



The SEMA referential framework:

Avoiding ambiguities in security and safety issues

March 16th 2010, CIP 2010, Washington D.C.

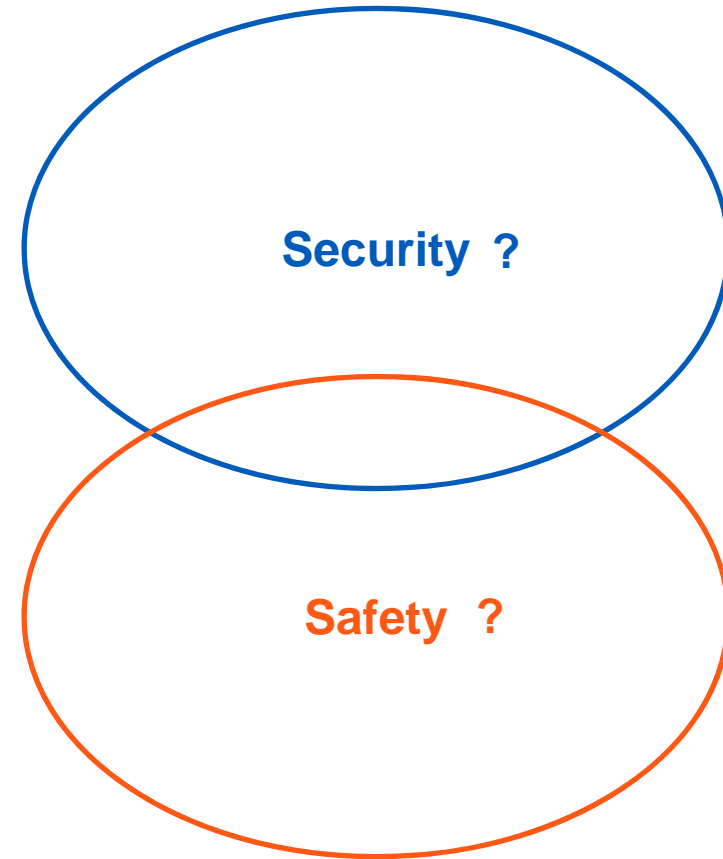
Ludovic Piètre-Cambacédès



LEADING THE ENERGY CHANGE



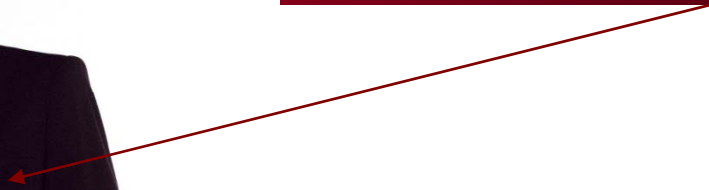
Cyber security of ICS (Industrial Control Systems)



Different contexts...
...different meanings



Sécurité - Safety







A (very) confusing situation

▶ A surprising diversity

- Norms & standards from different sectors
- Scientific and technical literature
 - ⇒ Dozens of different definitions, plus related/umbrella terms

▶ Language traps

- A unique word in many languages... E.g. in Europe:

 Spanish	<i>Seguridad</i>	
 Swedish	<i>Säkerhet</i>	
 English	<i>Safety</i>	<i>Security</i>
 French	<i>Sûreté</i>	<i>Sécurité</i>

Towards the SEMA referential framework

- ▶ CIP, particularly prone to safety/security terminological traps
 - Multi-domains, multiple engineering disciplines
 - International (e.g. ECI, European Critical Infrastructures)
- ▶ A need for disambiguation
 - In early stage projects, collaboration, policy making
 - For risk assessments perimeter definition
 - Myriad of definitions, but nothing really helpful...
- ▶ The key ideas of SEMA
 - Giving up absolute definitions, reasoning on distinctions
 - System – Environment (SE) & Malicious – Accidental (MA)

Avoiding equivocation about safety & security

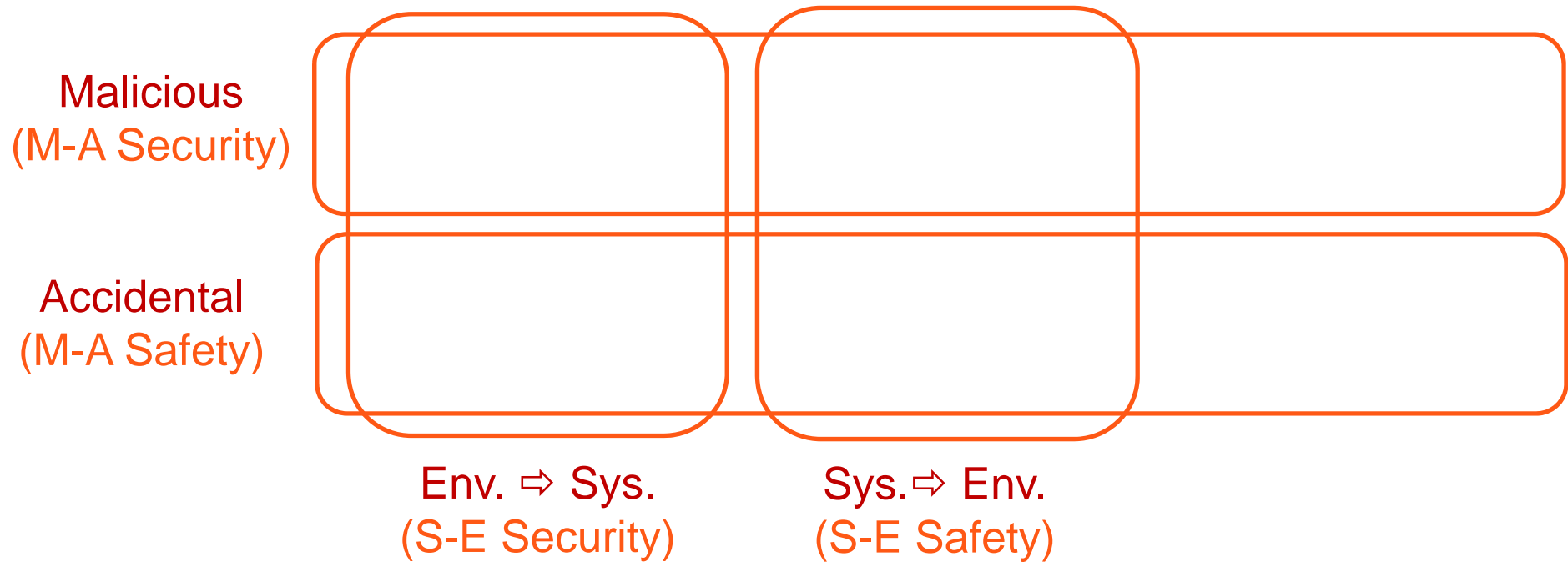
Malicious
(M-A Security)

An empty rounded rectangular box with a thin orange border, positioned to the right of the 'Malicious (M-A Security)' label.

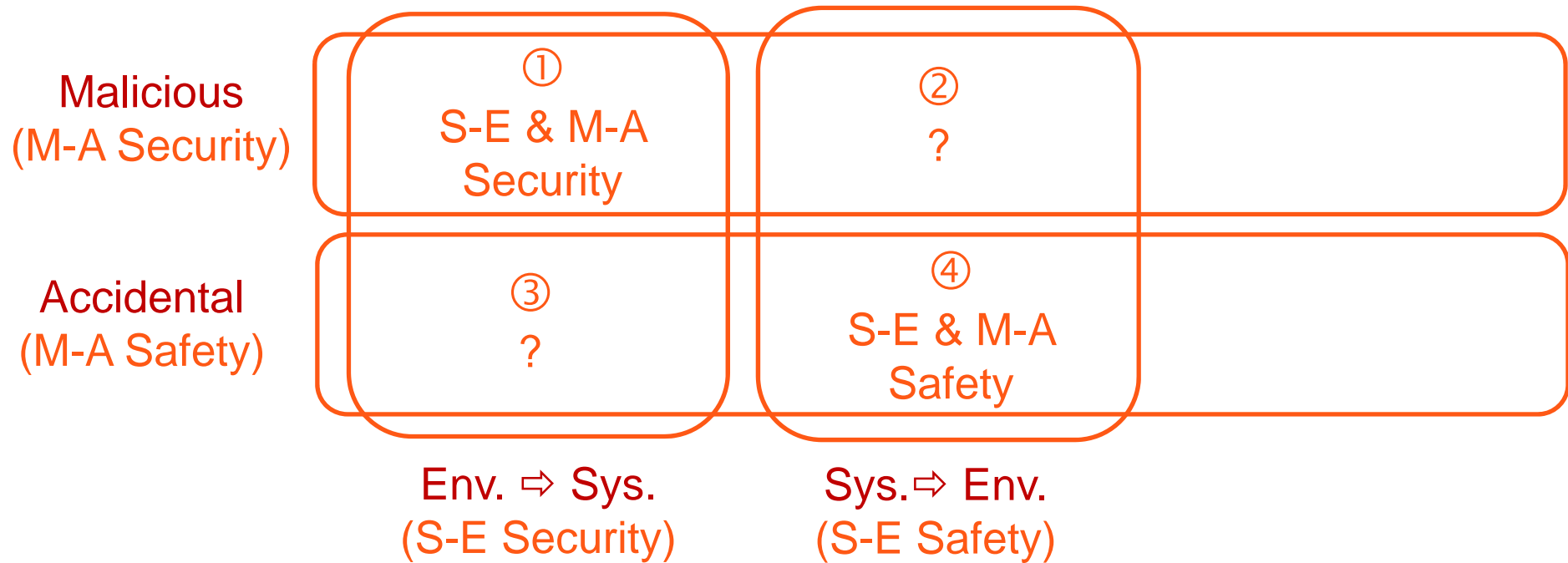
Accidental
(M-A Safety)

An empty rounded rectangular box with a thin orange border, positioned to the right of the 'Accidental (M-A Safety)' label.

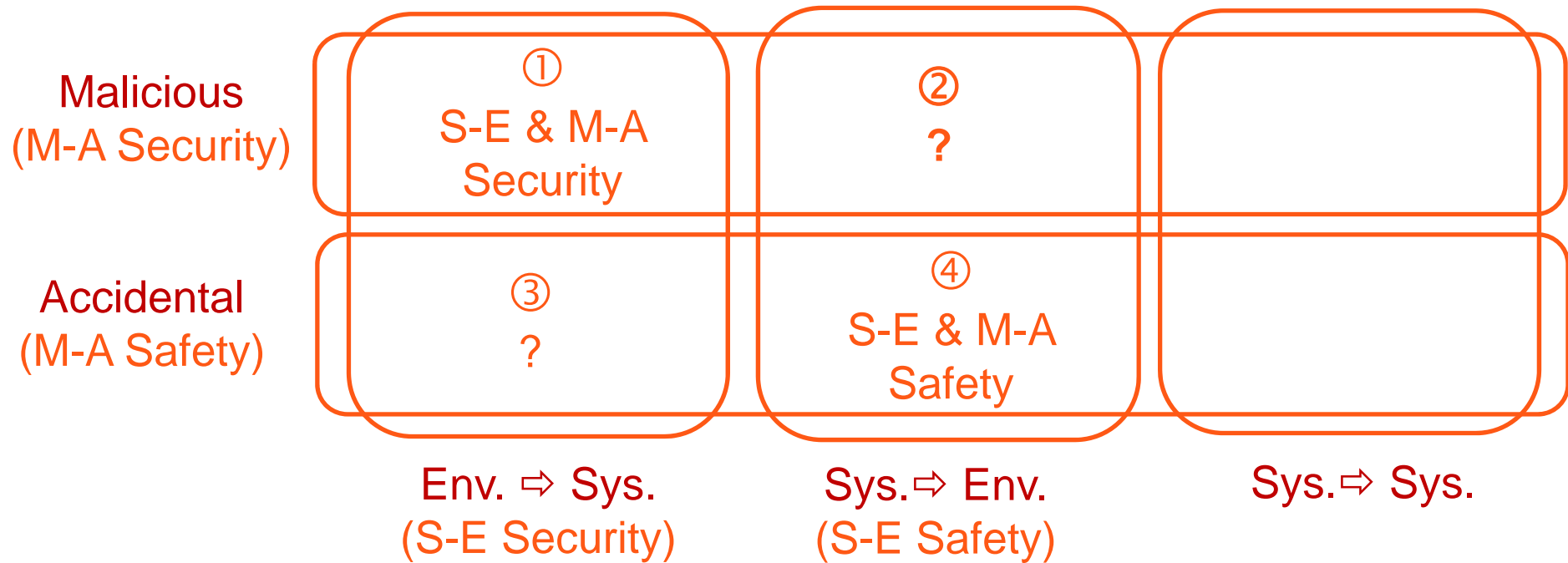
Avoiding equivocation about safety & security



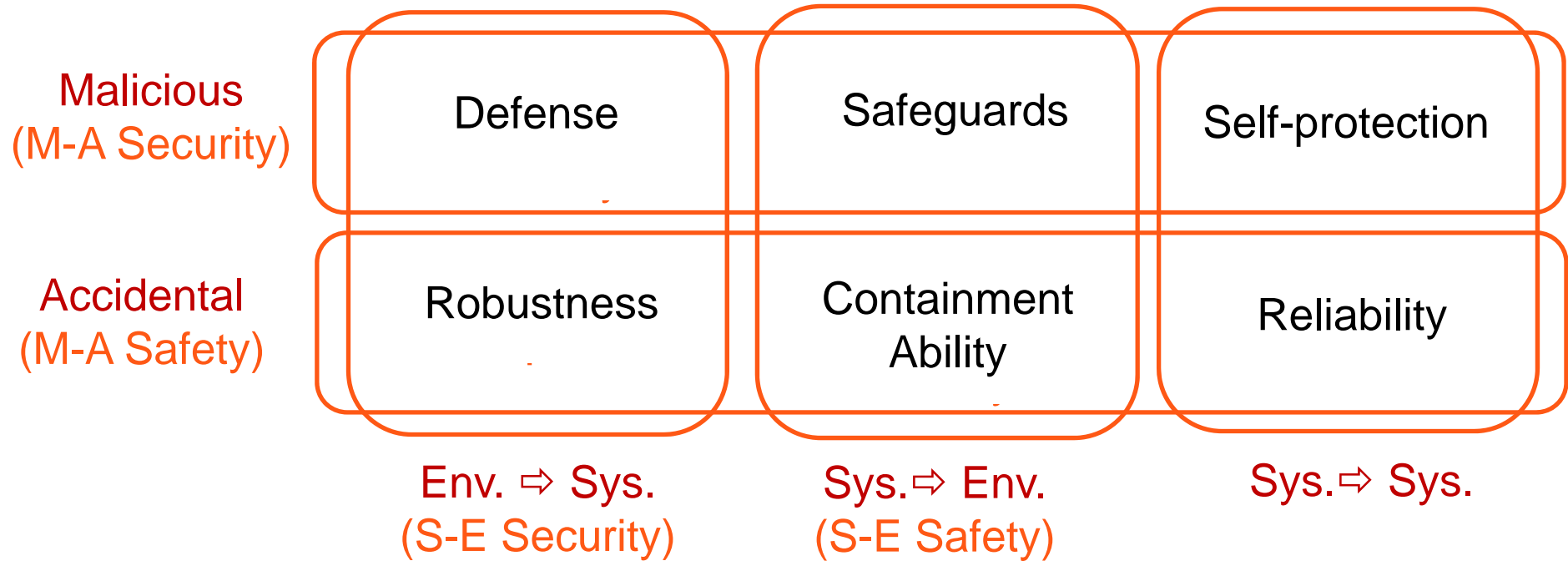
Avoiding equivocation about safety & security



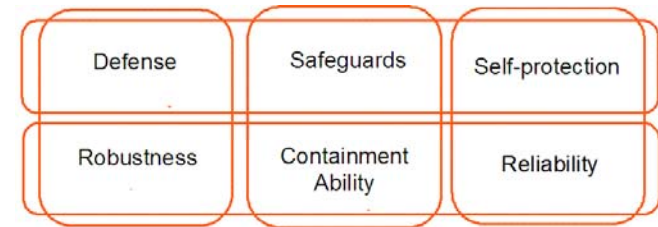
Avoiding equivocation about safety & security



Avoiding equivocation about safety & security

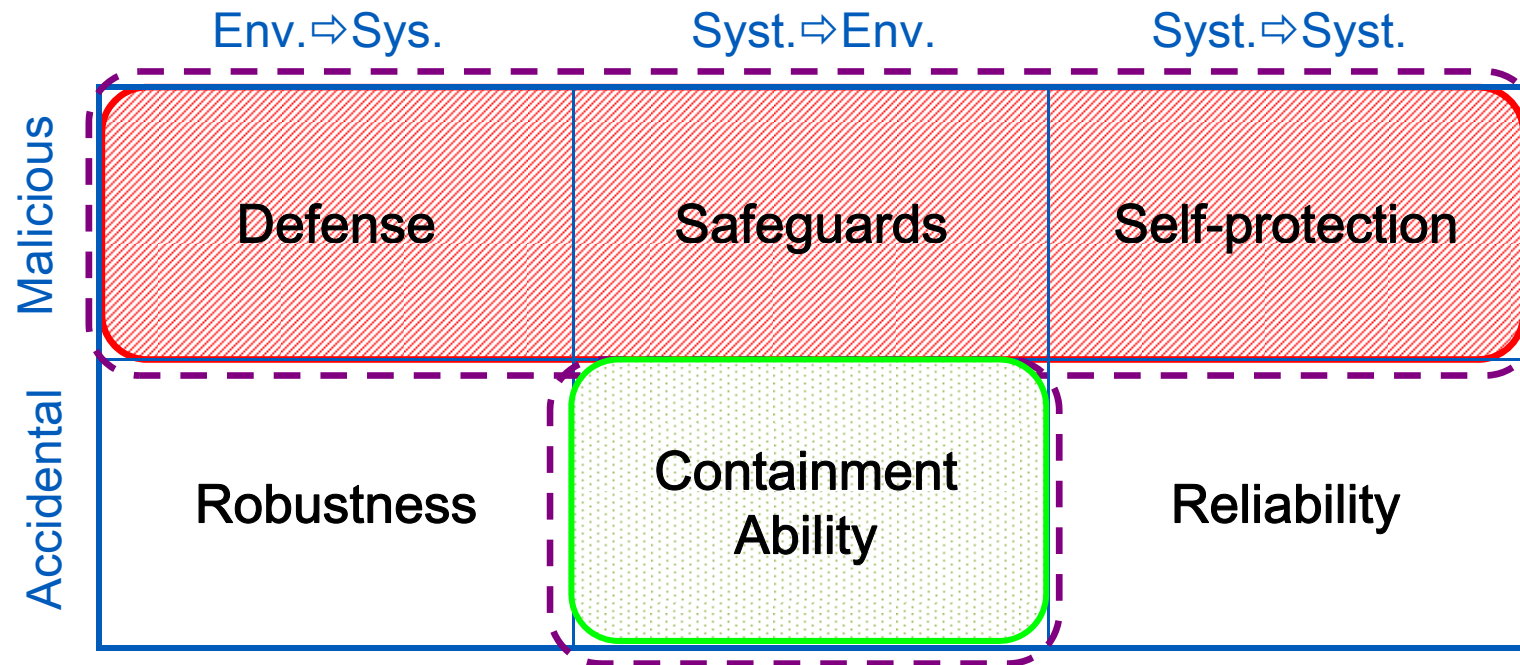


SEMA relevance and limits

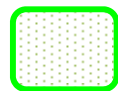


- ▶ Does not aim at replacing the terms safety & security
 - Clearly too much history, plus new debates on the sub-notions
 - Provide a handy reference to position them, draw their limits
- ▶ A holistic and indicative view of the risk space
 - A mnemonic tool for a better risk coverage
 - Sub-notions limits are soft limits (context, system definition...)
 - Sub-notions are not exclusive in essence
- ▶ Does not fix existing inconsistencies, only a conceptual help
- ▶ Enough of general concepts
 - Let see how we can use it in different CIP sectors

Nuclear power generation



IAEA security

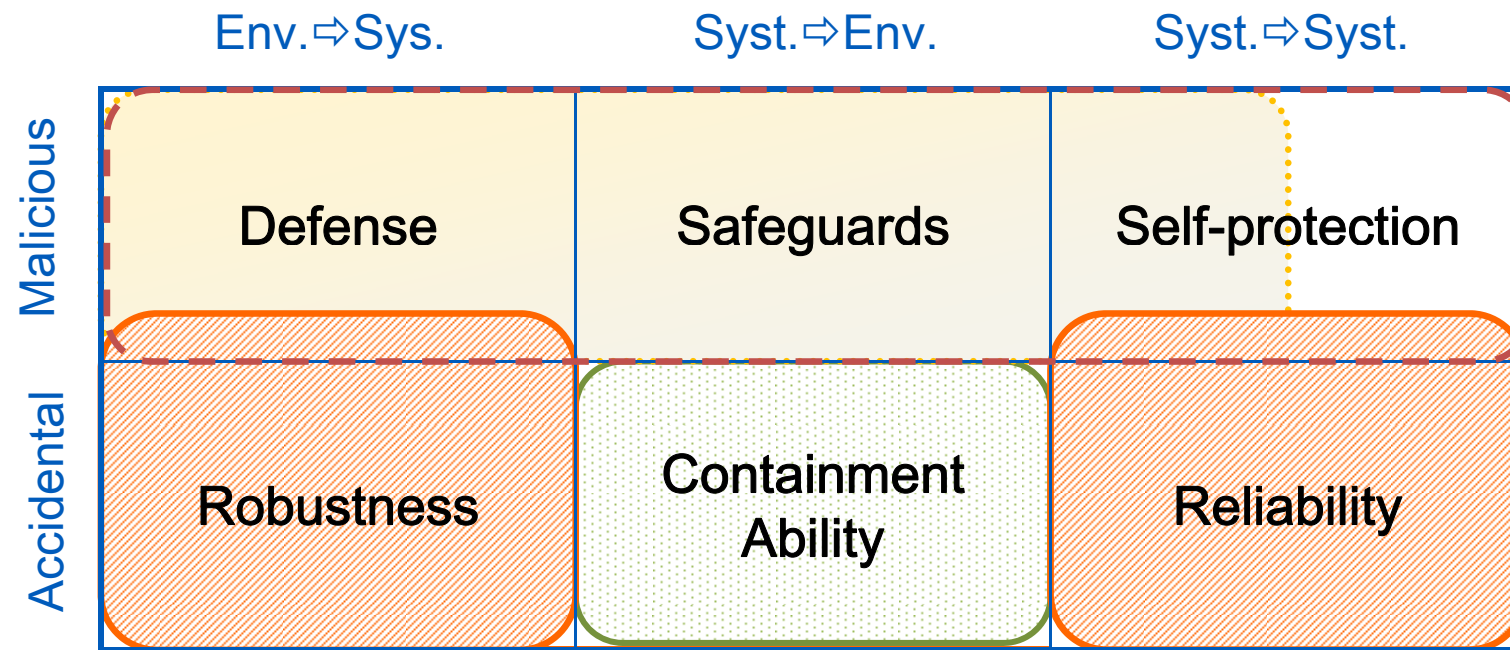


IAEA safety



“TSN” security
(French law)

The power grid



“Electrical” security



“CIP” security

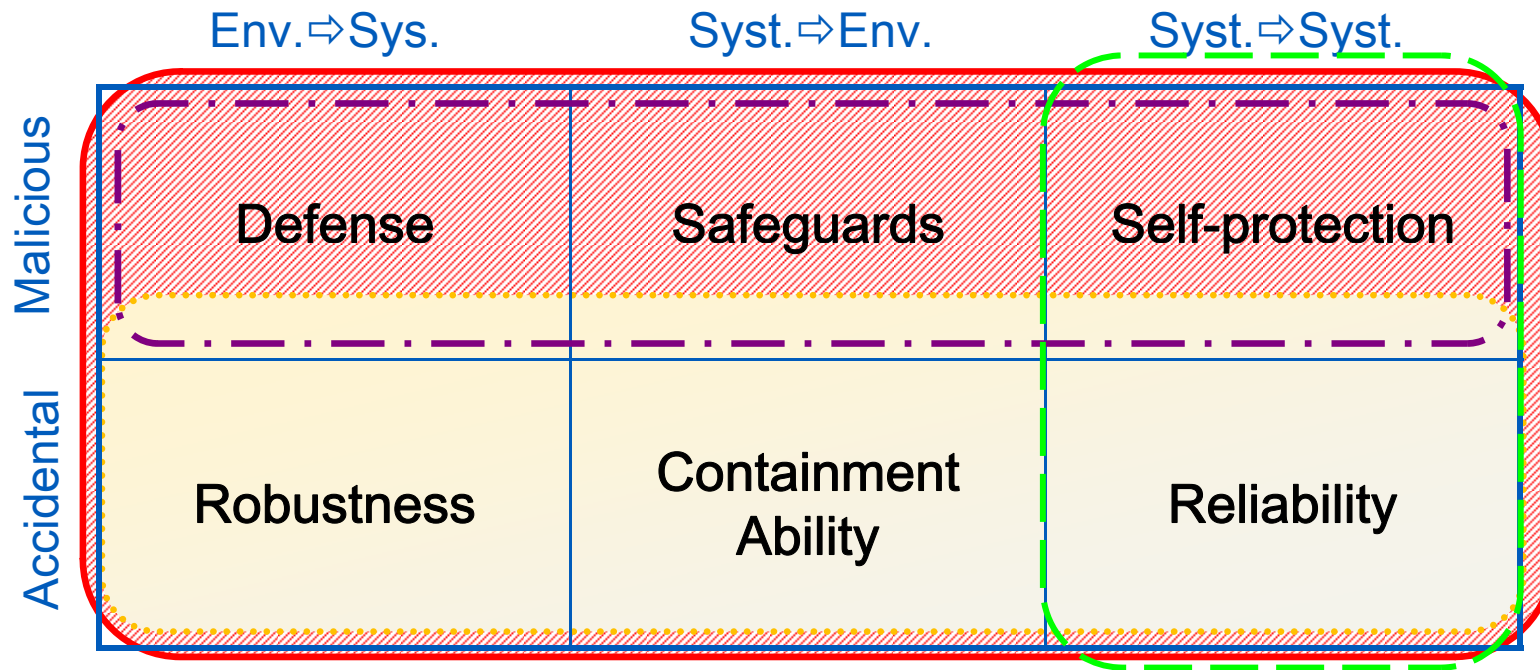


“Electrical” safety



“Cyber” security

Telecommunications and data networks



-  IETF safety
-  CIIP security
-  IETF security
ISO/IEC security
-  ISO/IEC safety

Concluding remarks and perspectives

- ▶ **Safety and security, an ambiguous terminology**
 - Equivocations & ambiguities to be avoided as early as possible
 - CIP is particularly prone to such difficulties
- ▶ **The SEMA referential framework**
 - Position the terms on a “conceptual map”
 - Make unsaid differences of interpretation explicit
 - May underline ambiguities and overlaps when they exist
- ▶ **On-going and future work**
 - Integrate your feedback
 - Distinguish the cyber and physical dimensions
 - Support interdependencies analysis

Thank you for your attention

Questions & Reactions

Ludovic Piètre-Cambacédès, EDF R&D

Email: ludovic.pietre-cambacedes@edf.fr

Tel: +33 1 47 65 58 11