Designing Secure and Dependable Banking Security Systems

ABISERVIZI
ABI EVENTI
ABI Associazione Bancaria Italiana

Flavio Frattini

flavio.frattini@rislab.it

rislab
Laboratorio di Ricerca e Innovazione per la Sicurezza

ESSERE AL SICURO

The question

Assets **protected** by a **secure** and **dependable** system

How to *properly* protect our sites (i.e. bank branches)?

- We need to *properly* **design** the banking security system (BSS) by considering all the topics related to *dependability*, *physical security*, *cyber security*, and *cyber-physical security*
- And to **assess** the proposed design, and the resulting implementation

Let's approach scientifically the problem of protecting our sites with a *secure* and *dependable* security system

Research and Innovation for Security Lab

3 main goals:

1. carry out both basic and applied **scientific research** to support
2. the **development** and
3. the **commercialization**

of innovative digital products to protect business and critical infrastructures, goods and people, in a wide sense

rislab: Team

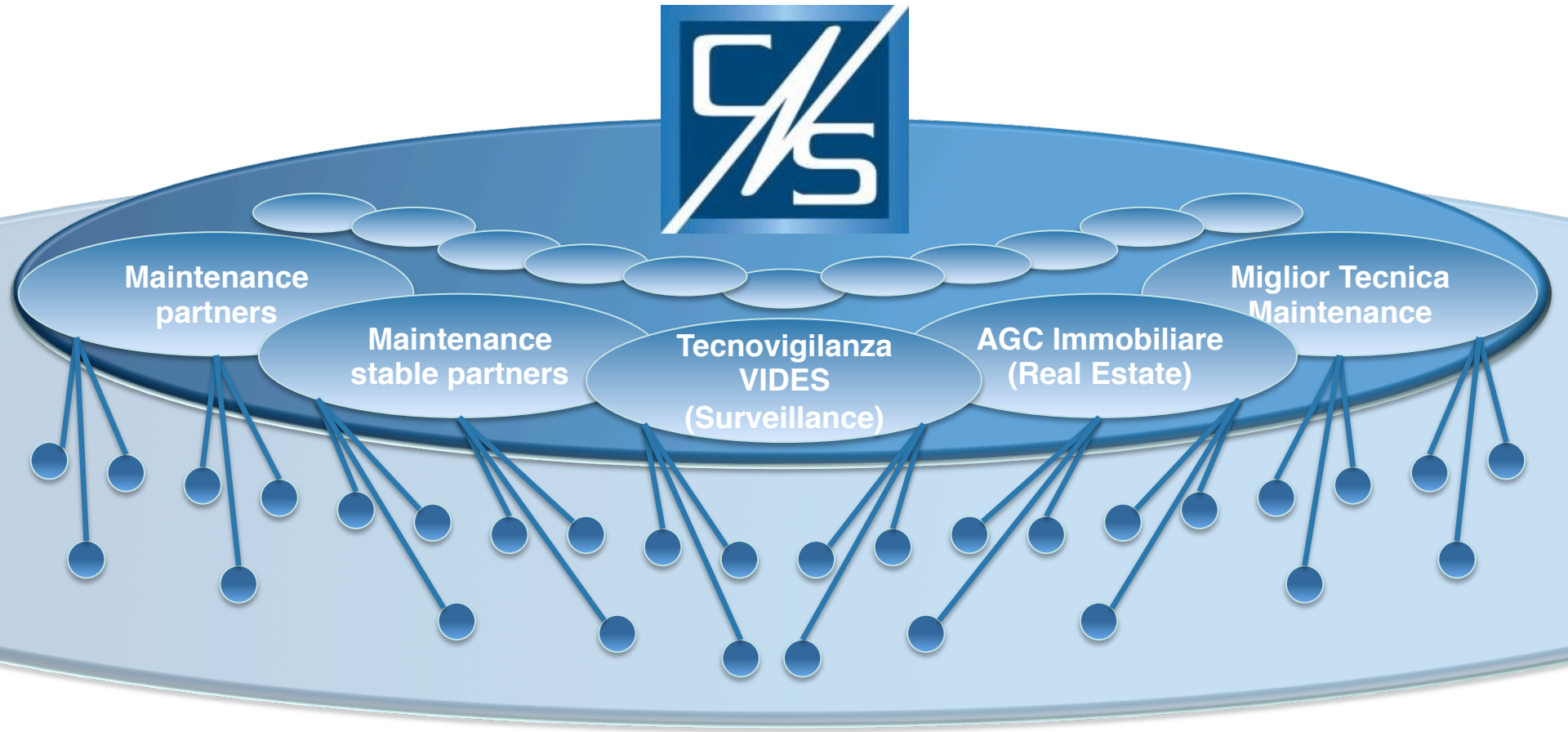
Research activities of RISLAB are carried out by a highly qualified staff with a long-lasting experience in research and/or physical security systems

- RISLAB has a **Scientific and Technical Committee** supervised by **Giorgio Ventre**, PhD, full professor, Head of Electrical Engineering and Information Technology Department at the Federico II University of Naples
- The **manager of research** activities is **Flavio Frattini**, PhD in Computer Engineering from Federico II University of Naples

- The personnel includes PhDs, computer engineers, and electronic engineers with a long-lasting experience in the security field

RISLAB main customer: CNS

SOCIETÀ CONSORTILE A R.L. – Consorzio Stabile *(Permanent Consortium)*



CNS employees: 76

Overall group employees: ~300

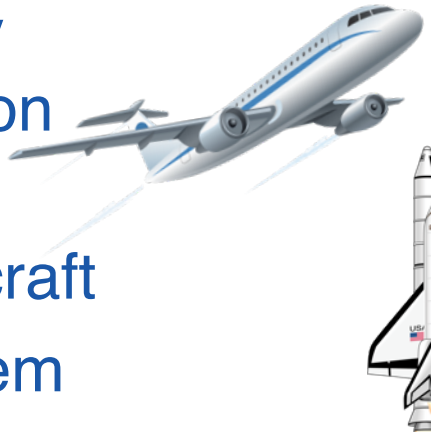
***Lean Six Sigma* Methodology**

8 OFFICES

NAPOLI, CASANDRINO, ROMA, MONZA, BOLOGNA, BAT, PERUGIA, ALESSANDRIA

Critical Systems

- Mission Critical Systems are those systems for which failures cannot be admitted since they may be critical for the success of their mission
  - E.g., monitoring systems in banking and transportation, control systems in spacecraft
- Depending on the domain, failures in a system are
  - **Safety Critical** when they hamper human life
  - **Business Critical** when they affect essential operations that dramatically impair company affairs



Outline

- Context
- RisLab & CNS
- The subject: Critical System
- Goals:
  - Security
  - Dependability
- Security System Design
- Conclusions

Security

Security: an integrated system of systems, activities, programs, equipment, personnel, and policies for the protection of critical systems, information, people; it rests on:

- **Confidentiality**: concealment of information or resources
- **Integrity**: trustworthiness of data or resources
- **Availability**: the ability to use the information or resource desired

- M. Bishopp – Computer Security: Art and Science – Addison-Wesley Professional, 2003

Dependability

Dependability: an integrating concept encompassing the following attributes

- **Availability**: the ability of an item to be in a state to perform a required function at a given instant of time
- **Reliability**: the ability of an item to perform a required function for a given time interval
- **Safety**: the absence of catastrophic consequences of a failure on the users and on the environment
- **Integrity**: the absence of improper system alterations
- **Maintainability**: the ability of a system to be maintained, usually if a failure occurs, by means of a repair strategy

- ITU (International Telecommunication Union) – Recommendation E.800 (09/08)
- Avizienis, A., Laprie, J.-C., Randell, B., and Landwehr, C. – Basic concepts and taxonomy of dependable and secure computing – IEEE Transactions on Dependable and Secure Computing, 1(1), 2004

Outline

- Context
- RisLab & CNS
- The subject: Critical System
- Goals
- Security System Design
  - *Deter-Detect-Delay-Respond*
  - Current architecture
  - Design steps
- Conclusions

Deter-Detect-Delay-Respond

- **Deter**: discourage an adversary from attempting an assault by making a successful assault appear very difficult or impossible
- **Detect**: determining that an unauthorized action is occurred or is occurring; detection includes sensing the action, communicating the alarm to a control center, and assessing the alarm
- **Delay**: impeding an adversary penetration into or exit from the protected area
- **Response**: counteracting adversary activity and interrupting the threat

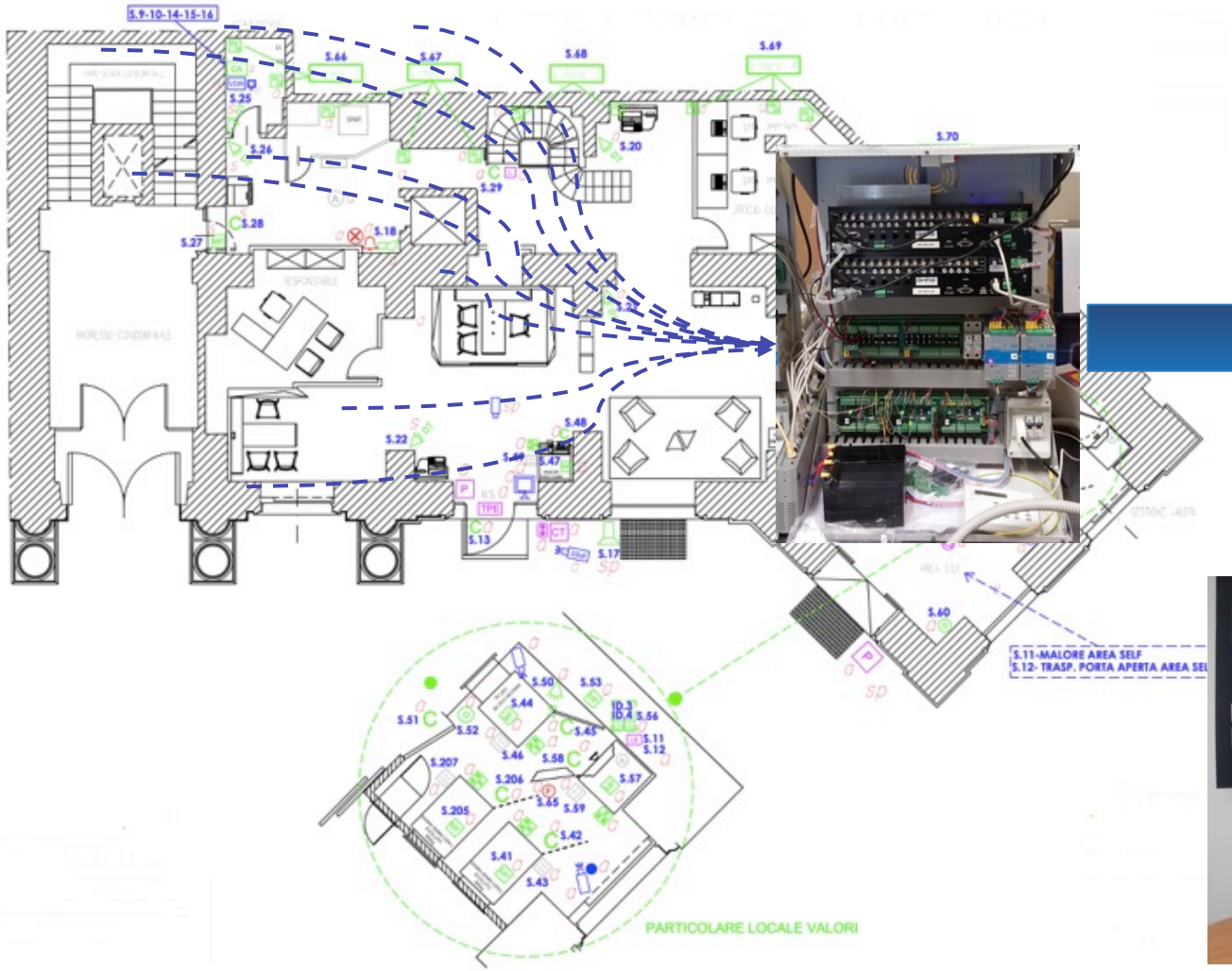
Bank Threats

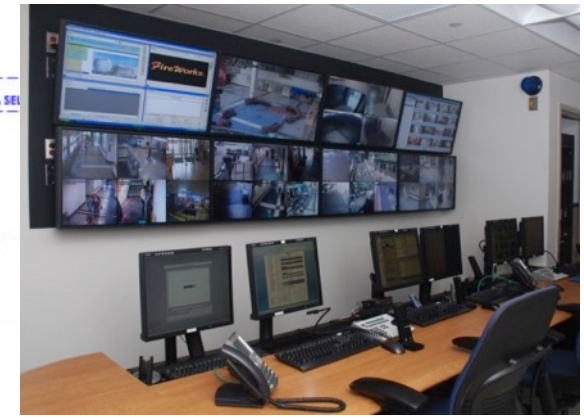
- What can happen in banks?
  - Robberies
  - Burglaries
  - Larcenies

…and Vulnerabilities

- **Of the assets**:
  - Whatever opening to the outside
  - Communication system (physical attack)
  - Authorization management (access codes, passwords, …)
  - …
- **Of the protection system**:
  - Insufficient software testing
  - Devices (Sensors, cables, concentrators, control panels, etc.)
    - Failures, outdated
  - Cyber-attacks
    - Communication systems (cyber attack)
    - Authentication and authorization (access to control panel)
  - …

Current System



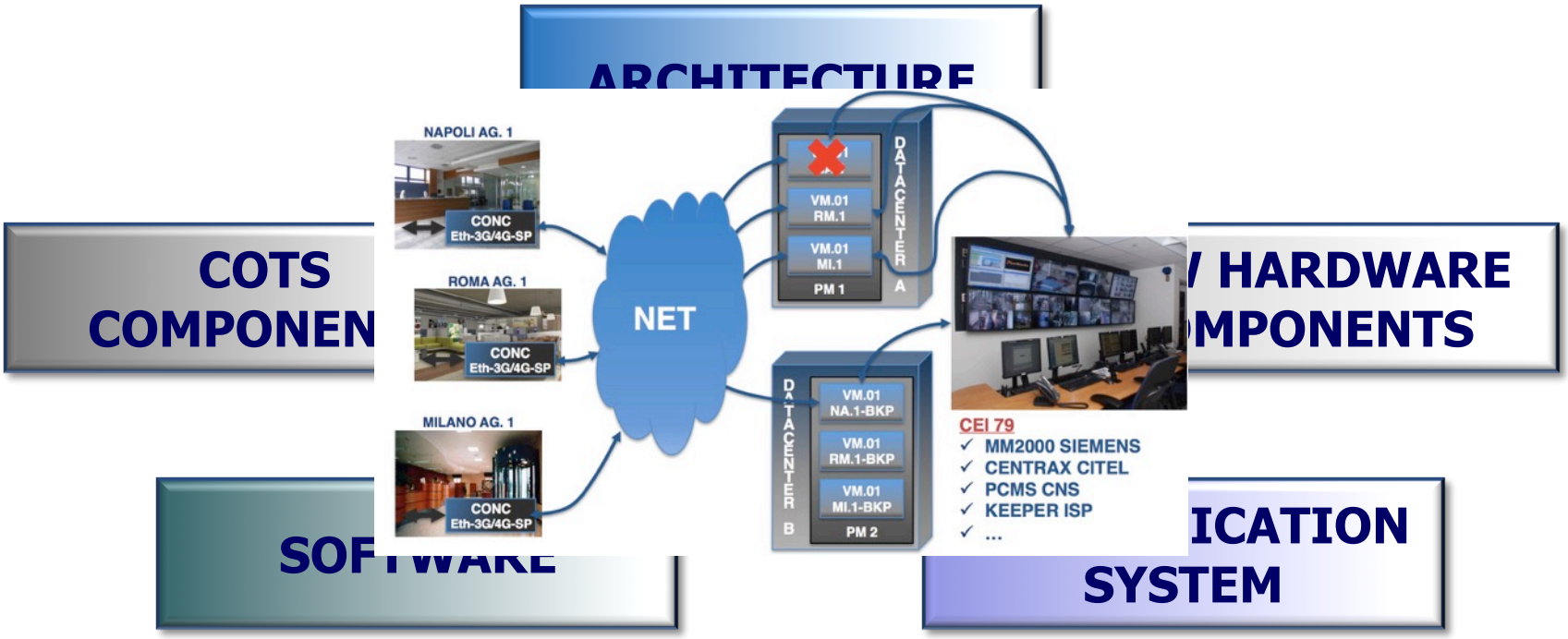


Starting from existing systems…

- Identify issues:
  - Known faults
  - Failure modes
  - Known attacks

- This is performed through field data analysis
  - System logs
  - Application logs
  - User reports

Hypothesis



Approach

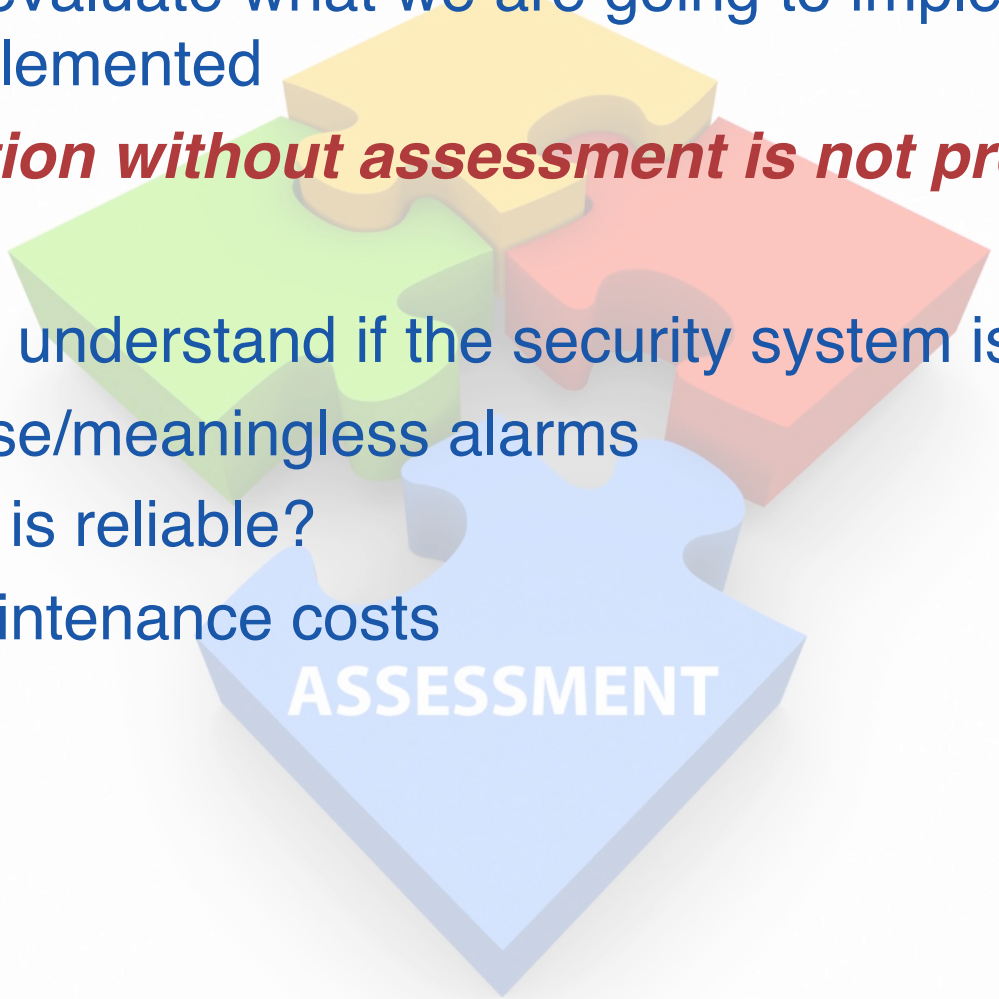
Question ⇒ Hypothesis ⇒ Assessment

Assessment

- We have to evaluate what we are going to implement and what we have implemented

Protection without assessment is not protection

- It is useful to understand if the security system is effective
- What are false/meaningless alarms
- How much it is reliable?
- Estimate maintenance costs



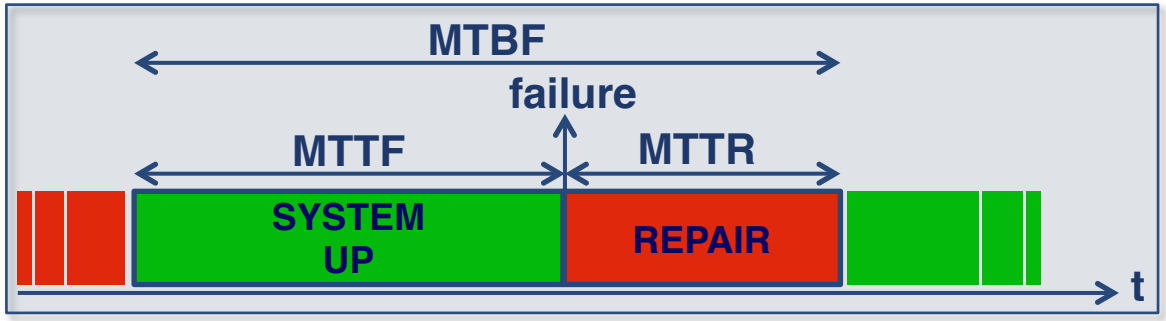
- M. Garcia – Design and Evaluation of Physical Protection Systems, 2nd Edition – Butterworth-Heinemann, 2007

Performance Assessment

- **Detection**
  - ✓ Probability of detection
  - ✓ Time for communication and assessment
  - ✓ Frequency of false alarms
- **Delay**
  - ✓ Time to defeat obstacles
- **Response**
  - ✓ Probability of accurate communication to operations center
  - ✓ Time to communicate
  - ✓ Time to deploy
  - ✓ Response force effectiveness

Dependability Assessment

- ✓ **Mean Time to Failure**
- ✓ **Mean Time to Repair**



- ➢ **Model based**
  - During the design phase, modeling is used for estimating how much a system is dependable
  - It requires being note (or the previous evaluation of) how much each component is dependable
- ➢ **Measurement based**
  - Once the system has been implemented and it is operational (at least in β-testing), actual values from the field can be used for quantifying its dependability

- F. Frattini et al. – Reliability Indices – Wiley Encyclopedia of Operations Research and Management Science, 2013

Outline

- Context
- RisLab & CNS
- The subject: Critical System
- Goals
- Security Systems Design
- Conclusions

Conclusions

- Objectives of a banking security system seems to be clear; **there are still many issues**, however
- The ***proper design*** of a system, encompassing both *security* and *dependability* attributes, and based on an engineered approach, is essential to improve efficiency and effectiveness
- The presentation introduced (briefly, very briefly…) the **steps** we followed for realizing a secure and dependable BSS
- Only with this scientific approach allows building **very dependable and secure** security systems for critical environments that
  - **Increase the MTBF**
  - **Reduce maintenance costs, time, and required expertise**
  - **Make the asset really secured**

Thank you!

ABISERVIZI ABI EVENTI

ABI Associazione Bancaria Italiana

rislab
Laboratorio di Ricerca e Innovazione per la Sicurezza

ESSERE AL SICURO

flavio.frattini@rislab.it