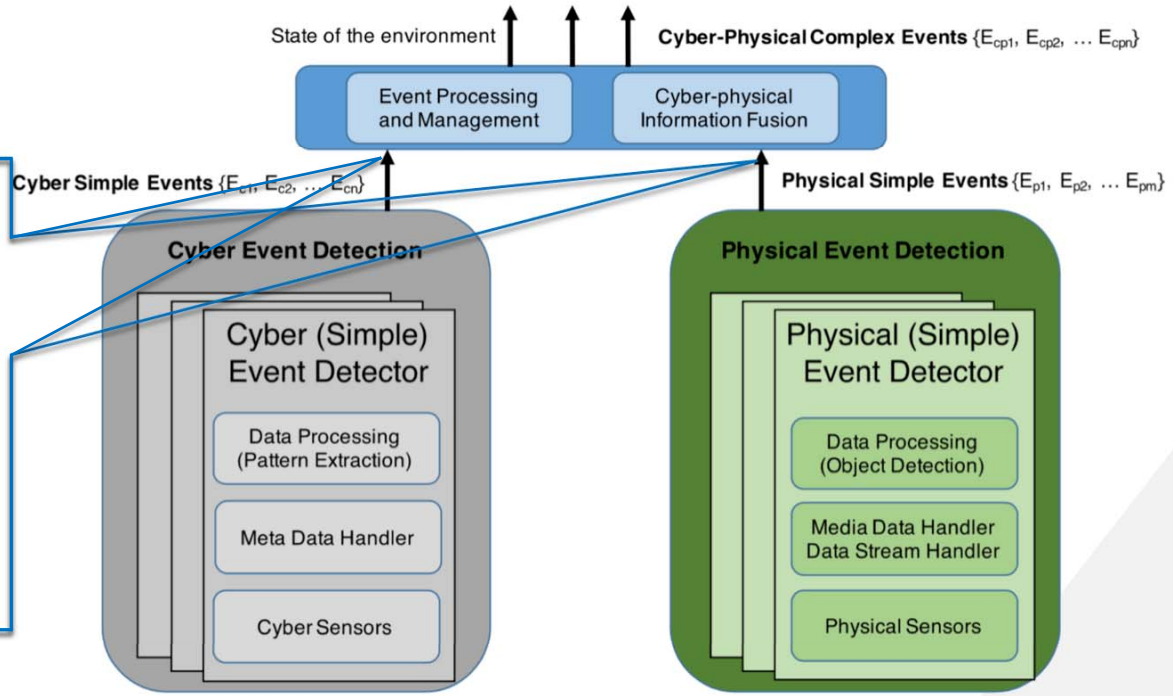
- **Simple Event Aggregation:** set of (temporally and spatially) correlated simple events related to the same phenomena (or condition) are aggregated.
- **Information Fusion:** set of aggregate simple events that match some patterns are fused in a complex event regarding a specific threat included in the threat classification.

```
Given a simple event S1 of category "penetration-test-detection" AND
      a simple event S2 of category "anomaly-behaviour-detection" AND
      S1 is followed by S2
When S1 and S2 involve the same CEI Element AND
      S1 and S2 are within the same time window of "20 minutes"
Then create a new Complex Event CE of type "Obtain-credential" AND
      assign to CE the location of SE1 AND
      assign to CE the CEI Element involved in SE1 AND
      assign to CE the severity value "high".
```

```
Given a set of Simple Event SE
When each Simple Event included in SE has the same category C AND
     the category C is included in following categories:
      |PenetrationTestDetection|
      |AtypicalUsageDetection|
      |AtypicalCommunicationDetection|
      |AtypicalBehaviourDetection | AND
      each Simple Event in SE involves the same CEI Element or none AND
      the time interval of each Simple Event in SE is within a time
        windows of "30 minutes" AND
      the geodetic distance of each Simple Event in SE from the other
        ones is at most of "500 meters"
Then aggregate simple events in SE
```

Cyber and Physical Detection

```
{
  category: "AnomalyVibration", -- Type of Simple Event Detected
  startTime: 20171130170100.000, -- timestamp of the most young measurement
                                 -- included in the sample from which the phenomenon
                                 -- or condition has been detected
  endTime: 20171130170800.000,   -- timestamp of the most old measurement included
                                 -- in the sample from which the phenomenon or
                                 -- condition has been detected
  location: {point: [41.904119, 12.498427]}, -- location of identification, if null
                                             -- will be used the location of the node
                                             -- from which was collected the data
  sensorDataPackage: {
    SensorSource: {nwId: "XXX", nodeId: "XXX_NID", sensorId: "XXX_NID_SID"}
    data: [{timestamp: 20171130170100.000, value: "3.0"},
           {timestamp: 20171130170200.000, value: "2.5"},
           {timestamp: 20171130170300.000, value: "2.7"},
           {timestamp: 20171130170400.000, value: "3.0"},
           {timestamp: 20171130170500.000, value: "2.7"},
           {timestamp: 20171130170600.000, value: "2.6"},
           {timestamp: 20171130170700.000, value: "2.3"},
           {timestamp: 20171130170800.000, value: "2.0"}]
  },
  CEIElement: {type: CRIT_INFRA_ELE, id: "Edison_CE01_Medium-Voltage-Transformer"} -- Asset to which the SE was detected,
                                                -- if null will be used the asset where
                                                -- is installed the node from which was
                                                -- collected the data
  otherInfo: {} -- optional free field for Additional data to add to the SE
}
```



Event Processing and Management

- **Complex Event Enrichment:** new CEs are enriched in order to specialise the classification, to assess the severity and so on;
- **Complex Event Aggregation:** aggregates groups of similar complex events involved in the same CI Elements and occurring in close time intervals and locations;
- **Complex Event Correlation:** performs space-time and causal correlation on each new complex event.
- **Simple and Complex Events Management**: several types of *event rules* drive the processing work performed within the Information and Event Modules. Sometimes a *visual rule modeller* can be provided to make easier the rule modelling either using a **specific language** or a pure **visual approach**.

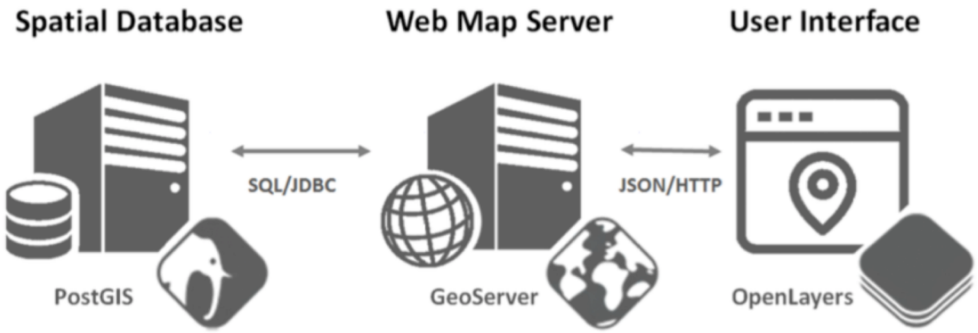
```
Given a new Complex Event CE of type "Obtain-credentials" AND
      CE includes a not empty set CEIs of CEI Elements, or that is a
        component element of one, of type "SCADA SYSTEM"
Then assign to CE the category value "Obtained-SCADA-credentials" AND
     assign to CE the CEI Element set resulting from the union of its
       current one and the CEIs
```

```
Given a new Complex Event CE1 AND
      a previously occurred Complex Event CE2
When the category of CE1 is equal to "Obtained-SCADA-credentials" AND
     the category of CE2 is included in:
       |"Obtain-Password"|
       |"Extract-Credential"|
       |"Impersonate-Authorized-User"| AND
     the distance between the time intervals of CE1 and CE2 is less
       than "10 minutes" AND
     the occurrence time interval of CE2 starting before of that of
       CE1 AND
     the CEI Elements included in CE1 and CE2 are all related to the
       same CEI Element of type "SCADA System"
Then add a new Causal Relationship from CE2 to CE1
```

Situation Perception and Comprehension

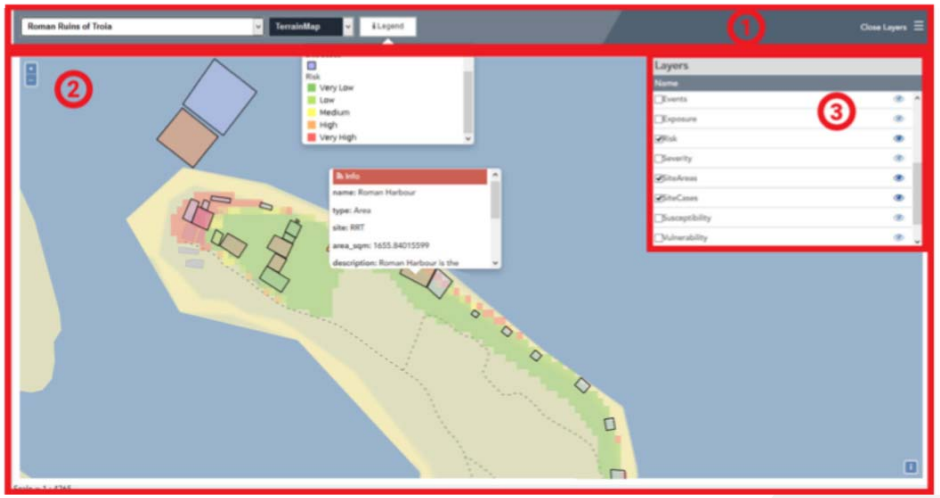
- **Prevention and preparedness**
  - Risk and Impact Assessment
  - Interdependencies and cascading effect
- **Monitoring and Early Warning**
  - Simulation
  - Causal Analysis
  - Surveillance and Monitoring
- **Response Mitigation and Recovery**
  - Quick Damage Assessment
  - Survey and Diagnosis
- **Post event analysis and improvement**
  - Prescriptive analytics and recommendations

Situation Visualisation (situational picture)

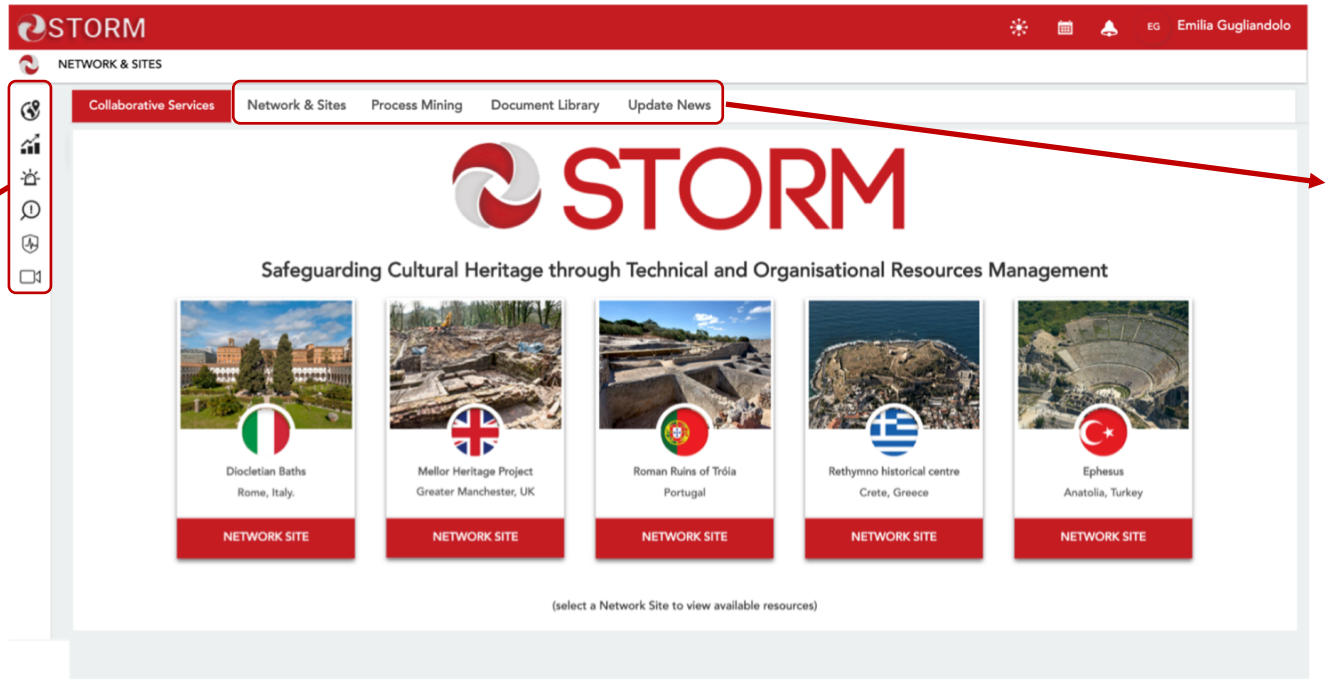


Open WEB GIS services and infrastructure

- **actions panel** (1), where different **actions** can be selected, such as pilot site area, base map for visualization,
- **map panel** (2), where web **map layers information** is displayed, as well as “pop- up” informative windows on features, zoom in/out and pan actions for the interactive map interface, and
- **layers panel** (3), where all **available map layers** of the corresponding web-GIS services are displayed for the selected pilot site area.



Situation Visualisation (situational picture)



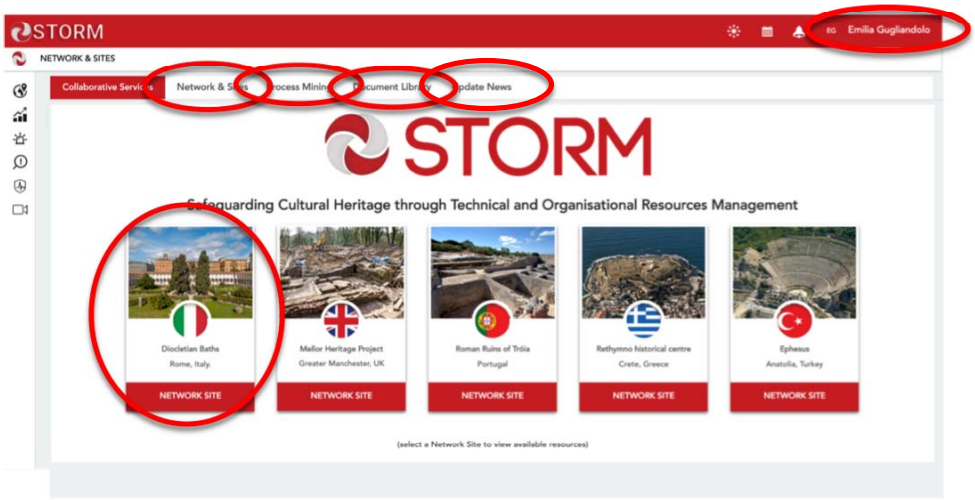
Operative Services

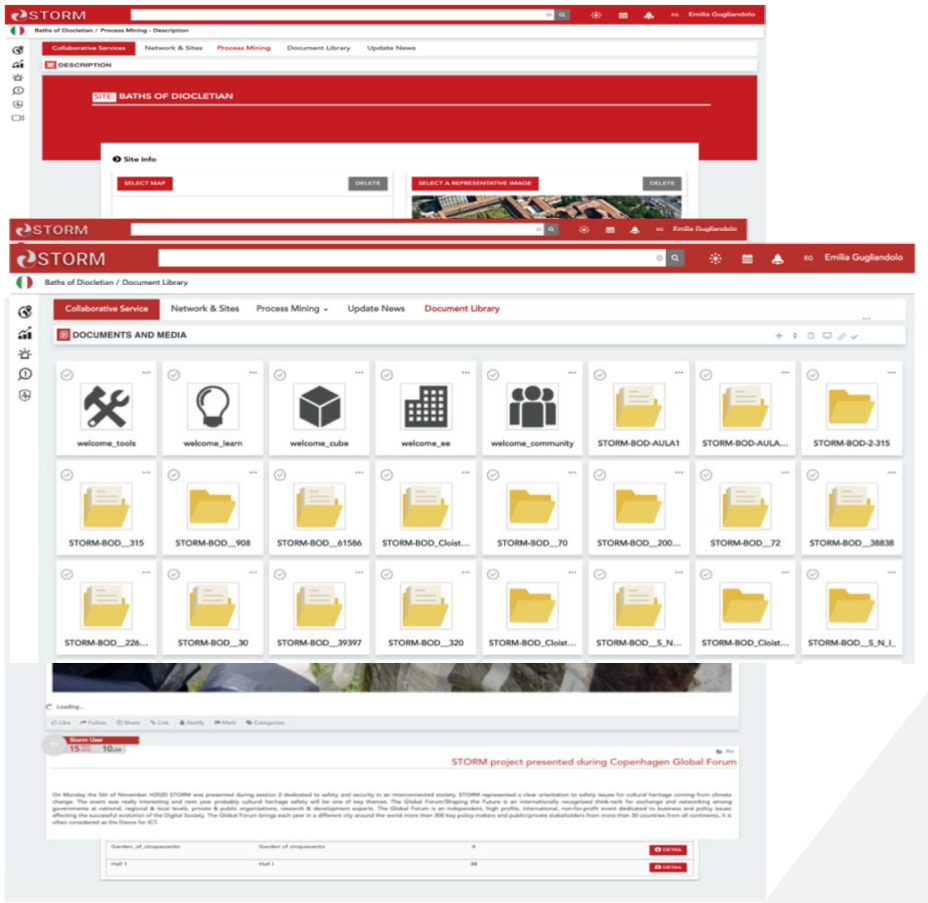
- *Sensory Map*
- *Visual Analytics*
- *Diagnosis Reporting*
- *Risk Assessment*
- *Situation Awareness*
- *Camera View*

Collaborative Services

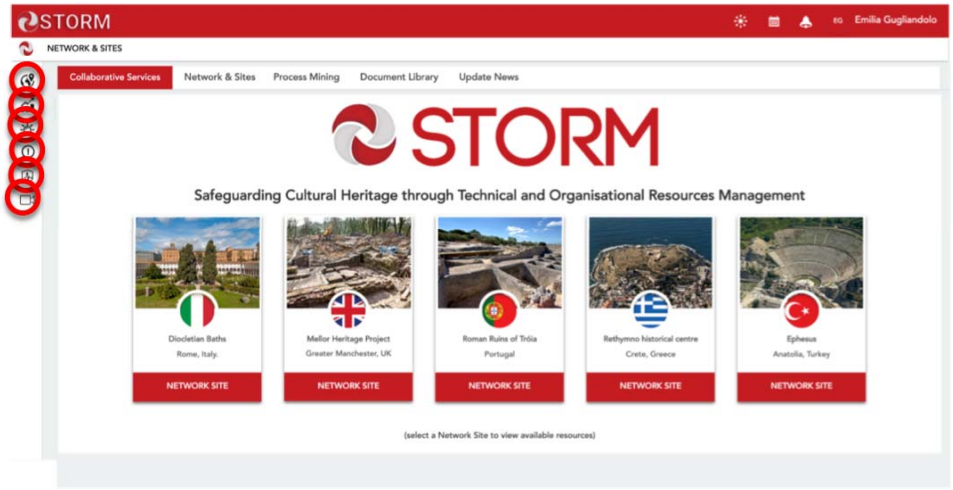
- *Semantic Search*
- *User Profile*
- *Network & Sites*
- *Process Mining*
- *Update News*
- *Document Library*

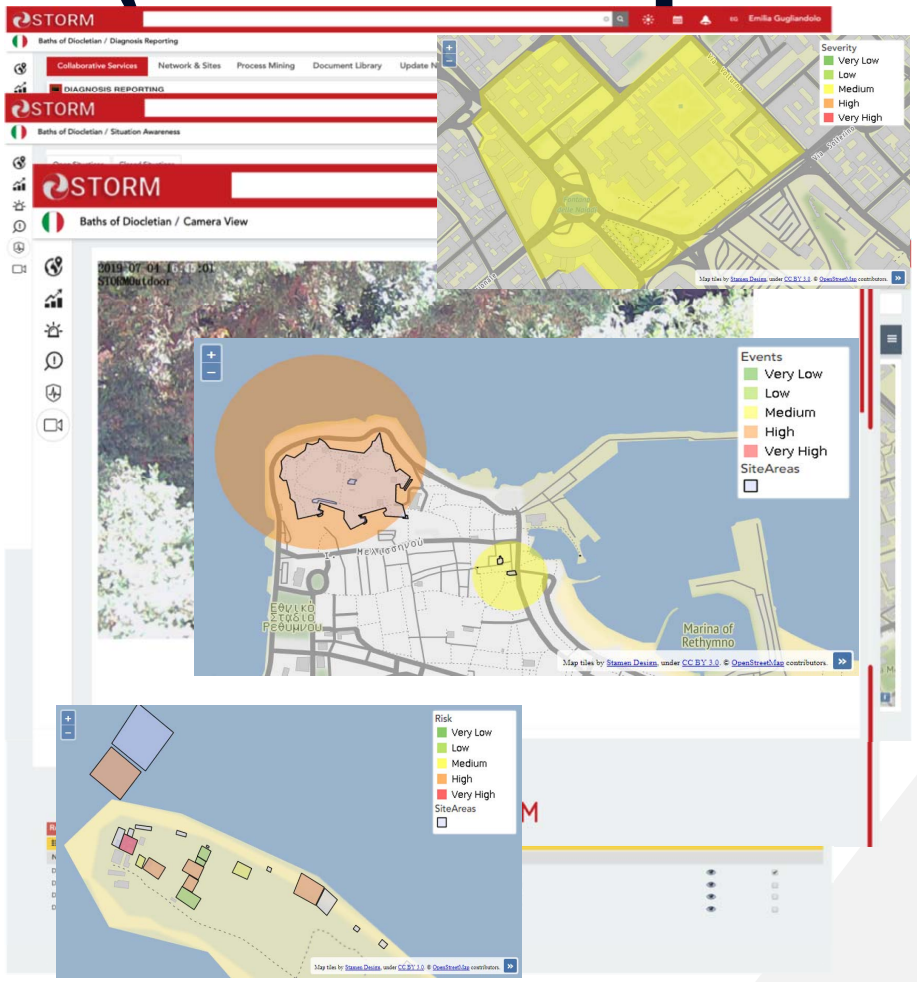
Situation Visualisation (situational picture)





Situation Visualisation (situational picture)





Related research projects

- POR CReO FESR 2007 –2013 **SECURE!**
- H2020-DRS-11-2015 **STORM** (http://www.storm-project.eu/)
- H2020-CIP-2016-2018 **DEFENDER** (https://defender-project.eu/)
- H2020-SU-SEC-2018 **FASTER** (https://www.faster-project.eu/)
- H2020-SU-INFRA-2018 **INFRASTRESS** (https://www.infrastress.eu/)

UNDER GRANT AGREEMENT PREPARATION

- H2020-SU-INFRA-2019 **7SHIELD**
- H2020-SU-INFRA-2019 **ENSURESEC**

THANK YOU

ENGINEERING

Gabriele Giunta

Head of Unit

www.eng.it

@EngineeringSpa

Engineering Ingegneria Informatica Spa

gruppo.engineering

gabriele.giunta@eng.it