Fraunhofer IESE

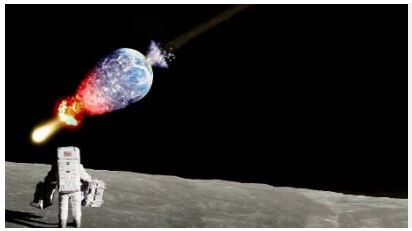
SMART Ecosystems

Safety und Security in der Industrie 4.0

GI Architekturen 2014, 7. Juli 2014, ABB Ladenburg

Dr. Mario Trapp
mario.trapp@iese.fraunhofer.de

Overview

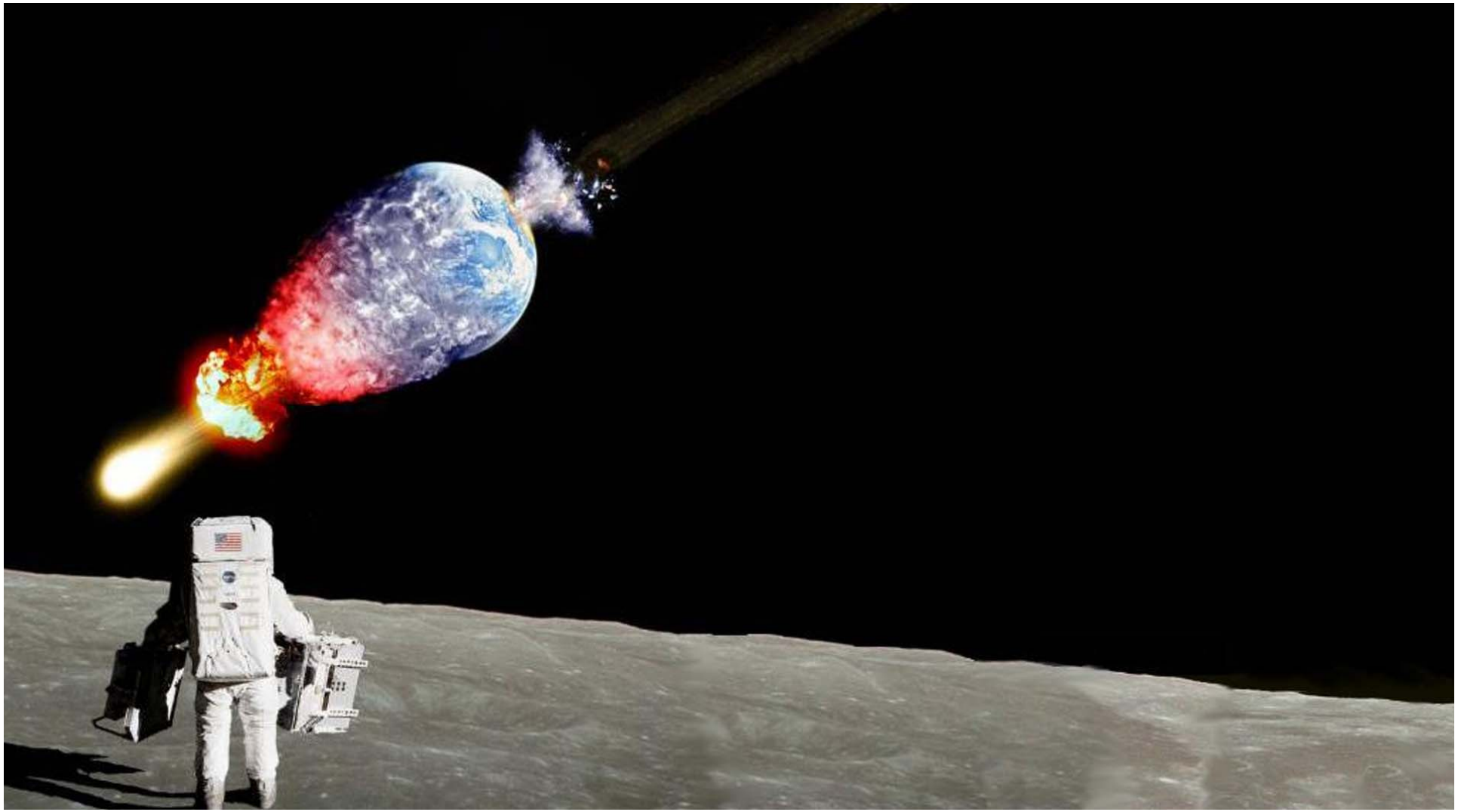


What are the Challenges?

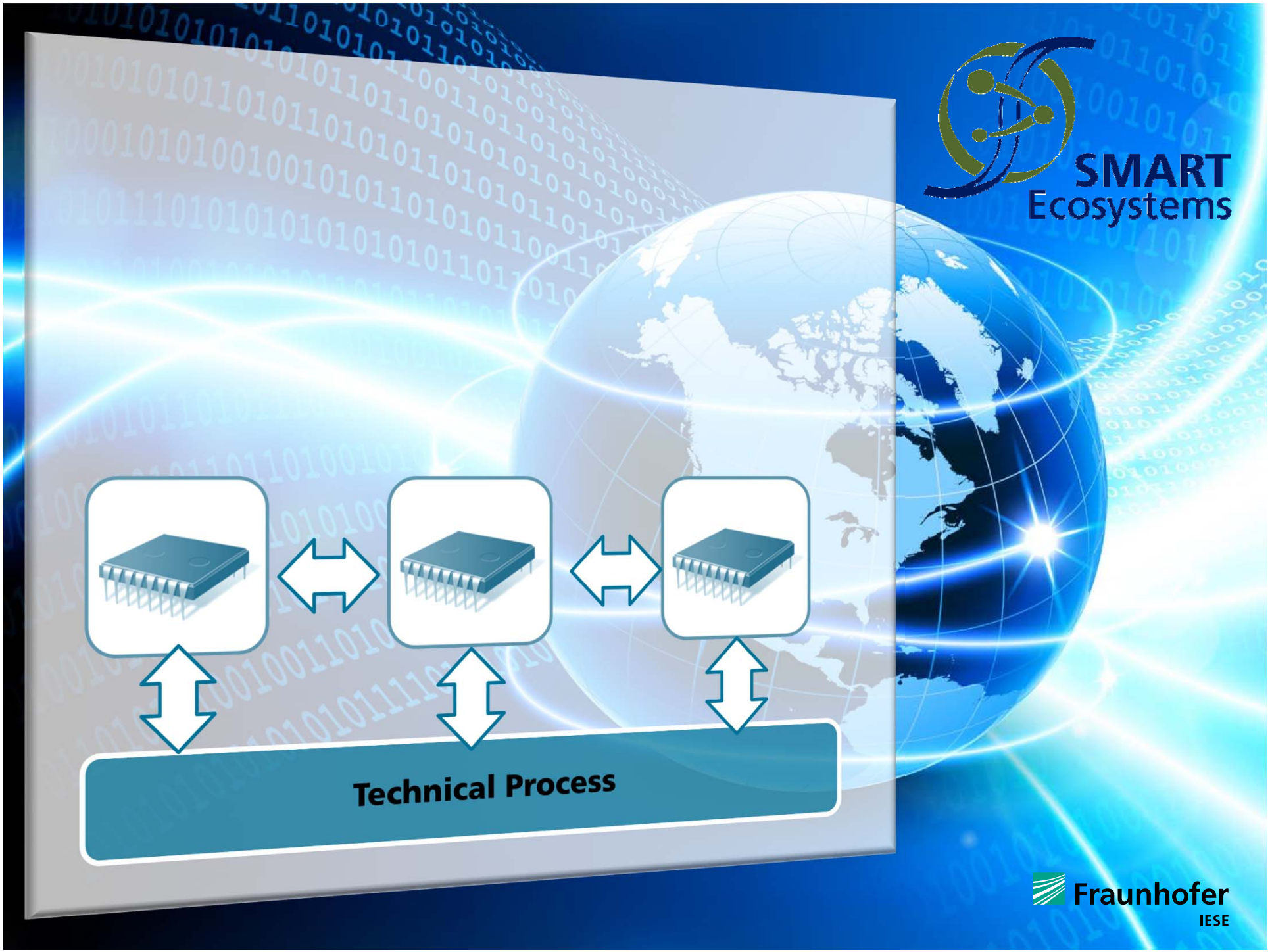
How to assure Safety?

How does Security influence Safety?

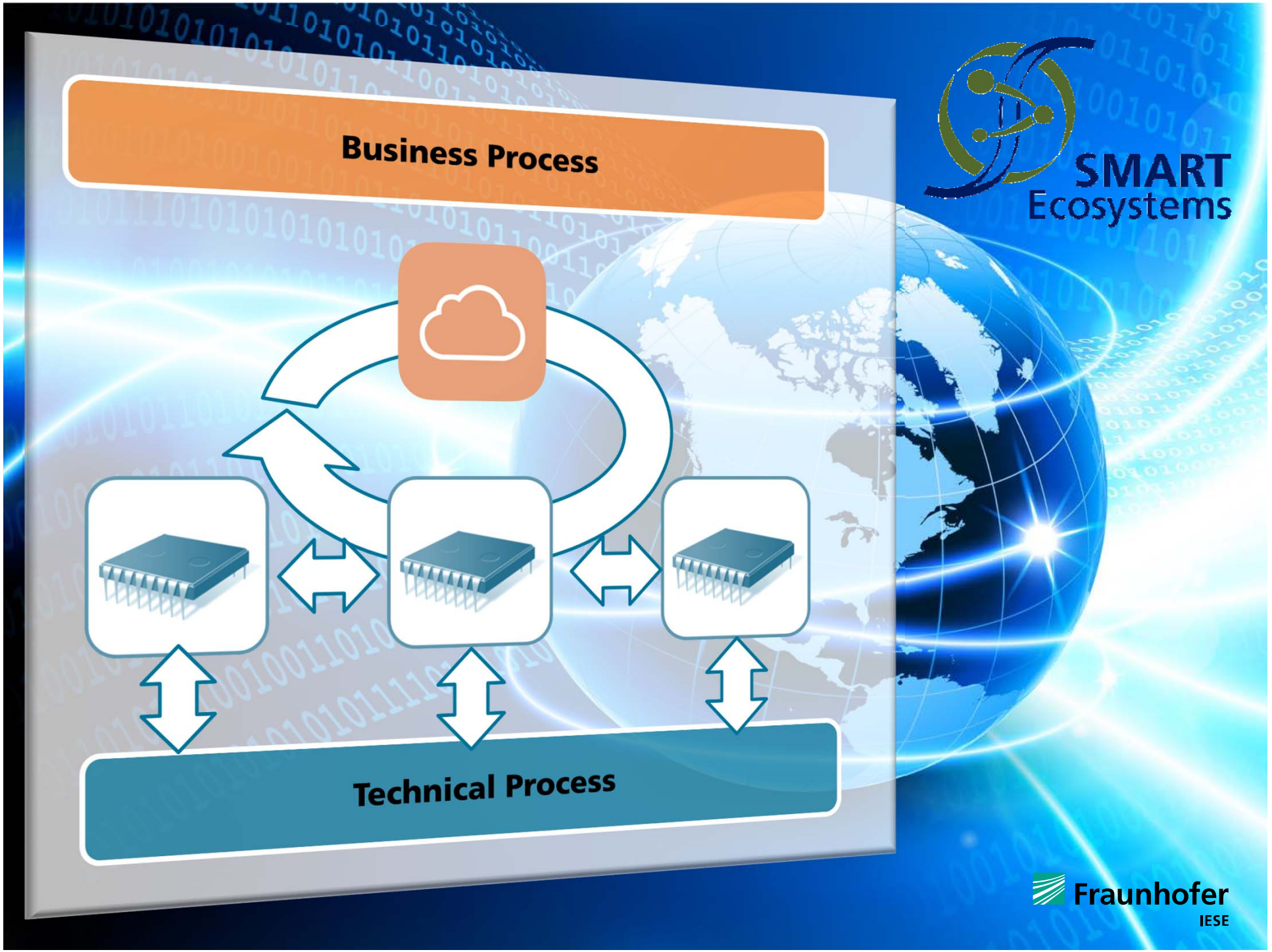
What are the Challenges?

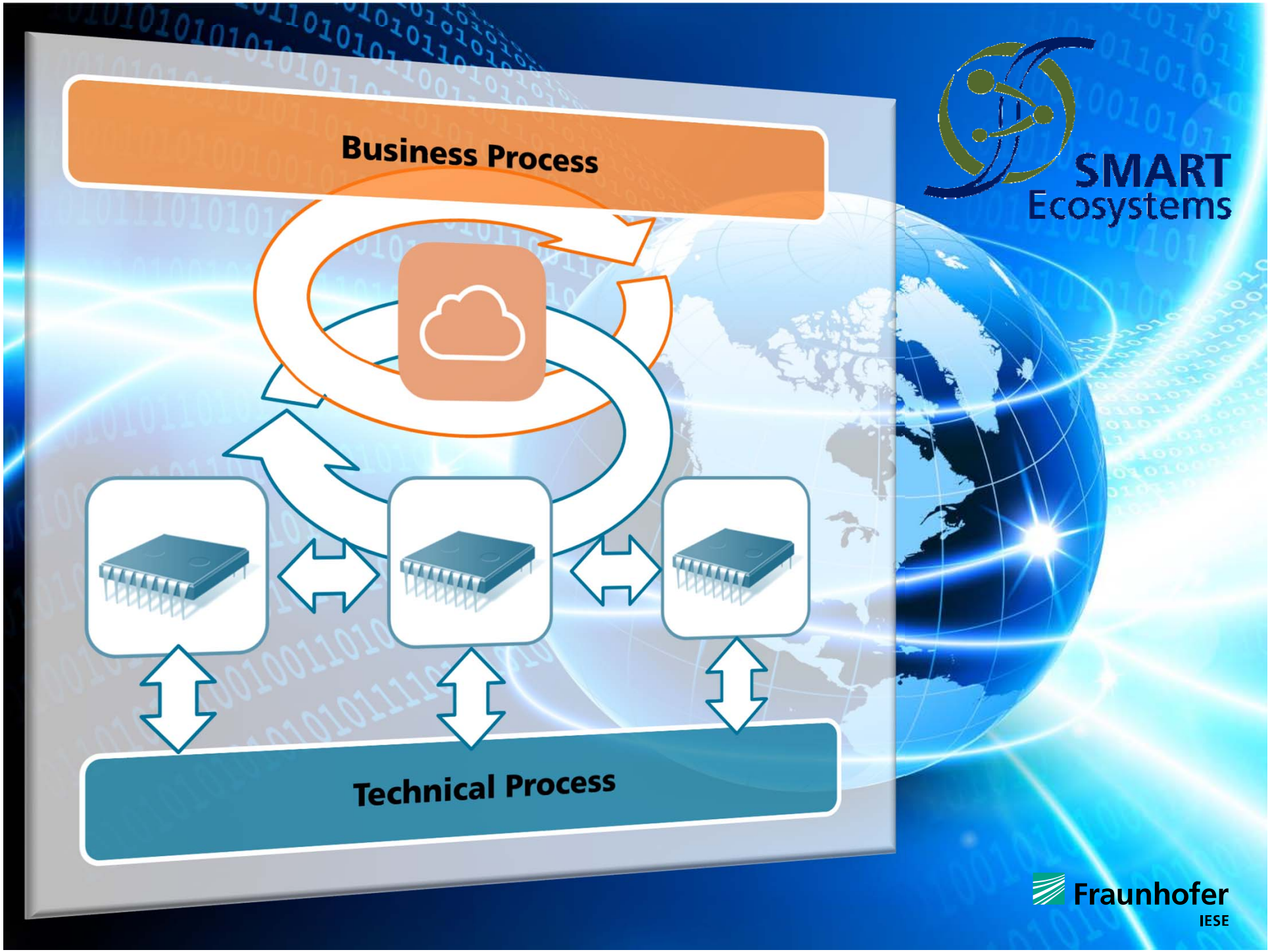



SMART
Ecosystems
Technical Process
Fraunhofer
IESE


SMART
Ecosystems
Technical Process
Fraunhofer
IESE


SMART
Ecosystems
Technical Process
Fraunhofer
IESE


Business Process
Technical Process
SMART
Ecosystems
Fraunhofer
IESE


Business Process
Technical Process
SMART
Ecosystems
Fraunhofer
IESE


Engineering/
Architectures
Safety
Security
UX


Engineering/
Architectures
Safety
Security
UX

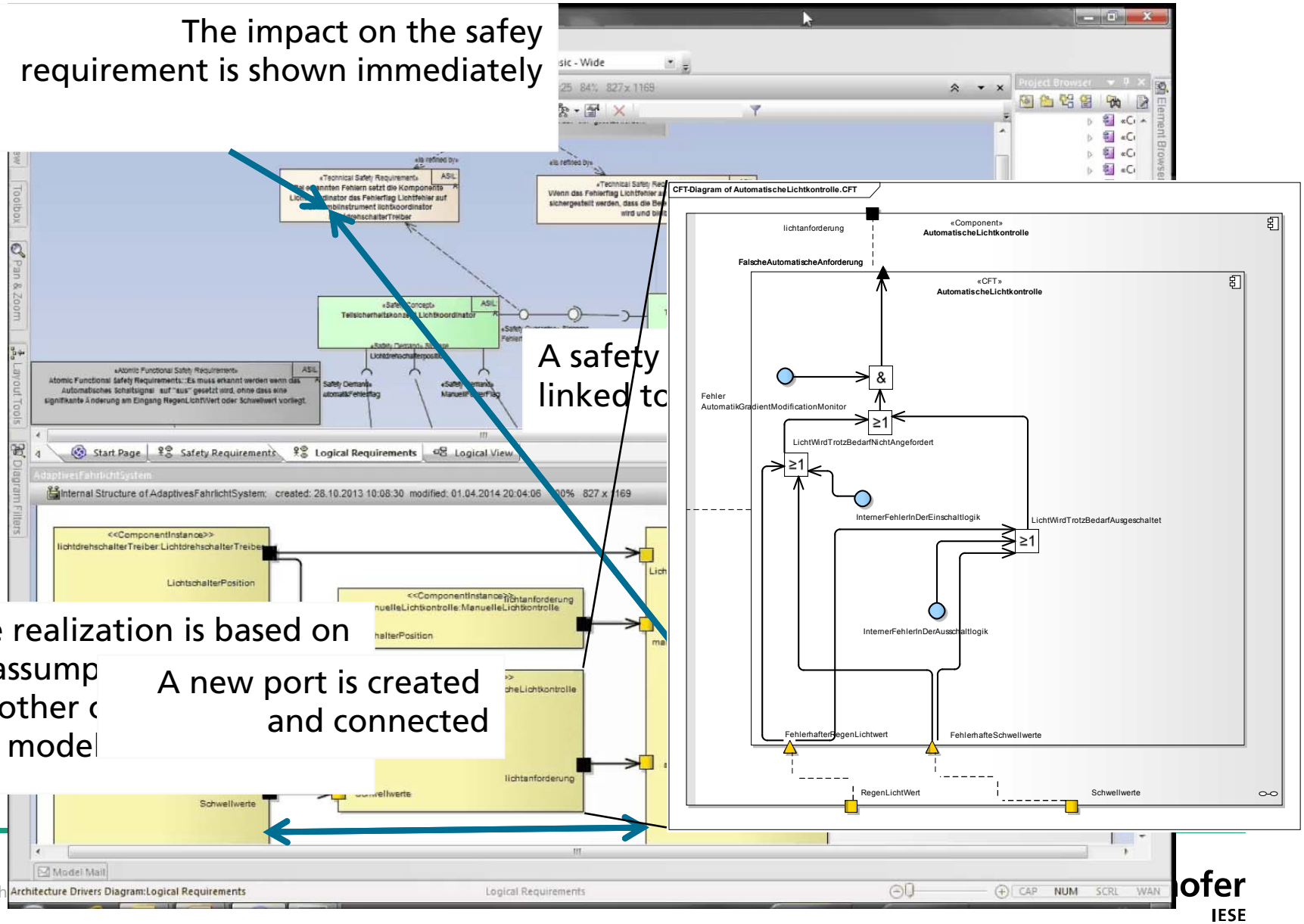
Challenges: Openness and Adaptivity leading to Uncertainties

- **Openness**
  - Systems are opened for supporting dynamic collaborations with other systems from different vendors / domains
  - Elements of the SoS can hardly be predicted at development time
  - Systems become vulnerable for security attacks
- **Adaptivity**
  - Systems dynamically adapt to their current runtime context (collaboration partners and their current quality of service, environmental conditions etc.)
  - Systems dynamically adapt their structure and / or behavior
- **Intelligent Behavior**
  - Systems are implemented using cognitive / intelligent behavior
  - Traditional quality assurance / runtime monitoring is insufficient
- **Uncertainty**
  - Resulting changes in the SoS‘s structure and / or behavior due to openness and adaptivity can hardly be predicted (at least: state space explosion)
  - At traditional certification / assessment times not all relevant facts are known

How to assure Safety?

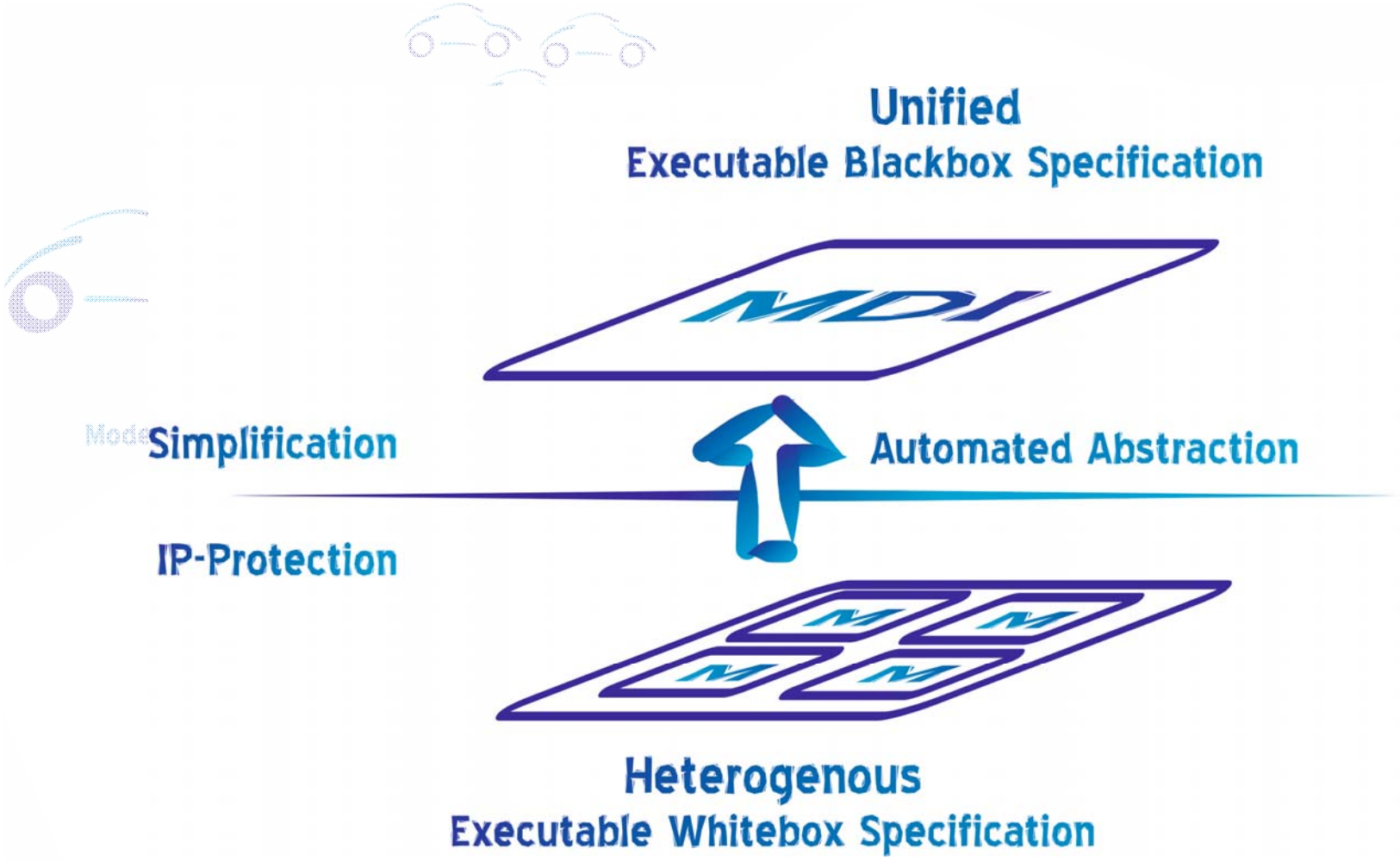
A key to success: Integrated model-based Safety Engineering (i-SafE)

The impact on the safey requirement is shown immediately

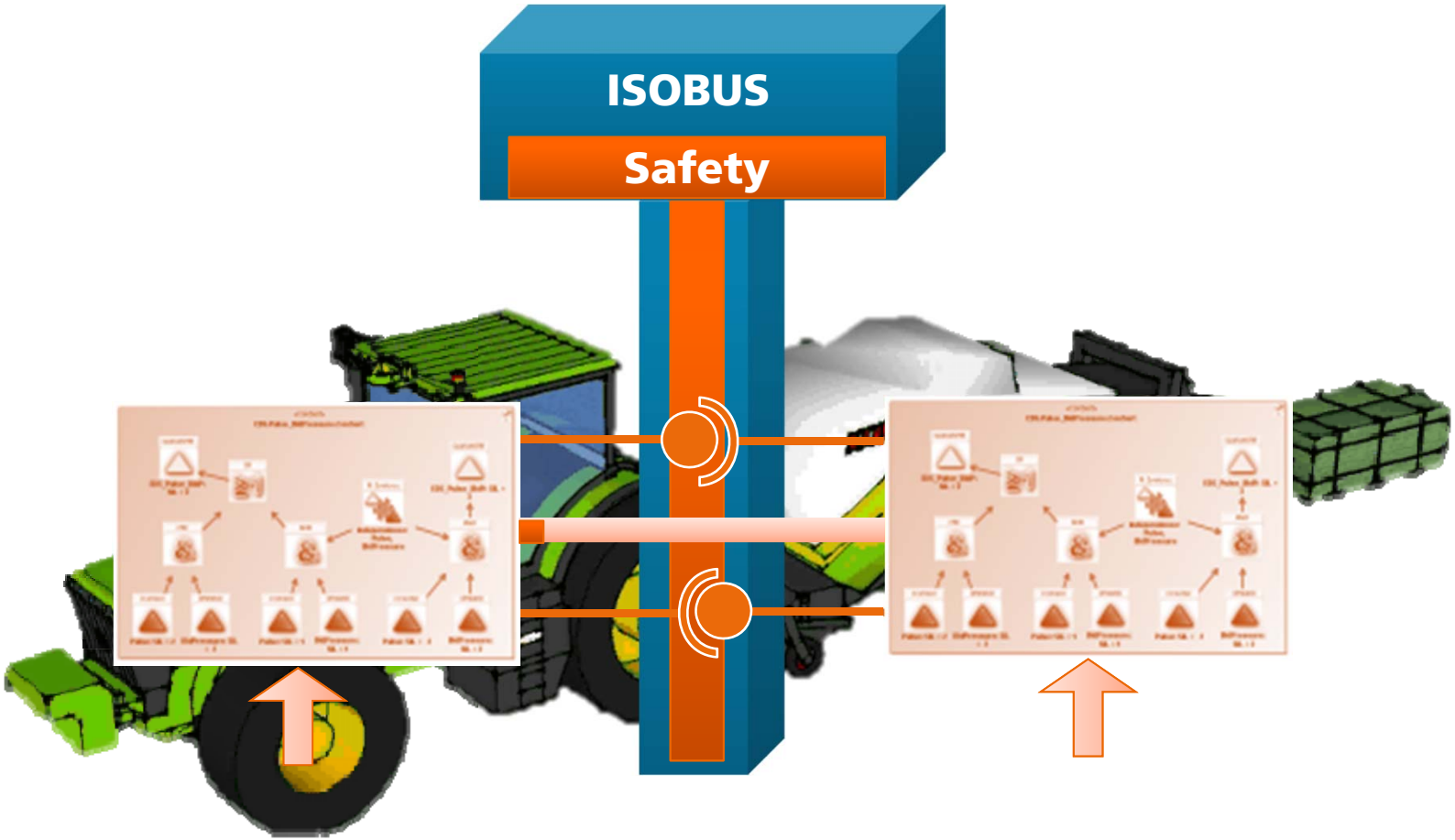


ofer
IESE

Virtual CPS-Integration

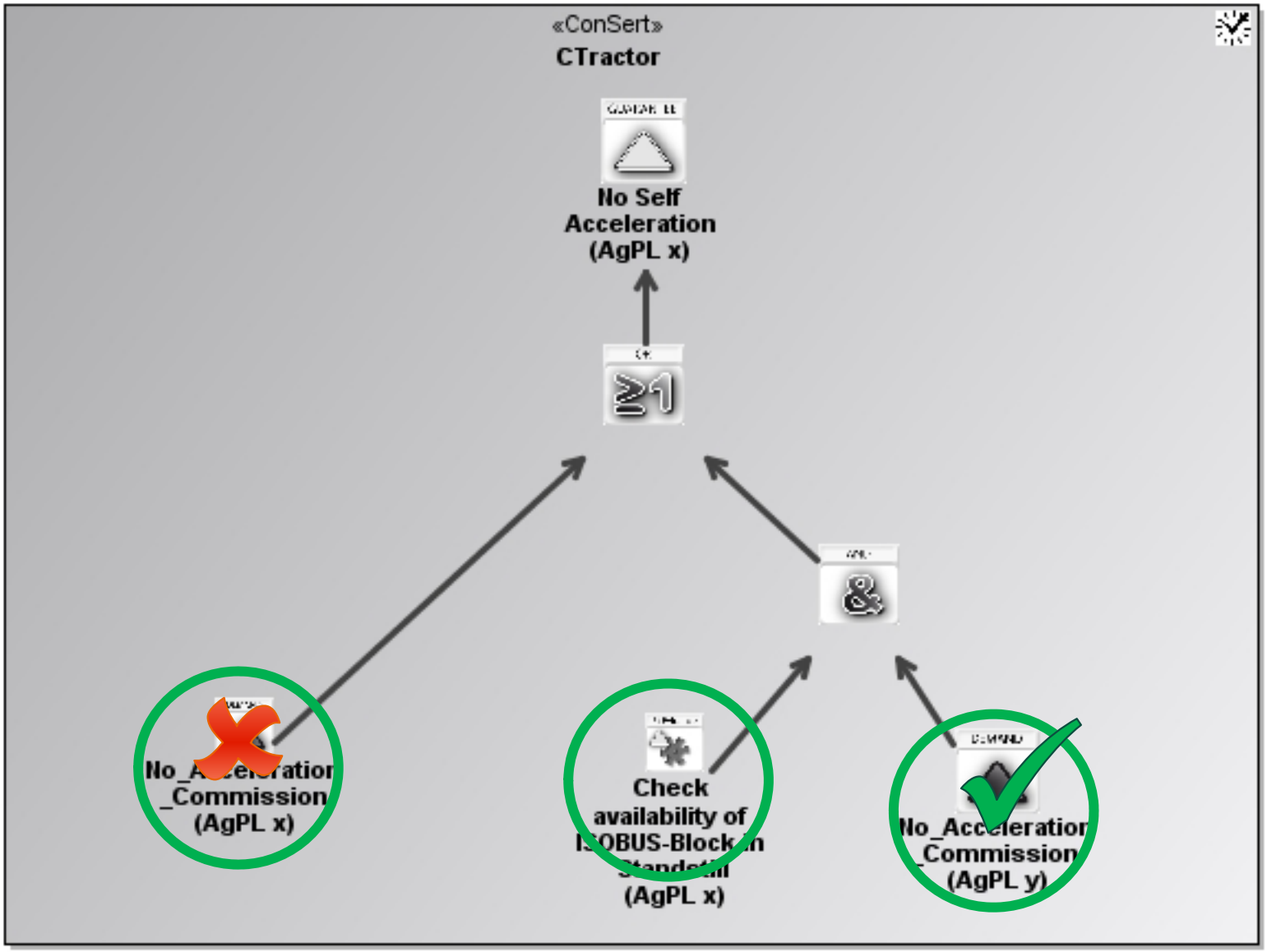


Conditional Safety Certificates – ConSerts
A Safety Model @ Runtime (SM@RT) as part of an MDI



Fraunhofer
IESE

Basic Idea

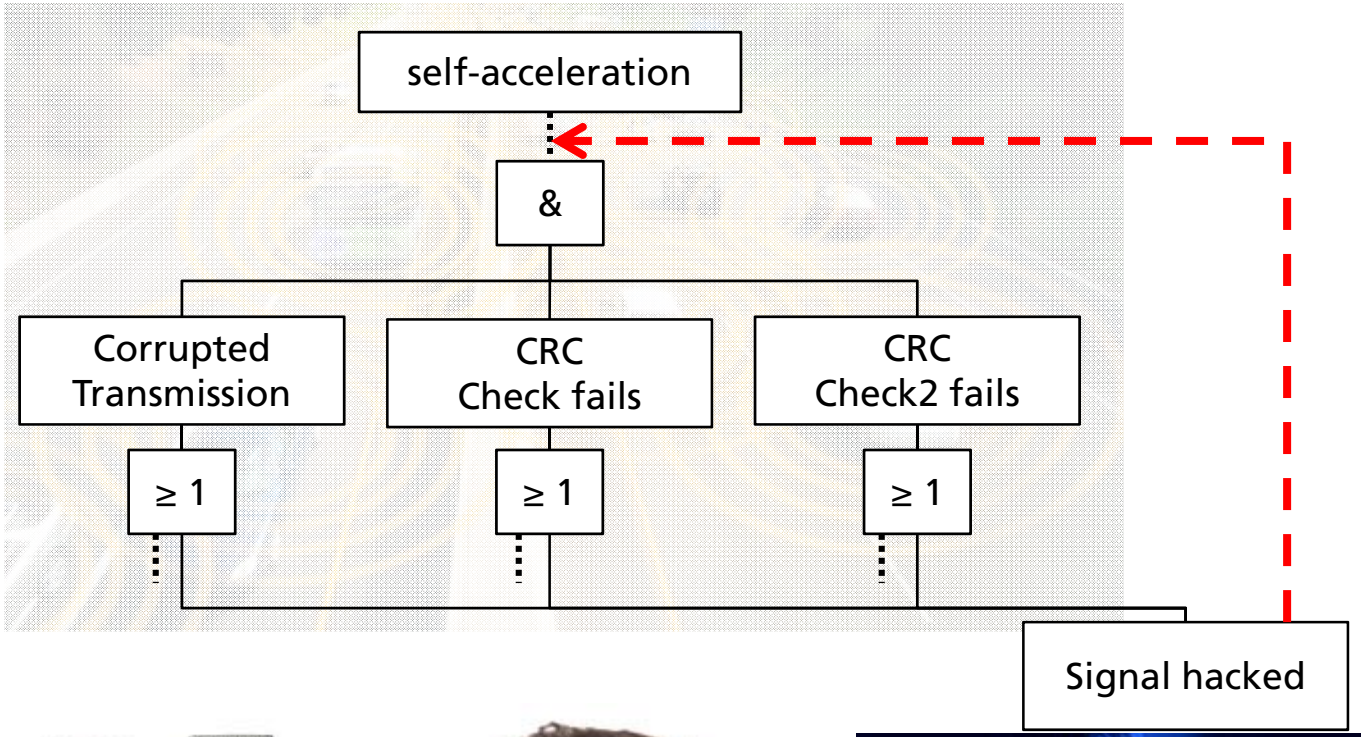


How does Security influence Safety?

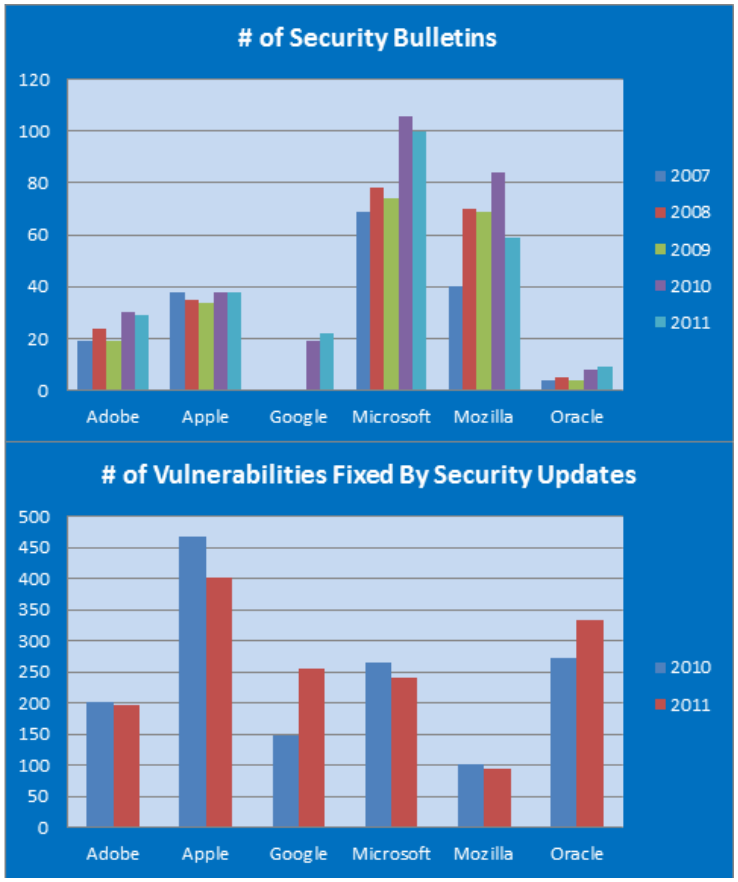
What‘s the difference – Just a matter of Probabilities?

- Safety is quantitative, security not?
  - No, safety is not quantitative if it comes to software
- Increasing the set of appropriate counter measures decreases the likelihood of safety-critical failures
  - This assumption does not hold for security
  - But how secure is safe enough then?
- If a system is safe at its release, its lifetime safety can be well-predicted
  - Even if a system is secure, this will not be true for a long time
  - Security is based on patches – Safety tries to minimize modifications

Hackers as neglected Common Causes



The Real Security Challenges take the Rear Entrance



- Embedded systems have reached comparable size
- Open systems will never be secure
  → how can they nonetheless be safe?
- Each patch means a software modifications
- How does a safety architecture look like enabling regular patches without requiring safety re-certification?

Summary

Safety

- Openness and adaptivity lead to uncertainty
- Behavior becomes more and more intelligent and partially indeterministic
- More intelligent safety monitors are required
- Safety Models @ Runtime provide an efficient and predictable means

Security as impact on Safety

- It is not only about qualitative vs. quantitative approaches
- Safety and security follow different basic „laws“
- Security has a far-reaching impact on safety assurance

Dr. Mario Trapp

mario.trapp@iese.fraunhofer.de

phone: +49 631 / 6800 - 2272

Fraunhofer
IESE