QUATIC 2026 International Conference on the Quality of Information and Communications Technology

Understanding the Concepts Behind Ethics in Designing Cyber-Physical Systems

Yelyzaveta Kurkchi, Ivan Compagnucci, Catia Trubiani

Gran Sasso Science Institute, L'Aquila, Italy

GRAN SASSO SCIENCE INSTITUTE
SCHOOL OF ADVANCED STUDIES
Scuola Universitaria Superiore

Introduction

- Cyber-Physical Systems (CPS) are increasingly deployed in **critical domains**, such as healthcare and industrial systems.
- These systems often **process sensitive data and make decisions that directly affect humans**.

Introduction

- CPS design should consider not only functional requirements, but also **ethics-based requirements**, e.g., **Privacy, Security, and Transparency.**

- Existing approaches provide limited guidance on the **design techniques needed to implement them in CPS.**

How can ethics-based requirements be systematically incorporated into CPS design?

Ethical Shortcomings

- **(W1) Privacy.** CPS may expose sensitive data when protection mechanisms and legal constraints are not explicitly considered.
- **(W2) Security.** Widespread CPS data streams increase exposure to cyberattacks, requiring security measures to evolve over time
- **(W3) Transparency.** Users often lack clear information about what data are collected, how they are used, and which safeguards apply.

Research Methodology

- **RQ:** What design techniques have been proposed and/or applied to address Privacy, Security, and Transparency requirements in the design of CPS?

DESIGN OR DEVELOP* OR MANAGE* OR ARCHITECT*	AND	”CYBER-PHYSICAL SYSTEMS” OR “CYBER PHYSICAL”	AND	“NON-FUNCTIONAL REQUIREMENT”	AND	PRIVACY OR SECURITY OR TRANSPARENCY

Development Stage

Domain

Specific Ethics-based Concerns

Research Methodology

- **RQ:** What design techniques have been proposed and/or applied to address Privacy, Security, and Transparency requirements in the design of CPS?

Inclusion Criteria		Exclusion Criteria	
I1	The paper is written in English.	**E1**	The paper was published before 2020.
I2	The paper has been peer-reviewed.	**E2**	The paper is a duplicate or a shorter version of an already included work.
I3	The paper specifies design techniques on ethics in the context of CPS.	**E3**	The paper is outside the scope of the study

16 papers

Extracting Design Concepts

16 selected papers

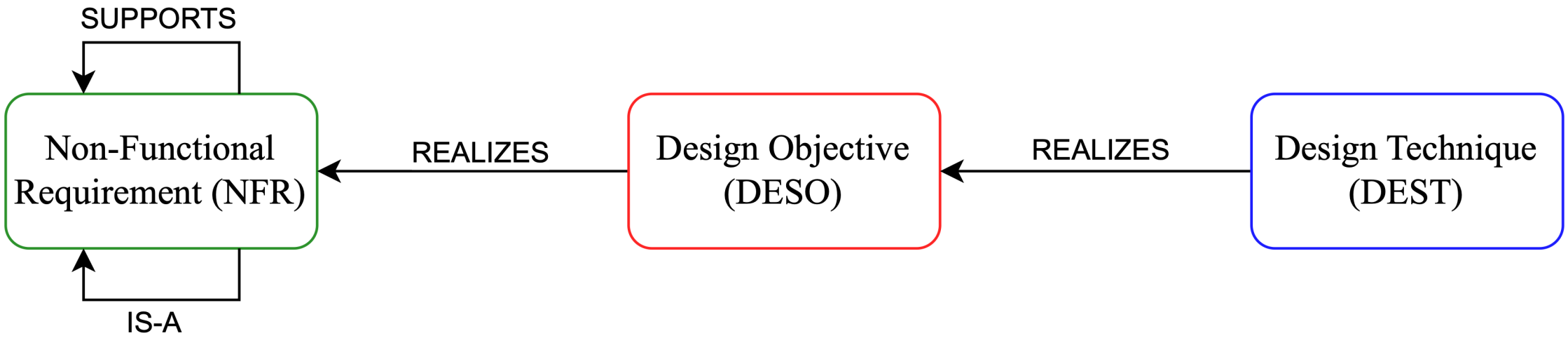
Extract design-oriented concepts

Code by ethical requirement

Group by semantic similarity

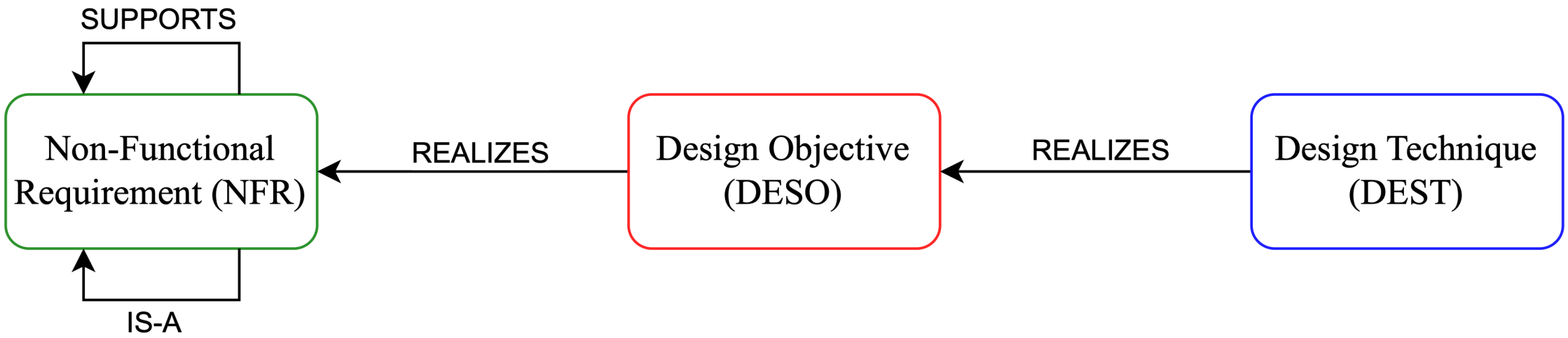
Identify recurring design strategies

Knowledge Base



NFR describes the target of a software system, e.g., privacy;
DESO represents the goals to realize the target, e.g., data protection;
DEST is concrete architectural or implementation-level solutions used to address the design objective, e.g., encryption.

Knowledge Base



RELIZES indicates that a DESO addresses a NFR, or that a DEST implements a DESO
SUPPORTS links complementary NFRs that reinforce one another without implying subclassing, thereby enhancing the parent concept's effectiveness.
IS-A denotes hierarchical specialization among NFRs

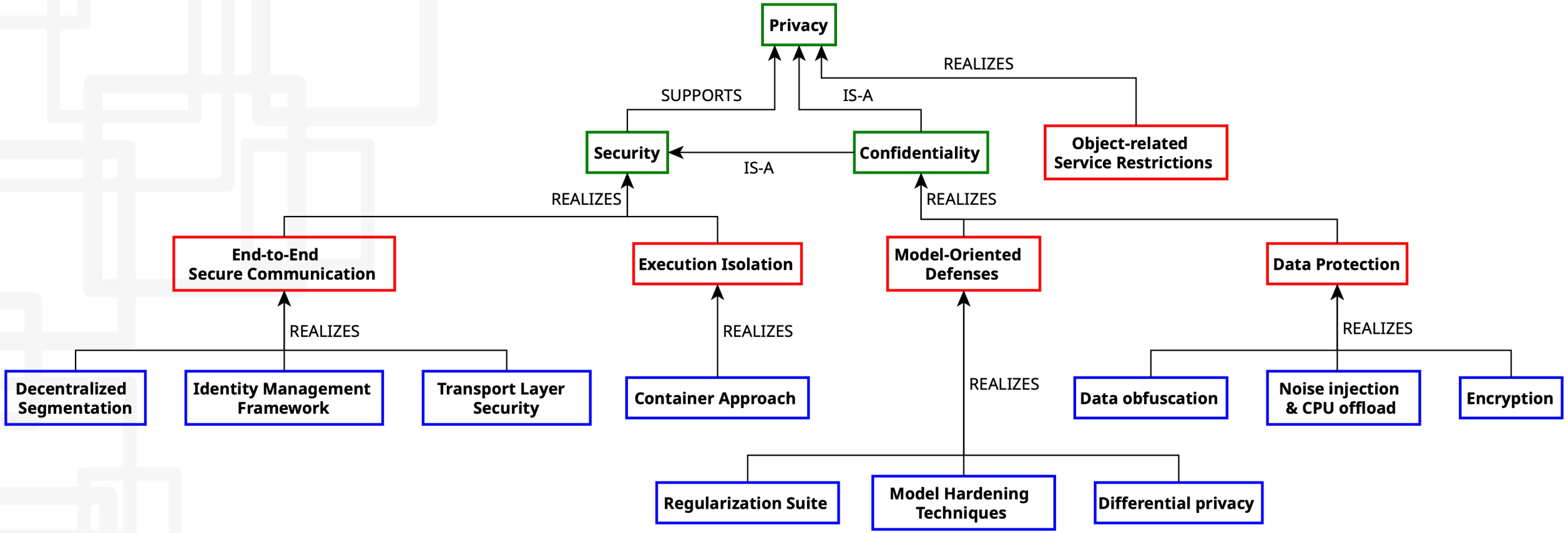
DeTe4CPES Design Approach

DEsign TEchniques for Cyber-Physical Ethical Systems (DeTe4CPES)

- Supports CPS design with Privacy, Security, and Transparency.
- Organizes knowledge extracted from the literature into knowledge graphs.
- Maps Design Objectives to corresponding Design Techniques.
- DeTe4CPES is publicly available.

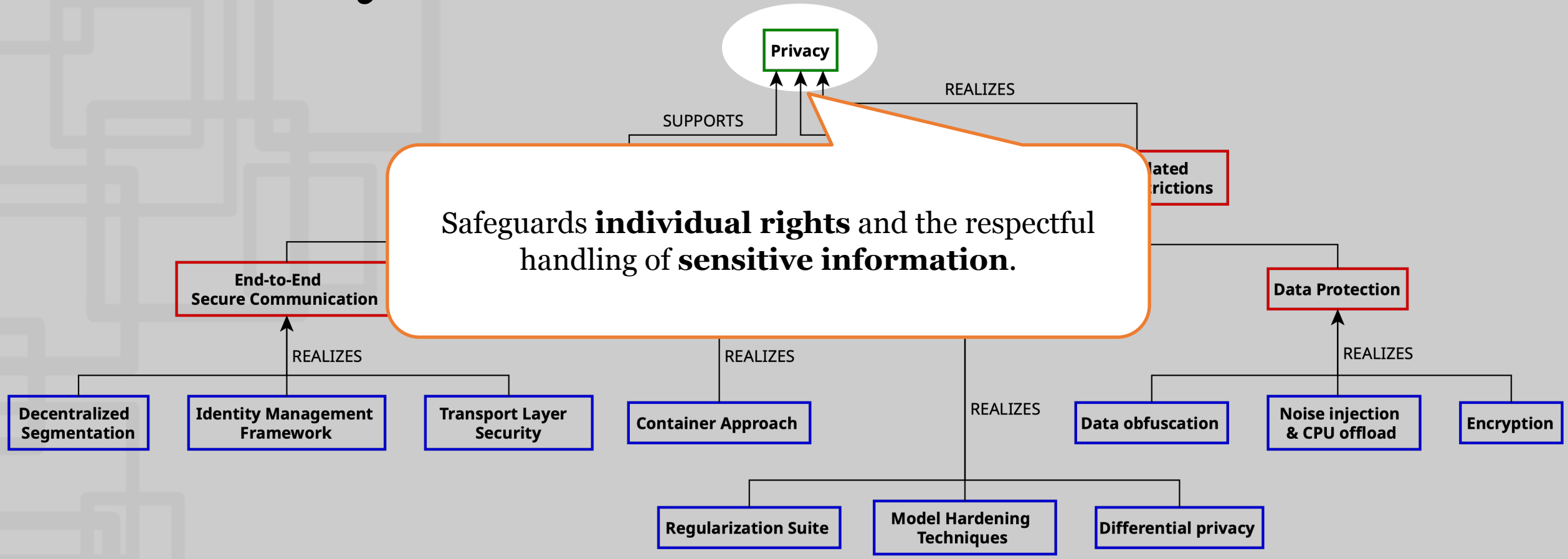
Replication Package

Privacy



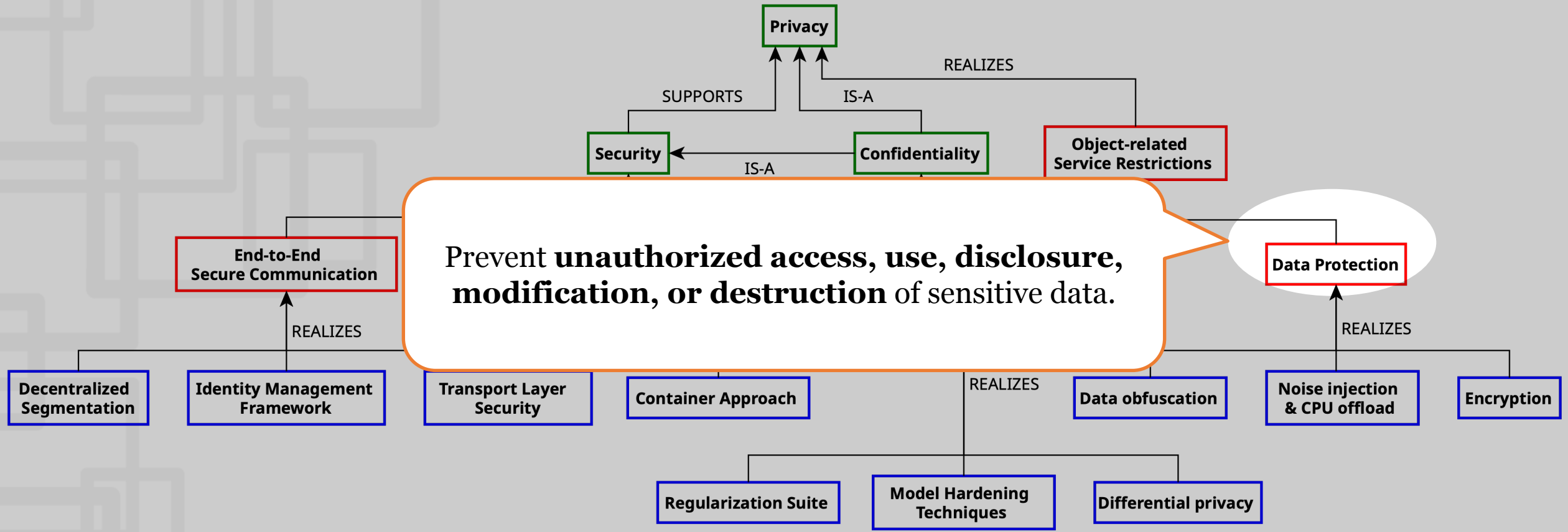
GRAN SASSO SCIENCE INSTITUTE

Privacy



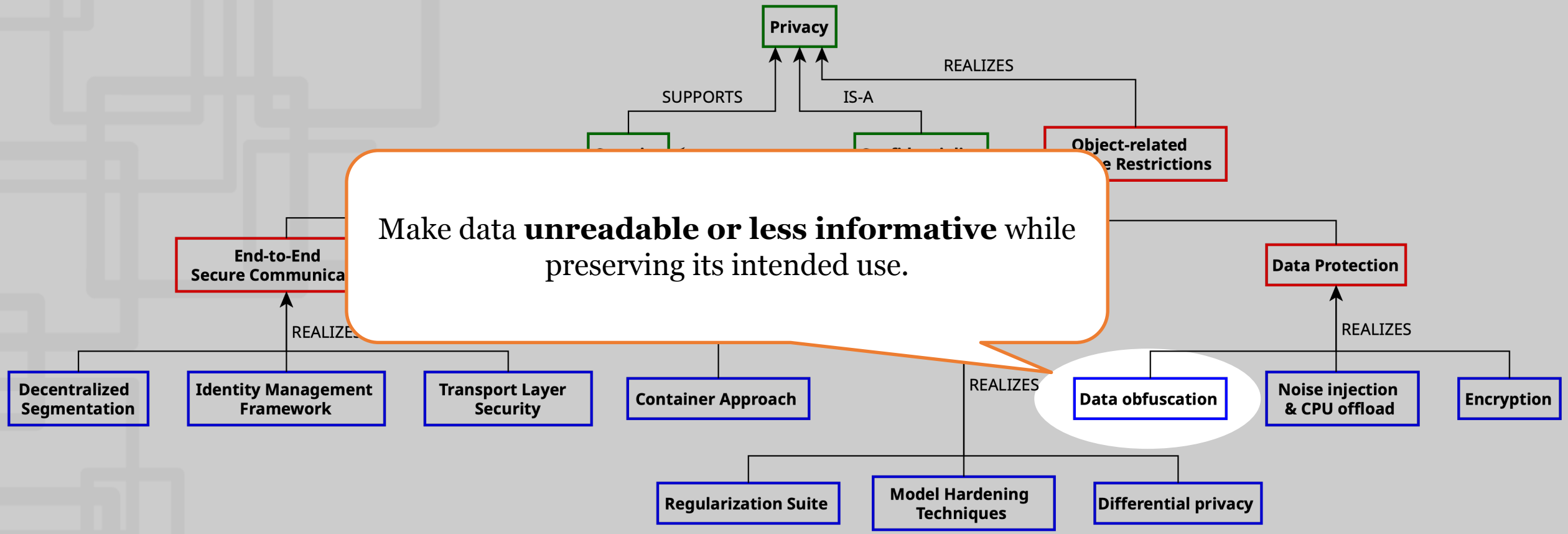
GRAN SASSO SCIENCE INSTITUTE

Privacy



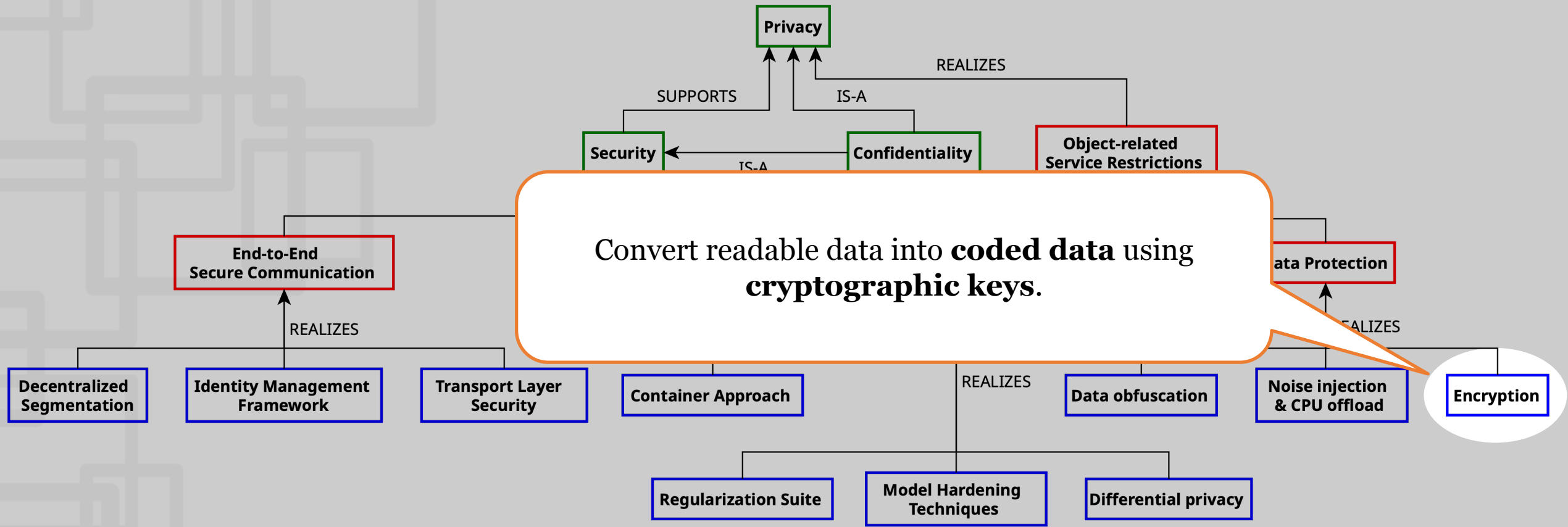
GRAN SASSO SCIENCE INSTITUTE

Privacy



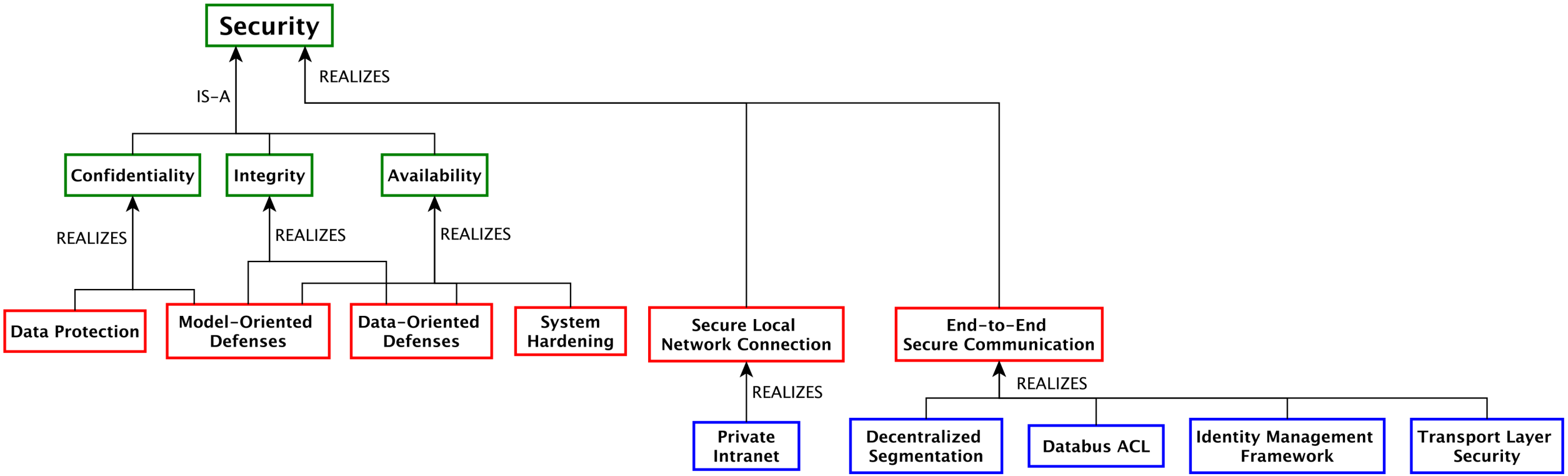
GRAN SASSO
SCIENCE INSTITUTE

Privacy



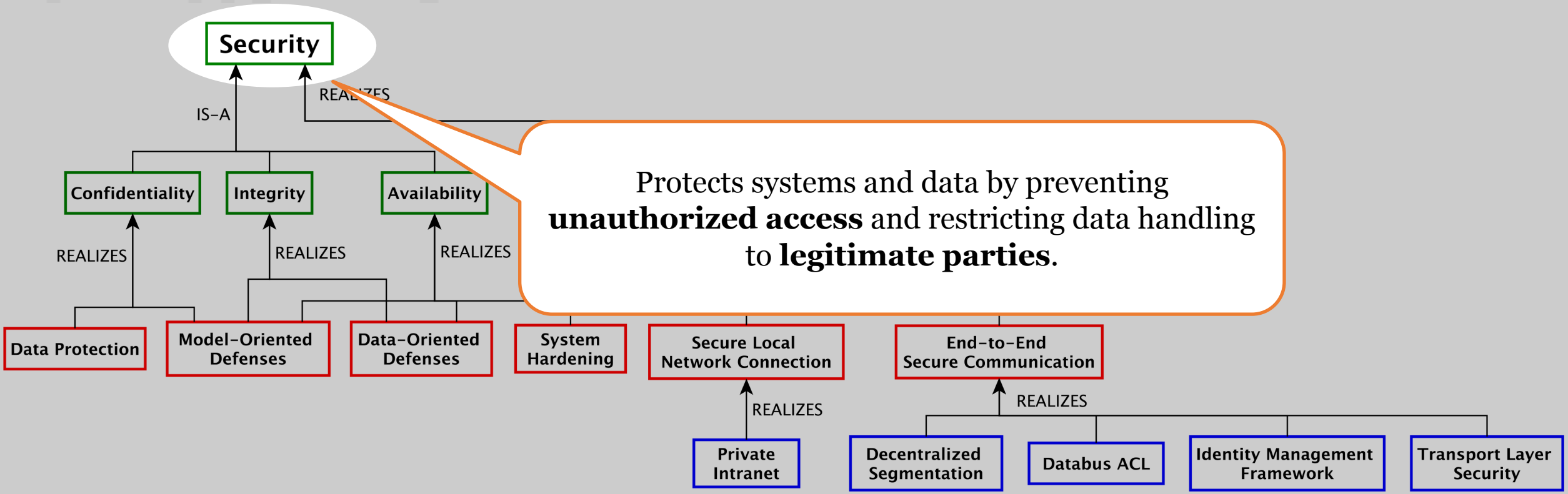
GRAN SASSO SCIENCE INSTITUTE

Security



GRAN SASSO SCIENCE INSTITUTE

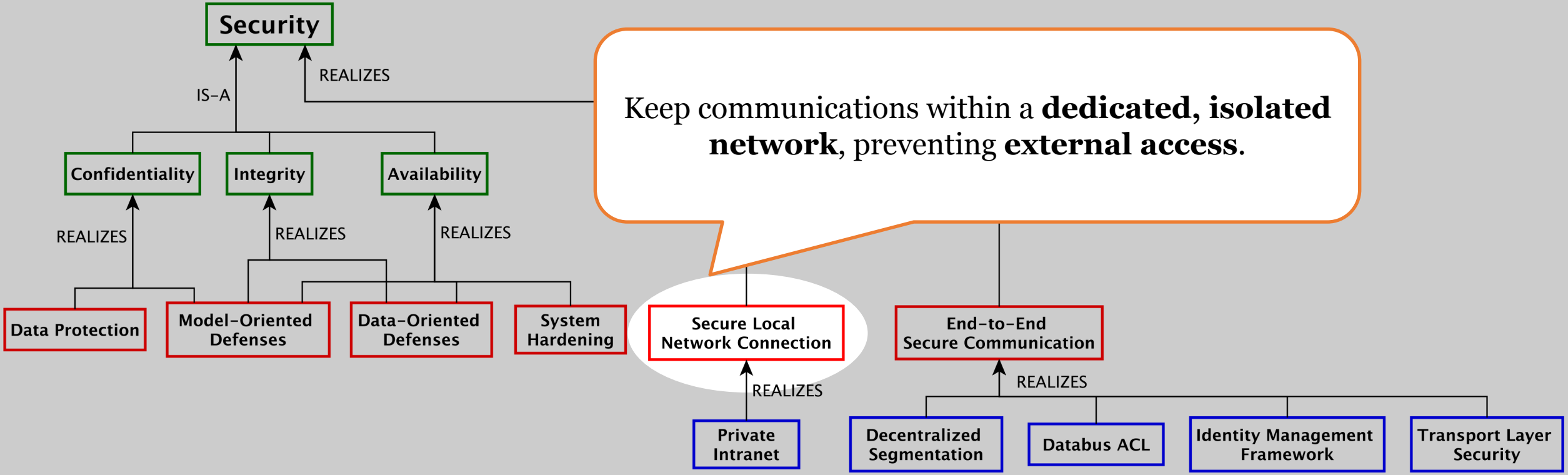
Security



Protects systems and data by preventing **unauthorized access** and restricting data handling to **legitimate parties**.

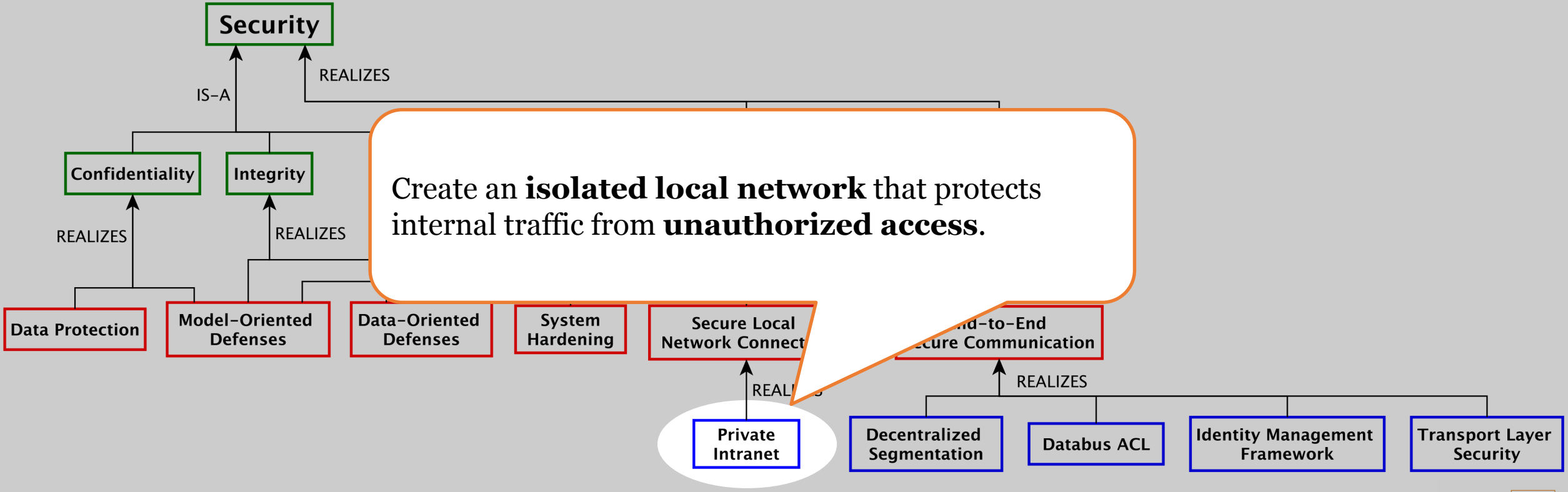
GRAN SASSO SCIENCE INSTITUTE

Security



GRAN SASSO SCIENCE INSTITUTE

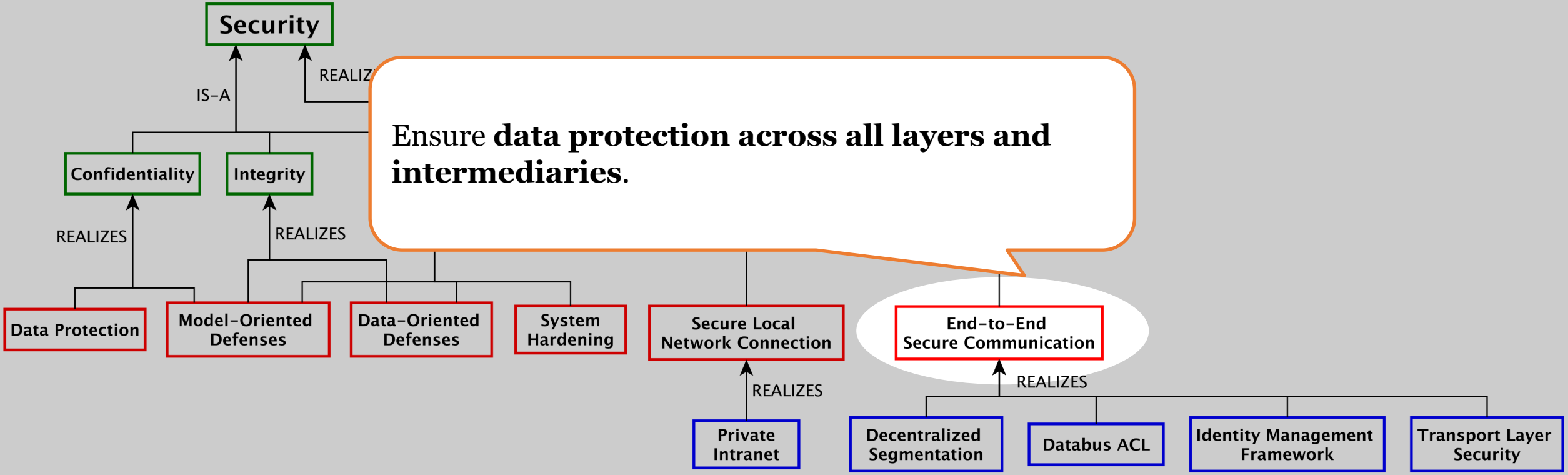
Security



Create an **isolated local network** that protects internal traffic from **unauthorized access**.

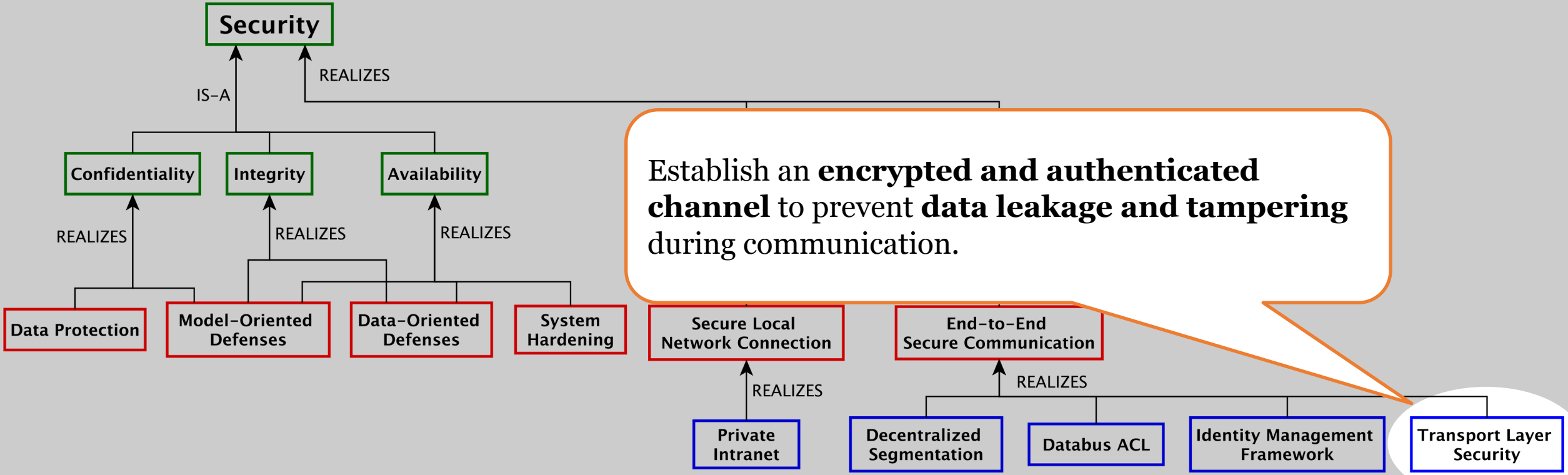
GRAN SASSO SCIENCE INSTITUTE

Security



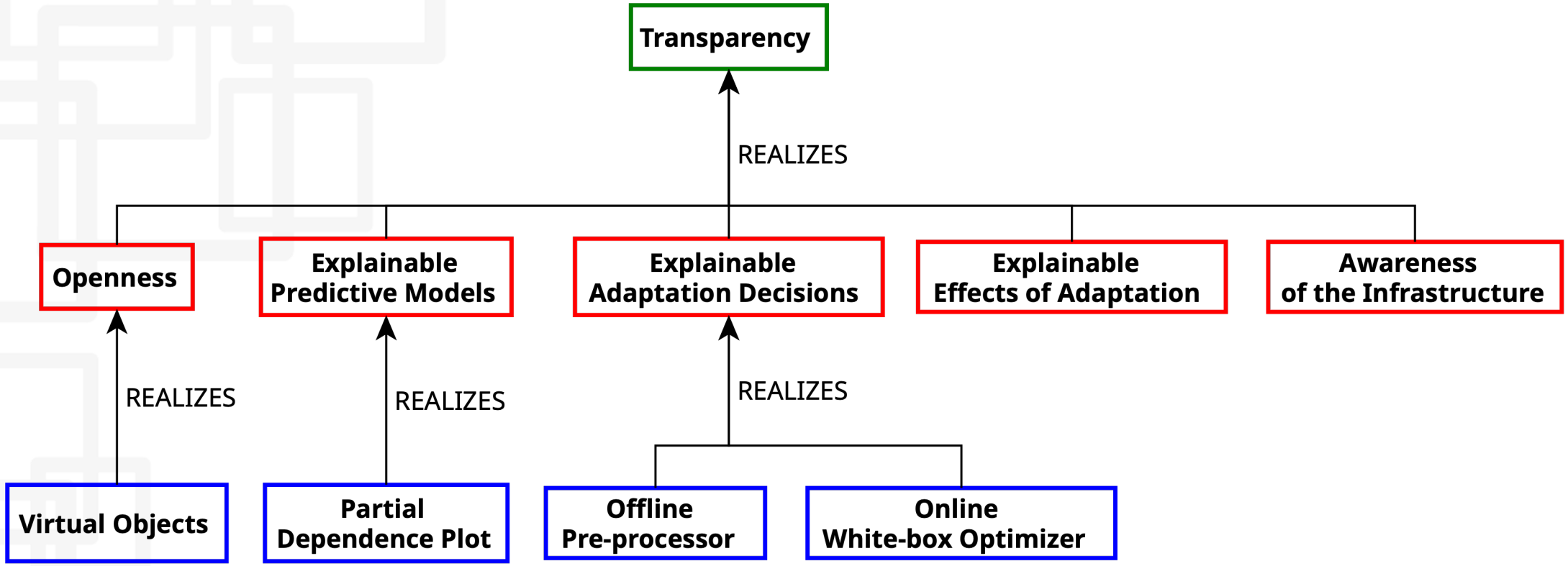
GRAN SASSO SCIENCE INSTITUTE

Security

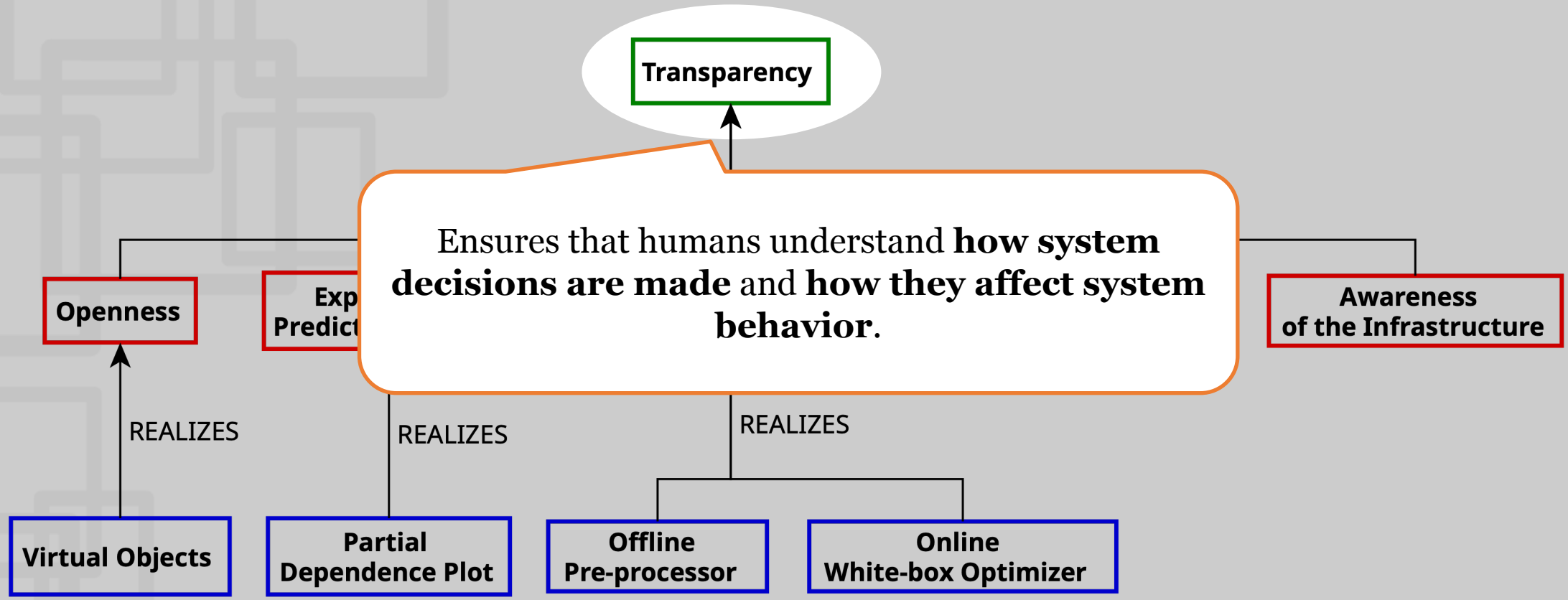


GRAN SASSO SCIENCE INSTITUTE

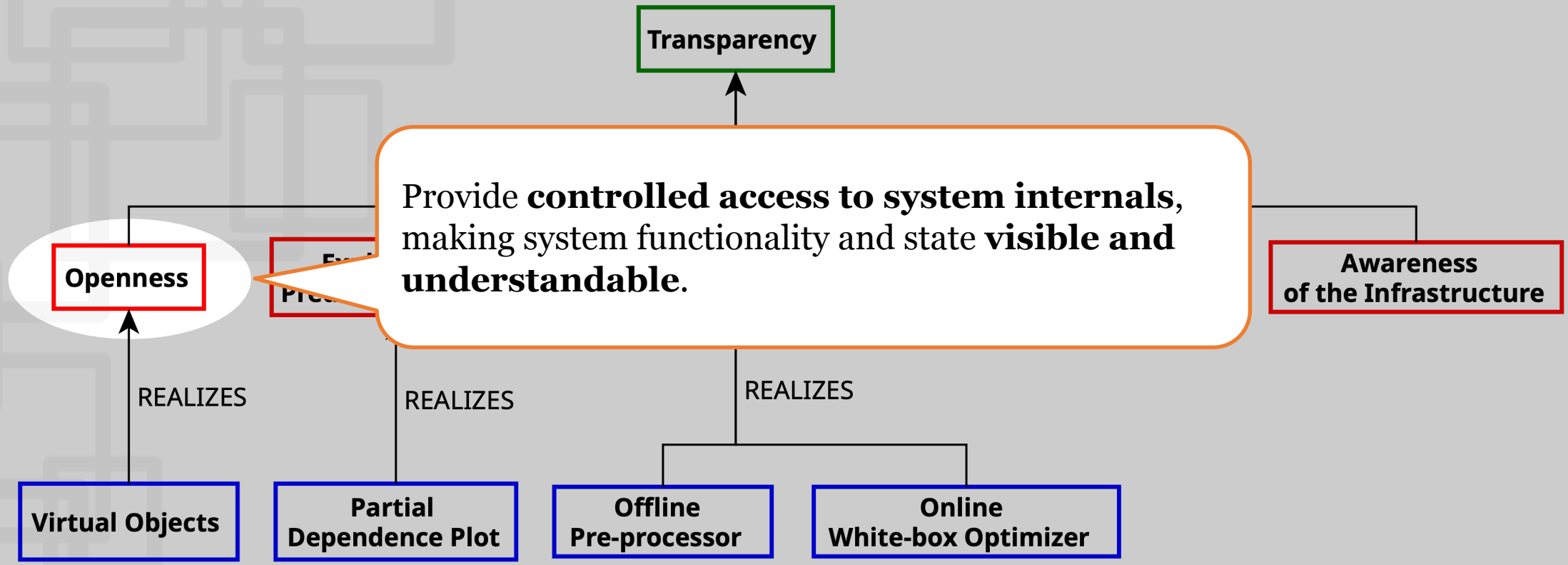
Transparency



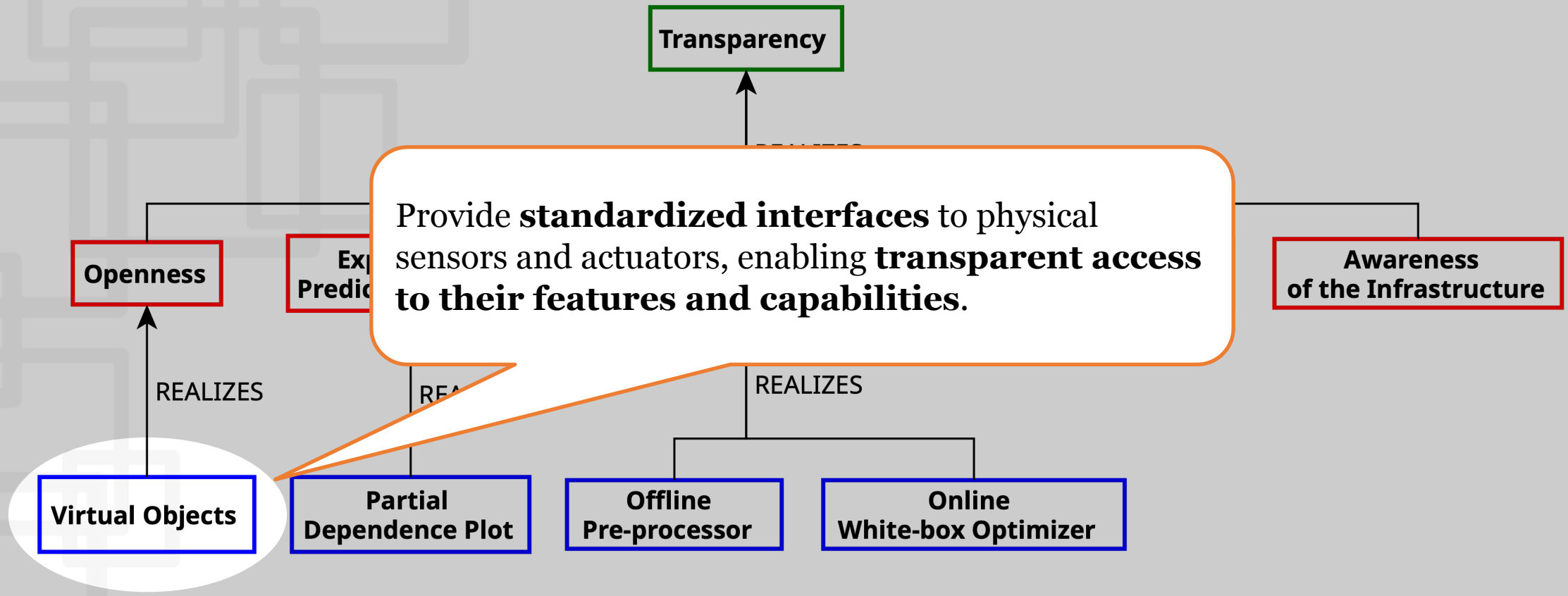
Transparency



Transparency



Transparency



Provide **standardized interfaces** to physical sensors and actuators, enabling **transparent access to their features and capabilities**.

GRAN SASSO SCIENCE INSTITUTE

Patient Monitoring System

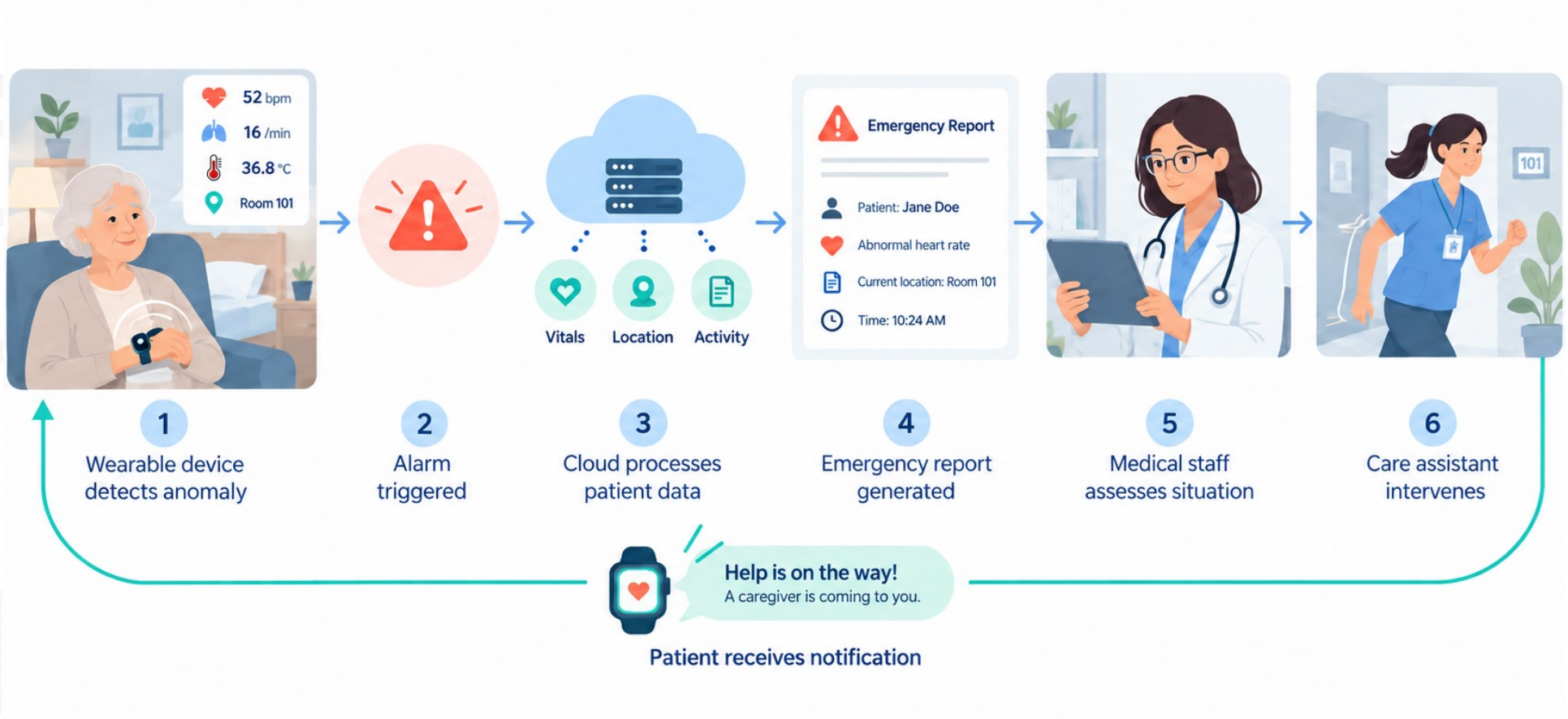
Context

- An assisted-living facility where patients are monitored through **wearable devices** collecting their location and vital parameters.
- The system involves a **cloud infrastructure**, the **head of medical staff**, and **care assistants**.

BPMN Representation

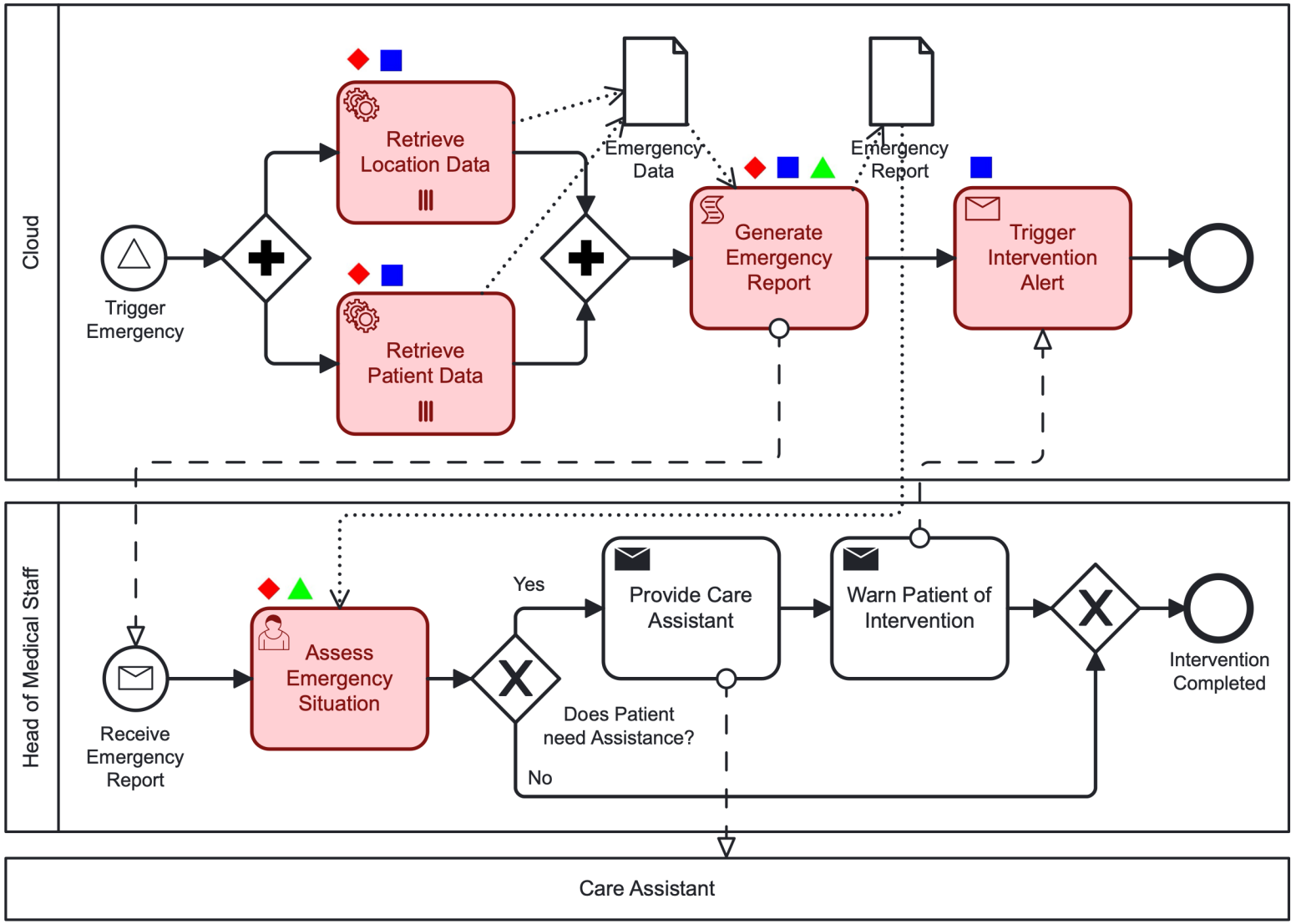
- The patient monitoring process is modeled using **Business Process Model and Notation (BPMN)** to represent its activities, events, and decisions.

Patient Monitoring System



GRAN SASSO SCIENCE INSTITUTE

BPMN Diagram



- Privacy
- Security
- Transparency

GRAN SASSO SCIENCE INSTITUTE

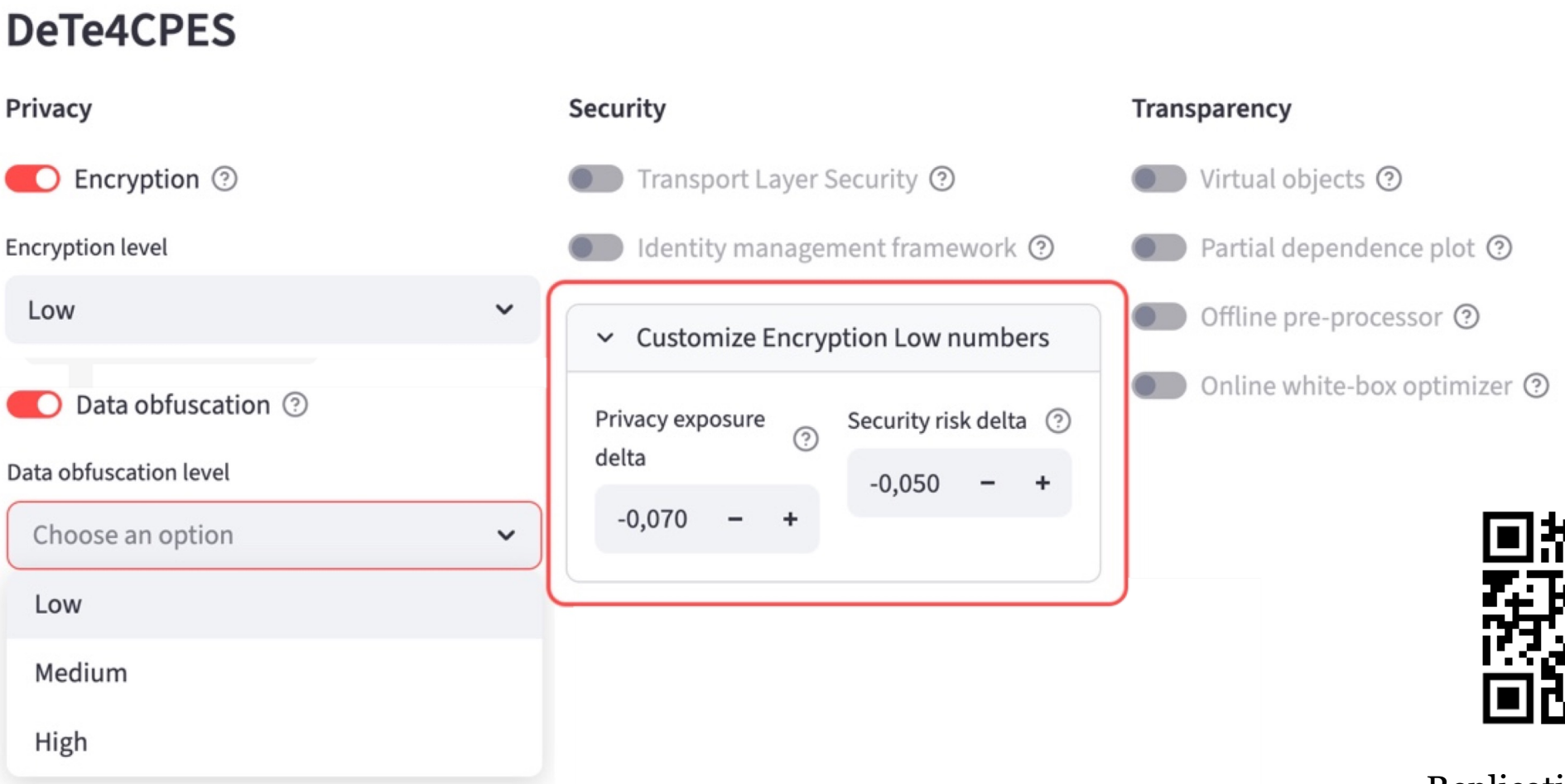
Mapping Shortcomings to BPMN

BPMN Activity	W1 Privacy	W2 Security	W3 Transparency
Retrieve Location Data	✓ Patient profiling without anonymization	✓ Data are sent over un-encrypted channels	–
Retrieve Patient Data	✓ Patient profiling without anonymization	✓ Data are sent over un-encrypted channels	–
Generate Emergency Report	✓ Use of personal and medical data	✓ The report could be manipulated	✓ Patient is unaware of which data is used
Trigger Intervention Alert	–	✓ An attacker could trigger the intervention alert	–
Assess Emergency Situation	✓ Access to personal and medical data	–	✓ Patient is unaware of emergency strategies

Addressing Ethical Shortcomings

Weakness	Design Objective (DESO)	Design Technique (DEST)
W1 Privacy	+ Data Protection	+ Encryption + Data Obfuscation
W2 Security	+ End-to-End Secure Communication + Secure Local Network Connection	+ Transport Layer Security + Private Intranet
W3 Transparency	+ Openness	+ Virtual Objects

Prototype Implementation



Replication Package

GRAN SASSO SCIENCE INSTITUTE

Lessons Learned

- Ethics-related requirements require **intermediate design concepts**.
- Privacy, security, and transparency are **interdependent**.
- Suitable design techniques depend on the **application context**.
- Ethics-related limitations can be identified in concrete **system activities**.
- Quantitative indicators require **careful interpretation**.

Conclusion

Contributions

- Identification of **ethical shortcomings** in CPS design.
- **DeTe4CPES** — a conceptual approach for integrating ethics-based requirements into CPS design.
- Application of **DeTe4CPES** to a **patient monitoring use case**.
- Development of **a prototype tool** supporting automated analysis.

Future work

- Apply design techniques to **other CPS scenarios**.
- Automate **quantitative evaluation** through monitored metrics.

Thank you for your attention!

Questions?

LinkedIn

yelyzaveta.kurkchi@gssi.it

GRAN SASSO SCIENCE INSTITUTE