Powering Innovation That Drives Human Advancement

Ansys medini analyze:
Model-Based Safety and Cybersecurity Engineering

Michael Soden / Senior Product Manager

Agenda

- Safety & Cybersecurity Analysis
- Model-Based Safety, Reliability, and Cybersecurity Analysis
- Demo: Ansys medini analyze
- Conclusion and Outlook

Safety and Cybersecurity of Software Controlled Systems

International standards dedicated to product development processes for **safety-related E/E systems**
(IEC 61508, ISO 26262, ISO 21448, ISO 21434, ARP4754A, MIL-882E, DO 356A, …)

Risk Management

Safety Case

Analysis of Systematic Failures

Hazard Analysis & Risk Assessment

Analysis of Random Failures

Safety Requirements

Reliability & Availability

Functional and Technical Safety Concepts

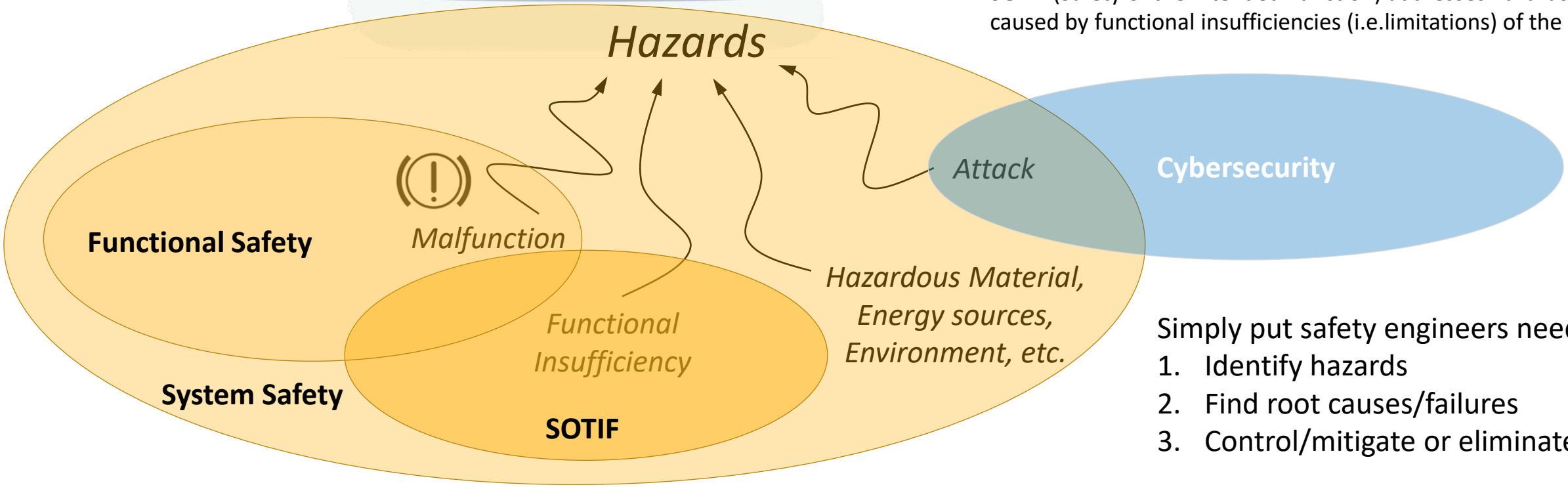
Threat and Vulnerability Assessment

Safety Architecture

Dependent Failure Analysis

Safety and Cybersecurity standards require to perform multiple analysis methods in a consistent, thorough manner

Safety in a Nutshell

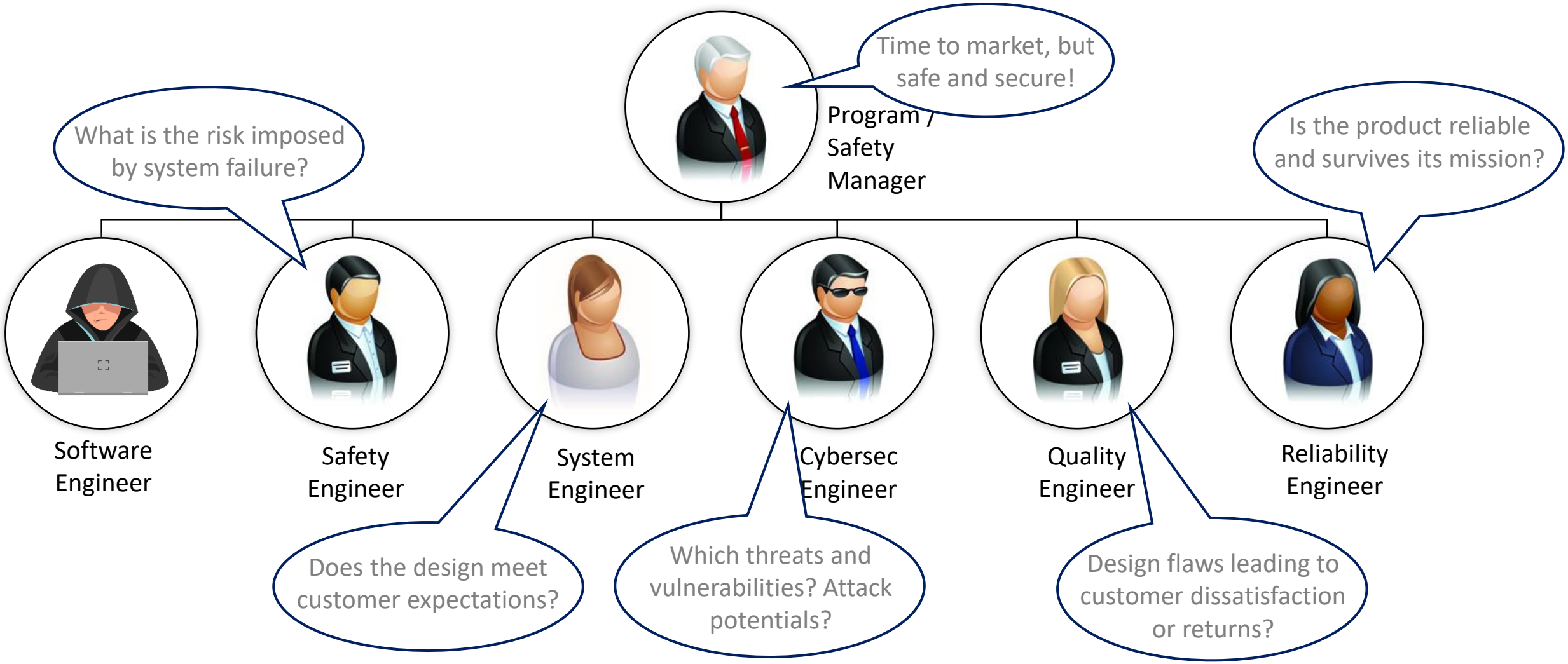


Safety: Absence of unreasonable *risk*
Risk: Combination of *Severity* x *Probability of occurrence*
Severity: Estimate of the extent of *harm* [to people] caused by *hazards* imposed by the system
Hazard: potential source of harm caused by (malfunctioning) behavior of the system
SOTIF (Safety of the Intended Function) addresses *hazards* caused by functional insufficiencies (i.e.limitations) of the system

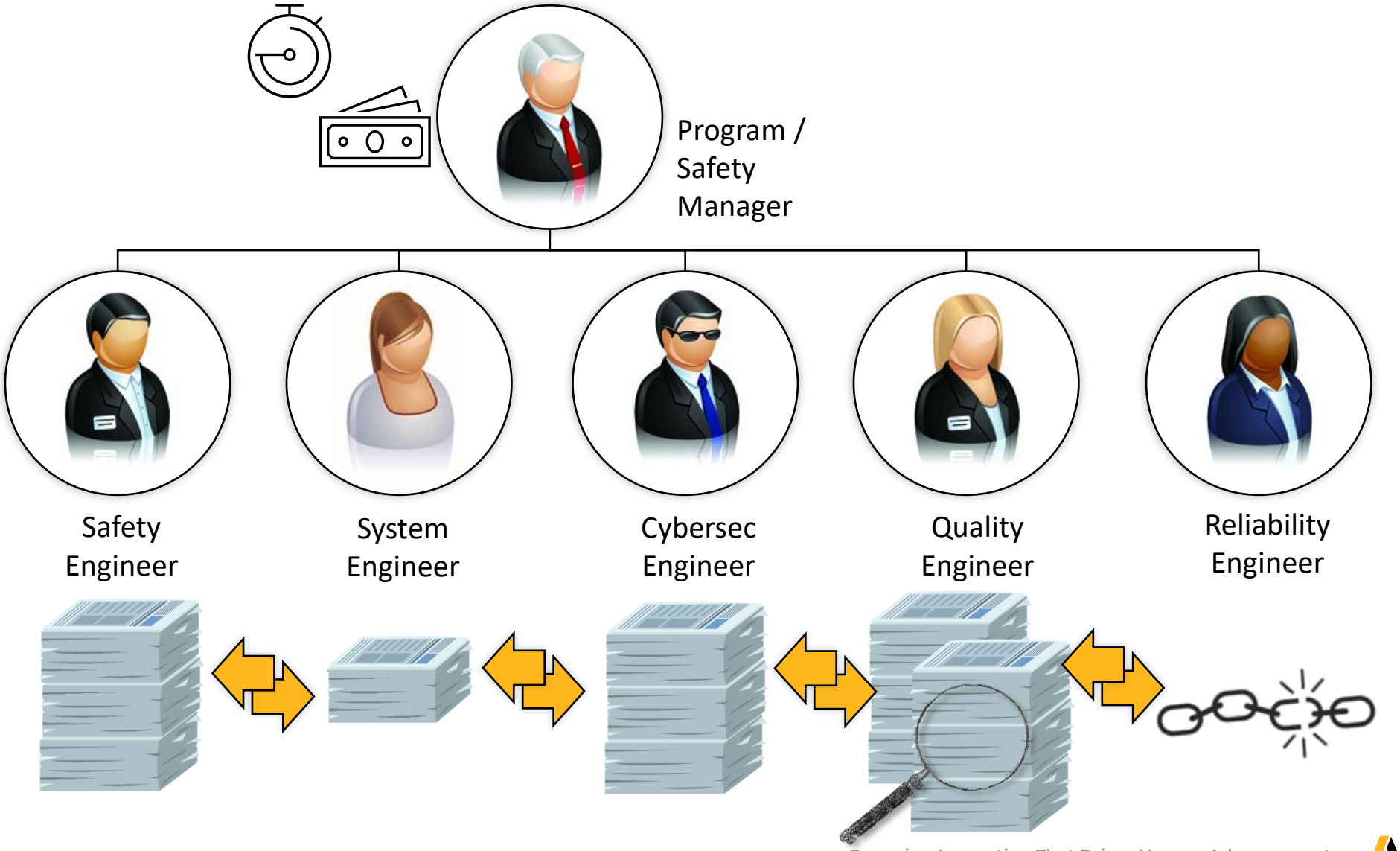
Simply put safety engineers need to:

1. Identify hazards
2. Find root causes/failures
3. Control/mitigate or eliminate them

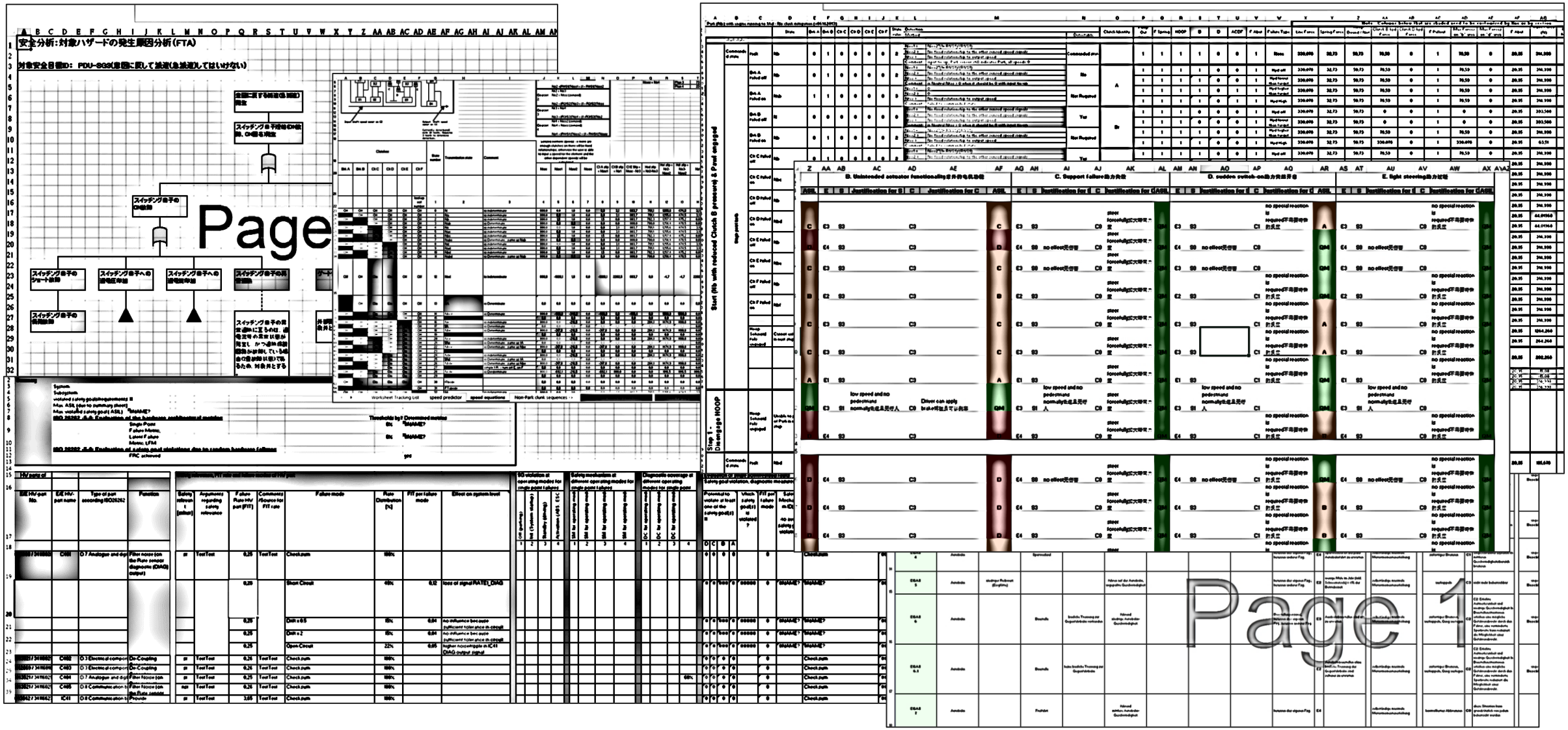
Engineering Roles to Design Safe and Secure Products



Traditional Approach: Point-Tools / Document-centric



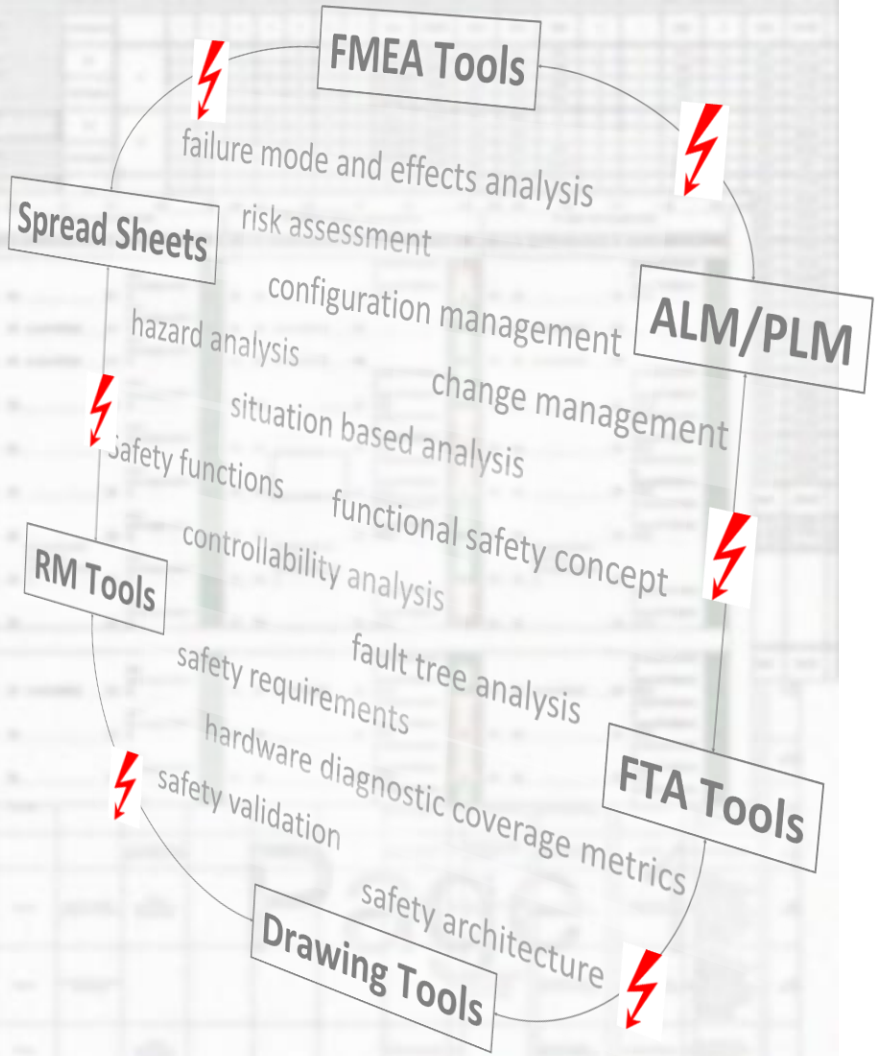
Document-based Processes are Challenging...



Document-based or Point Tools lead to High-Effort

The lack of interconnectivity of Point Tools leads to

- **Inconsistency**
  redundant data is created in the individual tools
- **Inefficiency**
  data is transferred by copy-paste or double work
- **Error prone workflows**
  in case of changes time consuming manual steps are necessary
- **No traceability**
  except for using another 3rd party tool to ensure traceability



Model-Based Safety and Cybersecurity Analysis

Ansys
DIGITAL SAFETY MANAGER

Program / Safety Manager

Safety Engineer

System Engineer

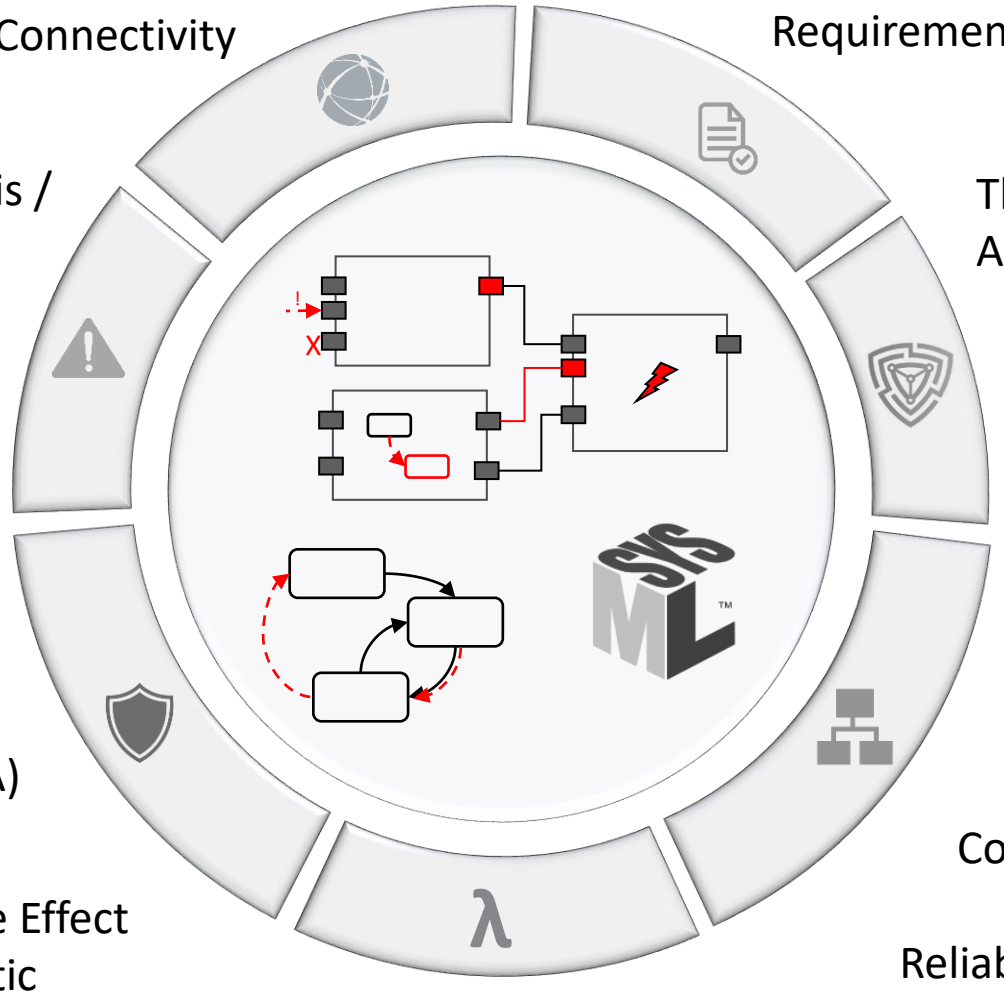
Cybersec Engineer

Quality Engineer

Reliability Engineer

Ansys
MEDINI ANALYZE

Model-Based Safety, Reliability, and Cybersecurity Analysis



3rd Party Connectivity

Requirements Management

Guideword Analysis / HAZOP

Threat & Vulnerability Analysis

Hazard and Risk Assessment (HARA / FHA)

Attack Trees

Failure Mode Effect and Criticality Analysis (FMEA/FMECA)

Common Cause Analysis (CCA)

System Weakness Analysis (SWA)

Fault Tree Analysis (FTA)

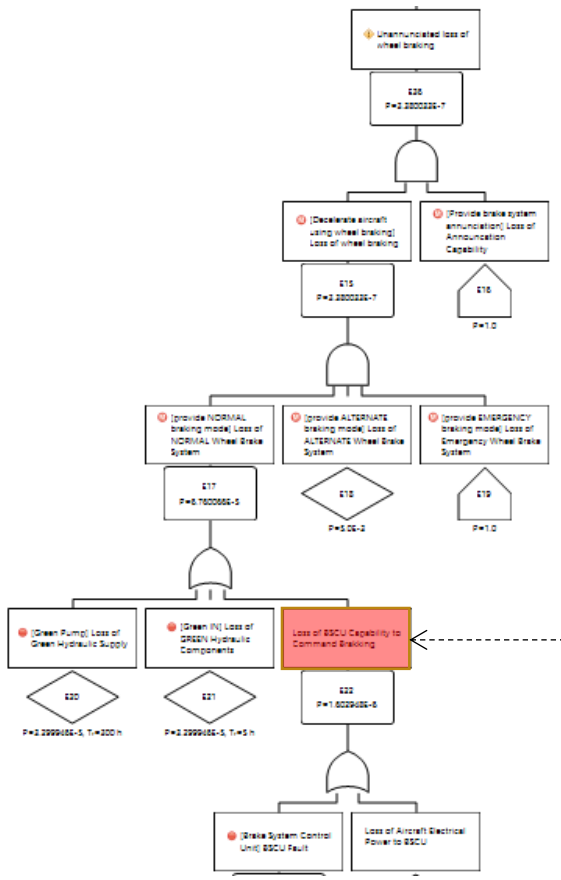
Component Fault Trees (CFT)

Failure Mode Effect and Diagnostic Analysis (FMEDA)

Reliability Block Diagrams (RBD)

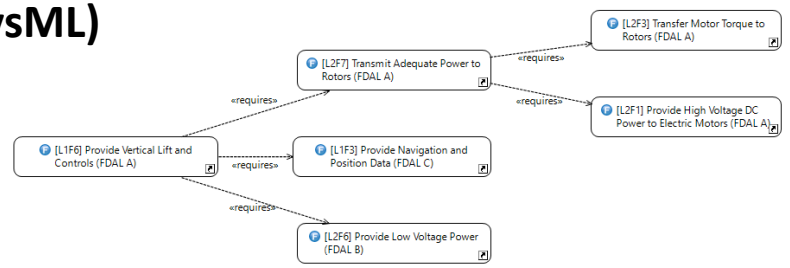
Failure Rate Prediction

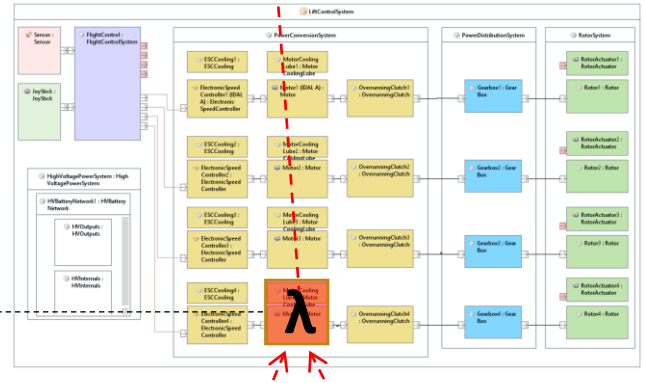
Principle: Model with connected Analyses

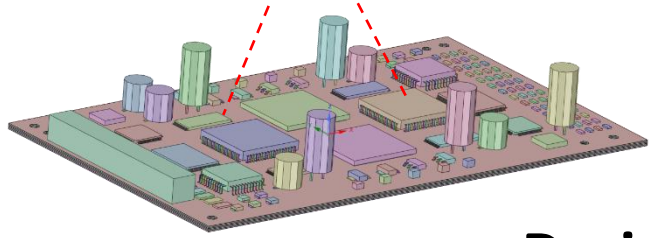


FTA

(SysML)

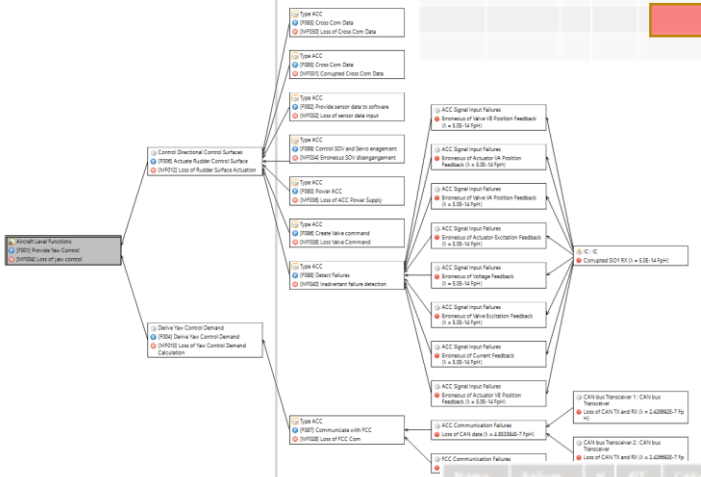




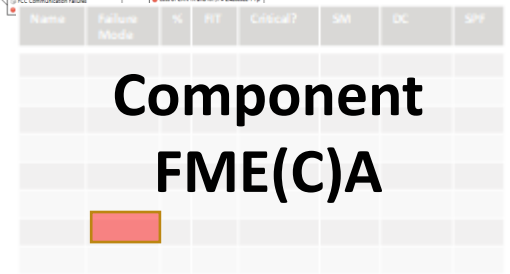


(CAD)

Design Models

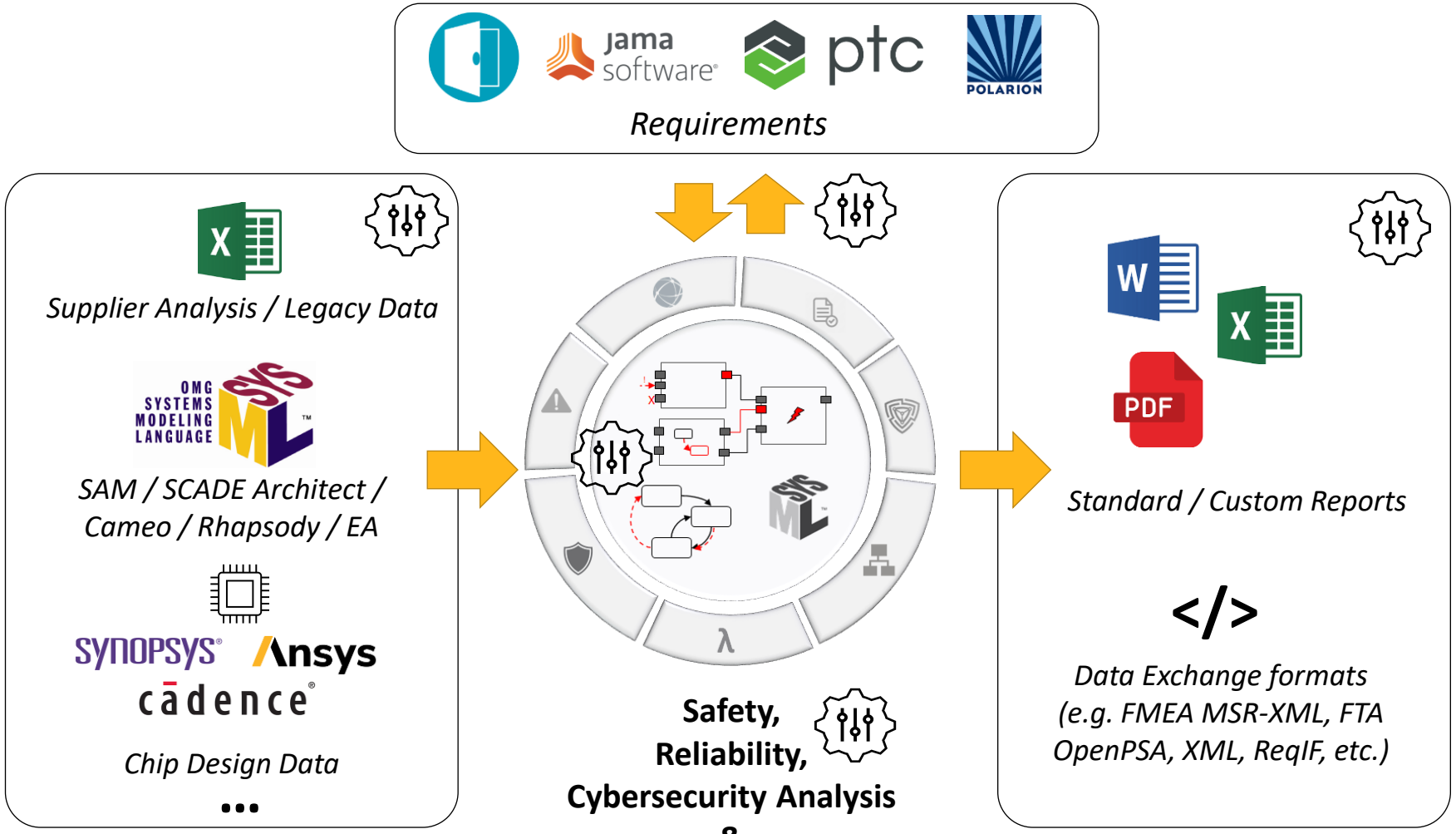


System FME(C)A



Component FME(C)A

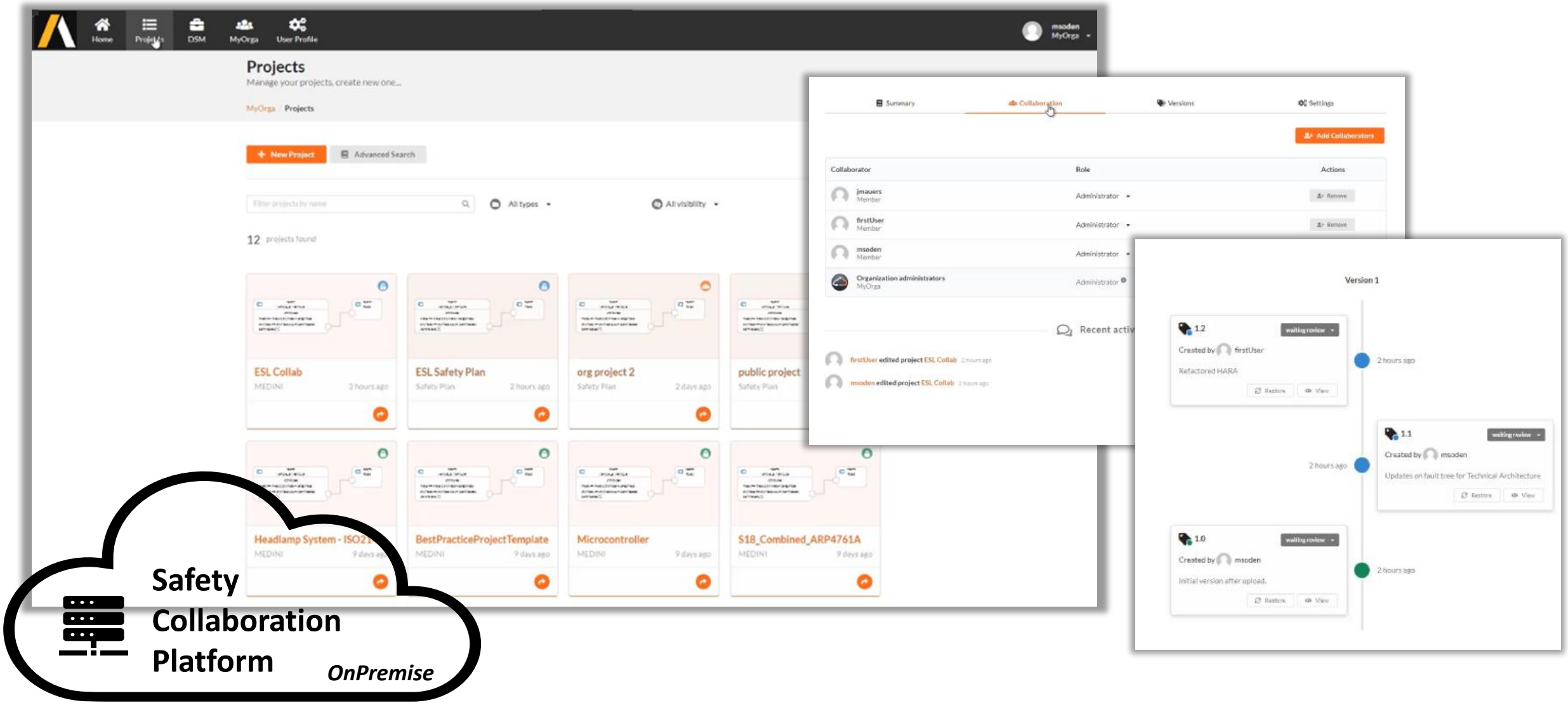
Seamless Integration



Customizations possible to adapt to custom workflows

Demo: Ansys medini analyze

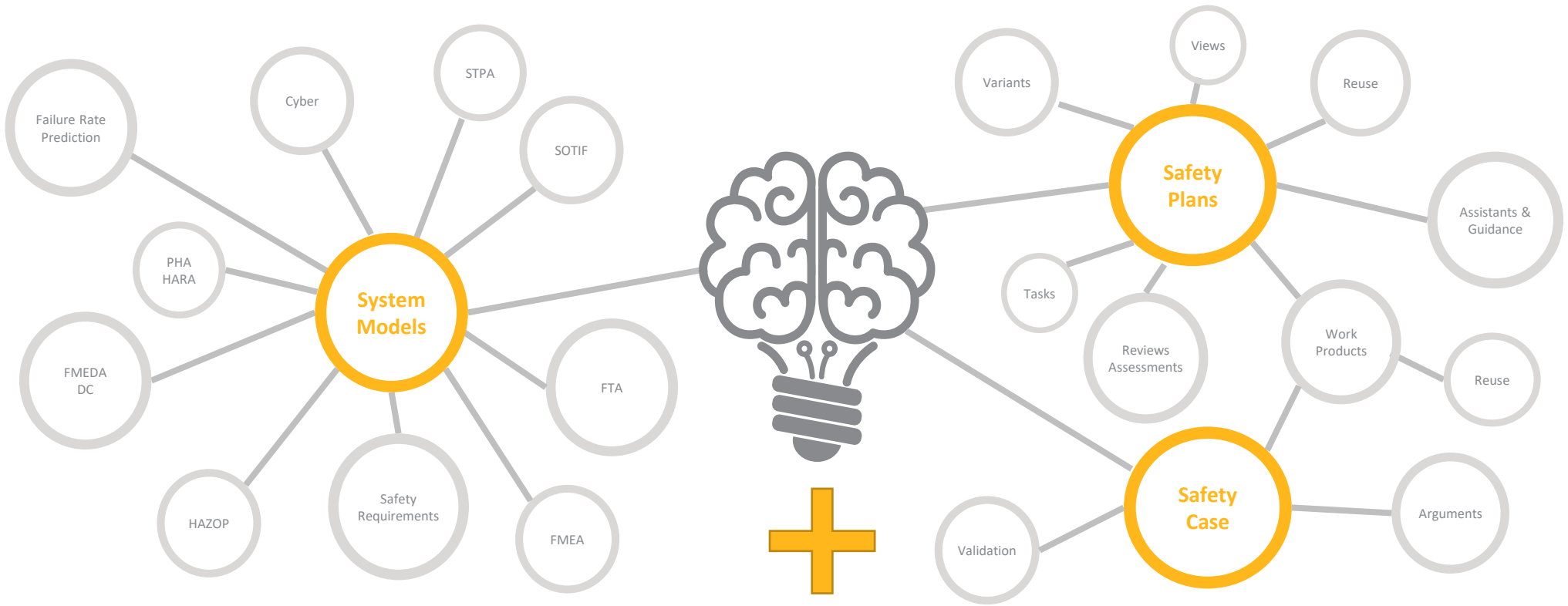
Safety Collaboration Platform – Tool Impressions



Solutions for Safety Engineers and Safety Managers

Ansys / MEDINI ANALYZE

Ansys / DIGITAL SAFETY MANAGER



Safety Engineer / Cybersecurity Engineer analyzing Functional Safety, SOTIF, Cybersecurity, and Reliability of a system

Solution for **Safety & Cybersecurity Managers** performing the overall risk management, planning, execution, and controlling of projects

Summary

- Ansys medini supports model-based analysis
  - SysML models used to represent system design
  - Safety and cybersecurity extensions to perform various analysis such as HARA/FHA, FMEA, FMEDA, FTA, HAZOP, etc.

- Note that Ansys Safety Products provide additional capabilities not shown today:
  - Cybersecurity analysis (e.g. TARA, AttackTrees)
  - Safety Concept Development
  - Safety Case and Safety Management
  - Dependent Failure Analysis
  - Quality and Reliability Analysis
  - Checklists, project difference analysis, reporting, and many more


Ansys