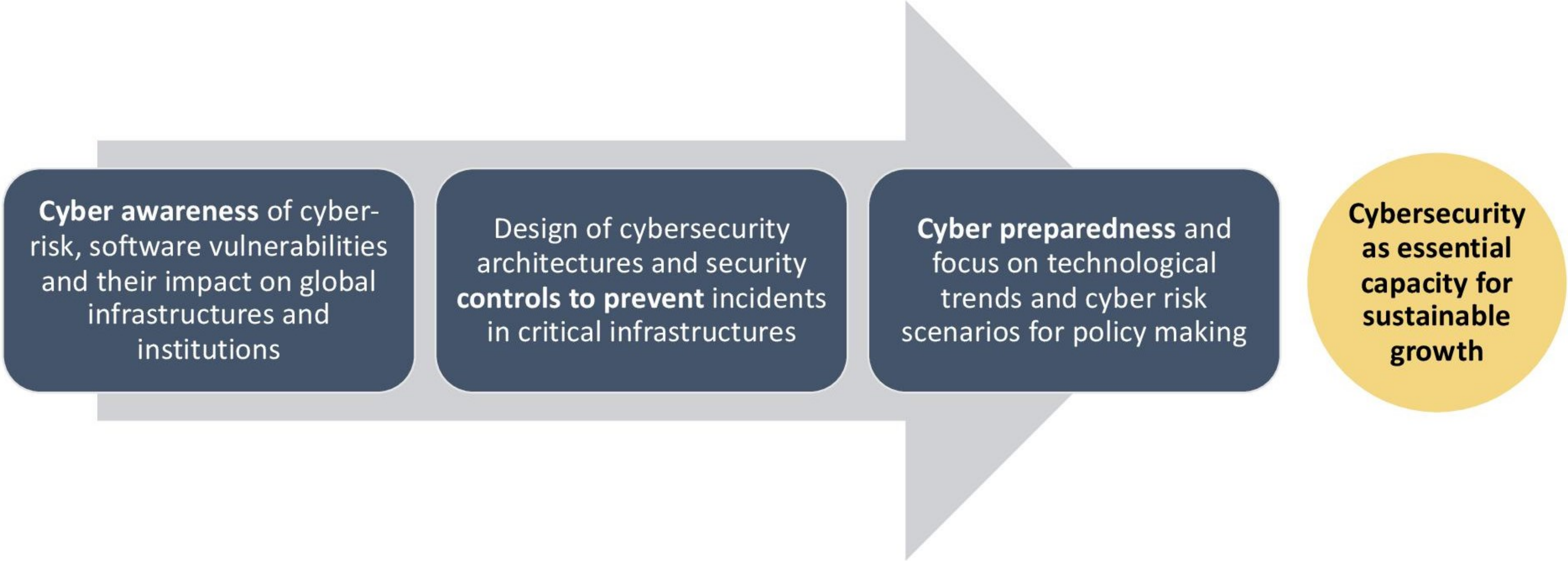
CYBER RESILIENCE

VINCENZO CALABRÒ

Il valore della cyber resilienza



Cyber awareness of cyber-risk, software vulnerabilities and their impact on global infrastructures and institutions

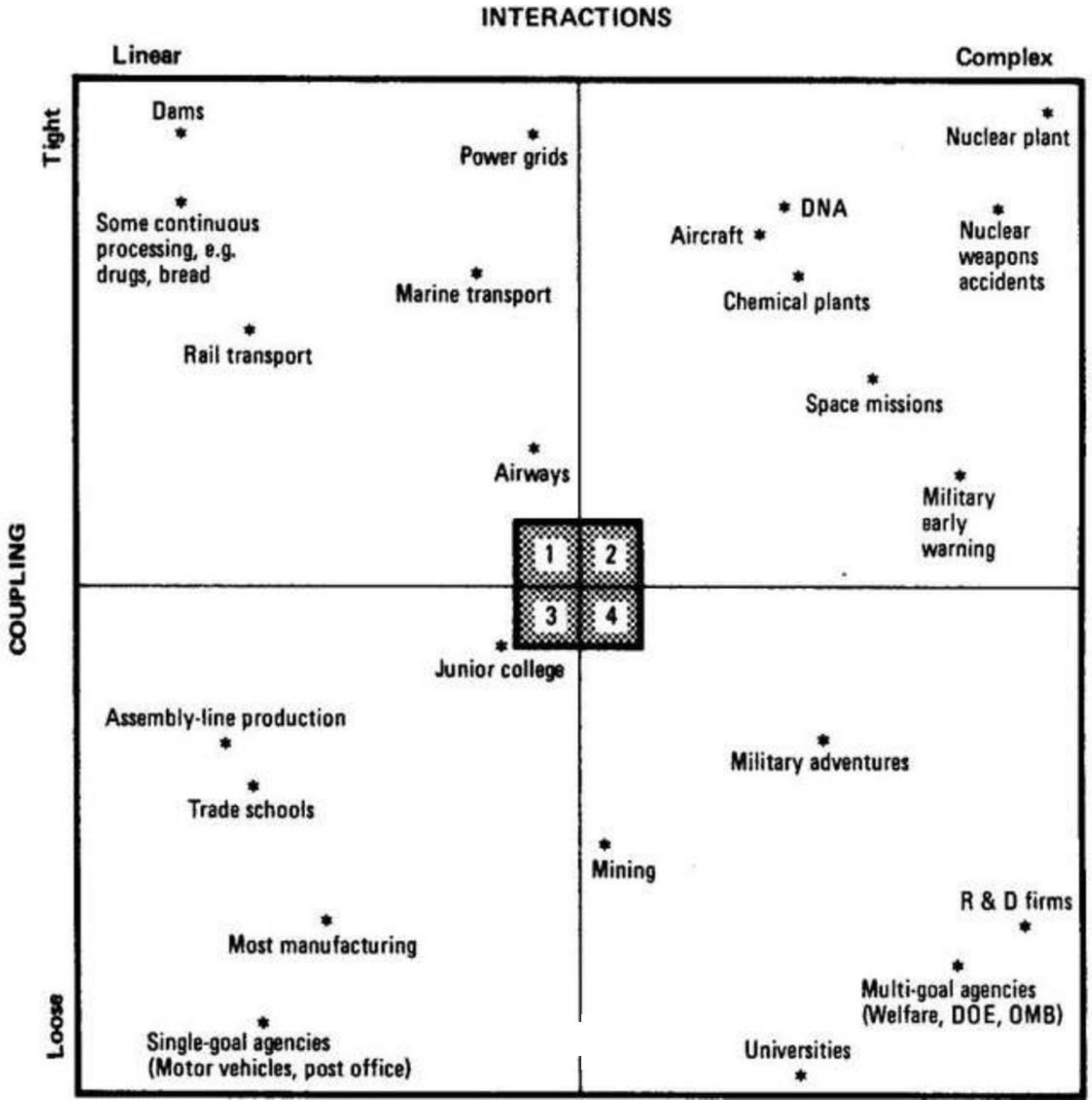
Design of cybersecurity architectures and security **controls to prevent** incidents in critical infrastructures

Cyber preparedness and focus on technological trends and cyber risk scenarios for policy making

Cybersecurity as essential capacity for sustainable growth

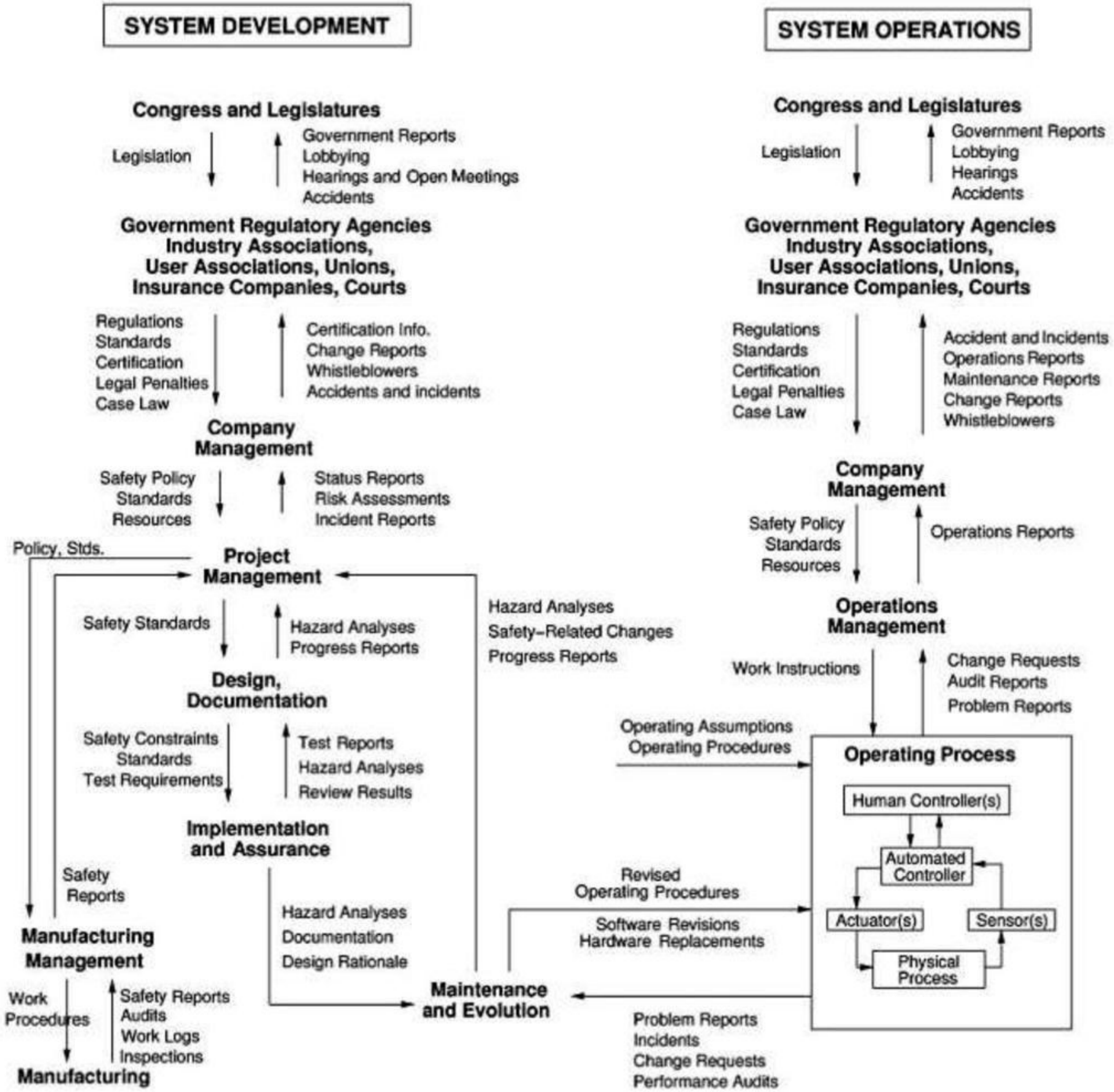
Normal Accident Theory

- Interactive complexity and tight coupling of technological systems
- Localized failures spread/disrupt/damage larger systems
- System accidents are inevitable or "normal"



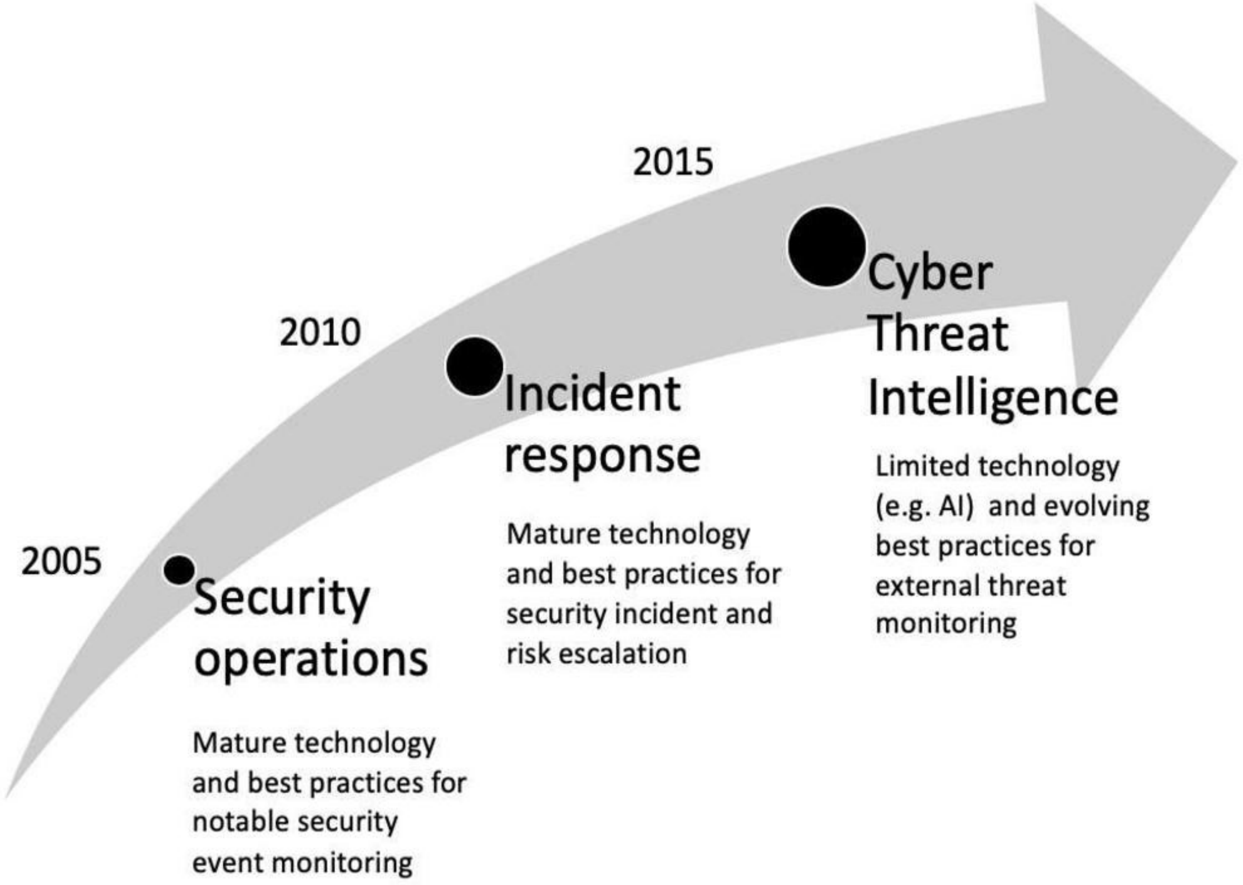
Safety Engineering

- The problem of ensuring safety can be stated as a *control problem* rather than a component failure problem
- accidents occur when component failures, external disturbances, and/or dysfunctional interactions among system components are not adequately controlled or handled



Le capacità organizzative per la cyber resilienza

- Capacità di prevenire incidenti attraverso controlli di sicurezza a carattere deterrente e preventivo
- Capacità di risposta per ridurre l'impatto di incidenti con azioni che limitano i danni provocati da databreach (es. detection, incident management)
- Capacità di innovazione per adattarsi all'ambiente e alle nuove minacce



2005 Security operations

Mature technology and best practices for notable security event monitoring

2010 Incident response

Mature technology and best practices for security incident and risk escalation

2015 Cyber Threat Intelligence

Limited technology (e.g. AI) and evolving best practices for external threat monitoring

Le sfide per una efficace resilienza cyber

FORMAZIONE

- *Pratiche gestionali «agili»* da adattare al contesto
  - Security studies and capacity building; Criminal law and GDPR; Organizational processes and practices; Security economics and behavior; Technologies for data security
- *Agilità* a livello strategico, tattico e operativo
  - Softskills per bricolage, improvisation, hacking (es. design thinking)
  - Enterprise architecture maintenance and evolution (es. scenario modelling)

TRAINING

- *Collective mindfulness* nel controllo delle operation
  - Preoccupation with failure, Reluctance to simplify, Sensitivity to operations, Commitment to resilience, Deference to experience
  - Active defense: digital twins, sandboxes, AI, etc.
- Capacità di *gestione delle crisi*
  - Fragmented coordination
  - Scenario based training for situational understanding

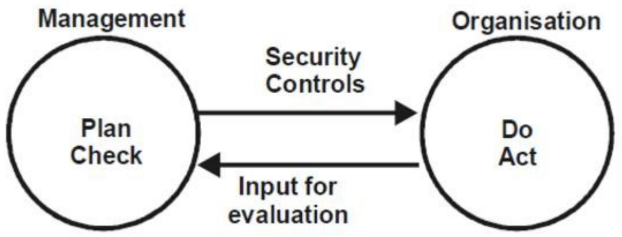


Figure 1.Common stages of an ISMS

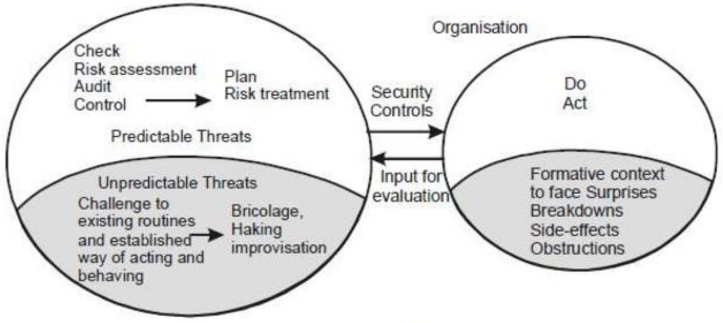


Figure 3.The duality of IS security

Spagnoletti and Resca 2008

GRAZIE

VINCENZOCALABRO.IT