MODEL-BASED SAFETY ANALYSES

Alessandro Badin - Annunziata Fiorilli

23 maggio 2024

We are truly global…

In-country delivery

Near-shore delivery

Off-shore delivery

7 GLOBAL INDUSTRIES

- Automotive & Transportation
- Aerospace & Defense
- Information & Communication Technology
- Manufacturing & Logistics
- Banking & Financial Services
- Life Sciences & Healthcare
- Energy & Clean Technology

7 GLOBAL TECH PRACTICES

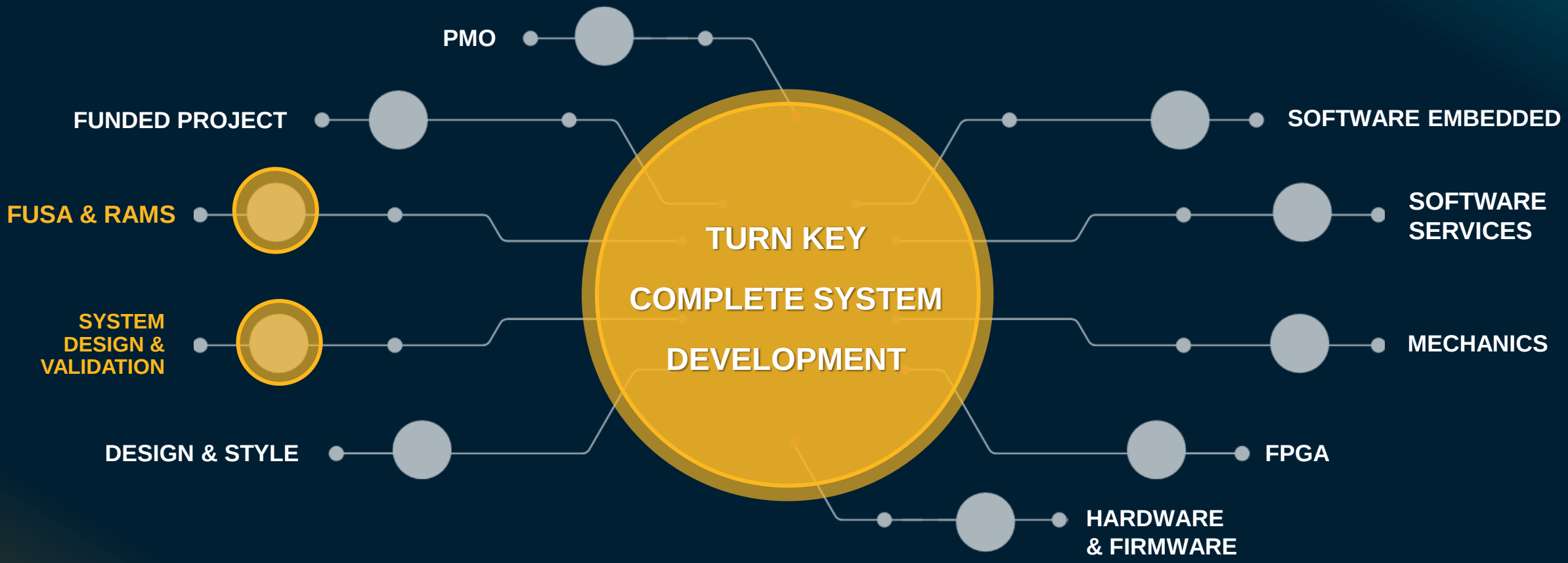
- Product & System Development
- Validation & Verification
- Manufacturing & operations
- Digital & Software
- Data Analytics & AI
- Cloud, Infrastructure & Security
- Wireless & Connectivity

4 SERVICE LINES

…and local, Akkodis in Italy

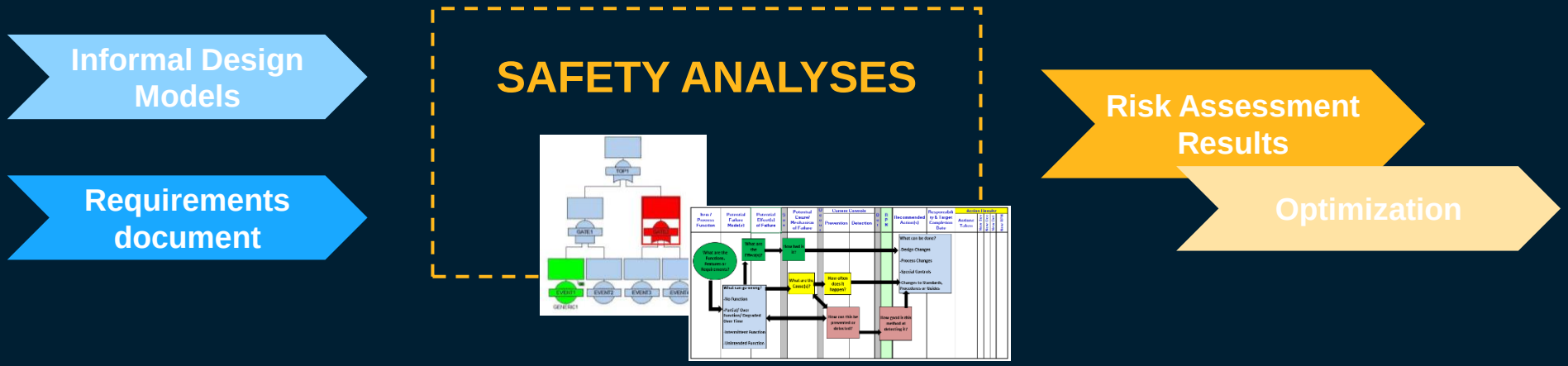
- **100+ M€** *Revenues*
- **1,600+** *talents*
- **16** *offices*
- **Leading Engineering, IT & R&D capabilities** *across several industries:*
  Life Sciences & Healthcare, Automotive, Aerospace & Defence, Railway, Naval, Telecomunication & Media, Industrial, Oil&Gas, Energy, Financial Services & Banking, Fashion

Technology & Innovation HUB



Introduction

Traditional Approach For Safety Analyses



System safety analysis techniques are well established and are used extensively during the design of safety-critical systems

These techniques are mostly subjective, and the result depends on the skill of the analyst

Introduction

Traditional Approach For Safety Analyses

- *Manual development of safety cases and safety analyses*, by using manufacturer templates (mainly in Office format).
- *Highly subjective analysis*, strongly dependent on the skill of the engineers/analysts.
- *Weak traceability of the safety analyses back to design artifacts,* by means of naming conventions or hyperlinks in development tools

Safety assessment process is document-based!

Introduction

Limits of the traditional approach

DIFFERENT RESULTS DEPENDING ON THE ANALYST

NOT COMPLETE, CONSISTENT, AND ERROR FREE RESULTS, DUE TO THE INFORMAL MODELS

TIME-CONSUMING, DUE TO A CONTINUOUS BRAINSTORMING BETWEEN SYSTEM AND SAFETY ENGINEERS

Model-based Development

Comparison with a traditional approach

In model-based development various development activities such as simulation, verification, testing are based on a formal model of the system under development. They strongly interact with all the development phases

TRADITIONAL ENGINEERING METHODS

Informal notation

Text-based documents

manual processes

MODEL BASED DEVELOPMENT

Formal notation (digital modeling and simulation to design systems)

Interactive process

Model-based Development

Benefits of Model Based development

COLLABORATION
BETWEEN STAKEHOLDER OF ALL THE DEVELOPMENT PHASE

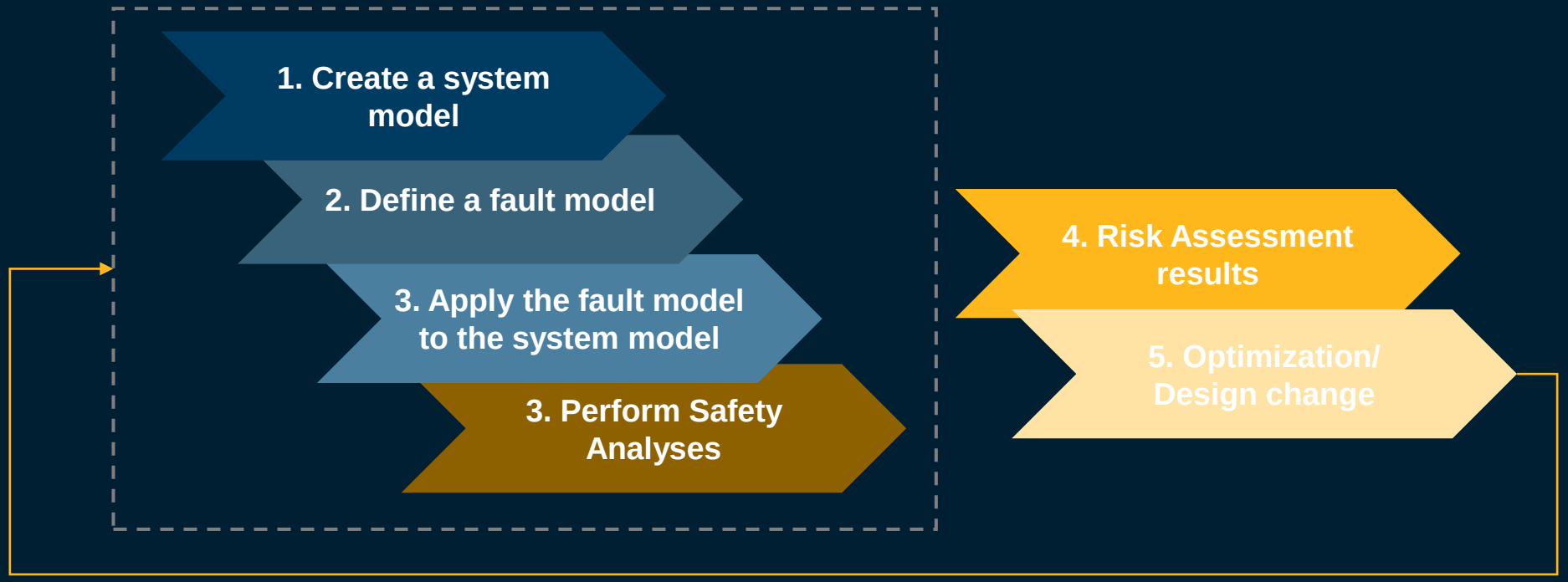
QUALITY IMPROVEMENT
ERROR REDUCED AND BETTER TRACEABILITY

SPEED UP DEVELOPMENT
THROUGH AUTOMATIC DEVELOPMENT PROCESS

GOOD ADAPTABILITY
TO DIFFERENT SIZES OF PROJECT COMPLEXITY

Model-Based Safety Analyses

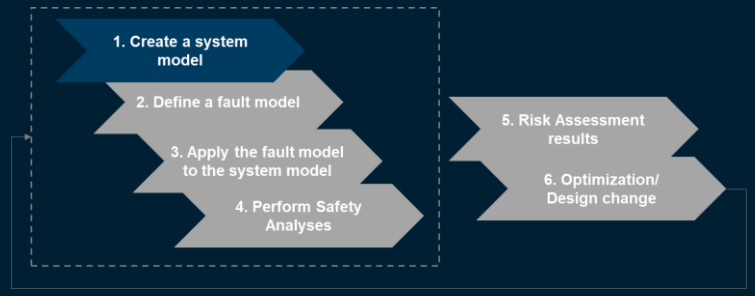
The approach



An approach for automating portions of the safety analysis process using executable formal models of the system

Model-Based Safety Analyses

The steps of the approach



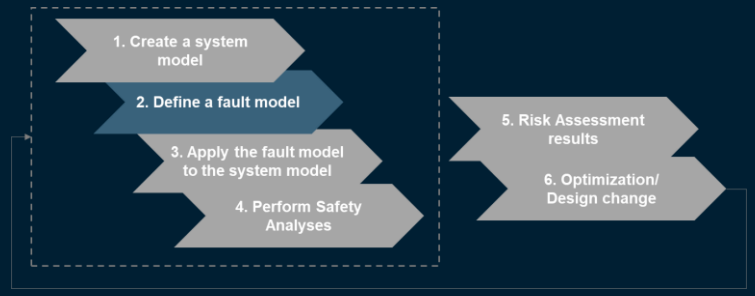
1. CREATE A SYSTEM MODEL

The system model with model-based notation define the nominal (non-failure) system behavior.

This means to define a set of formal properties to represent the (informal) safety requirements of the system

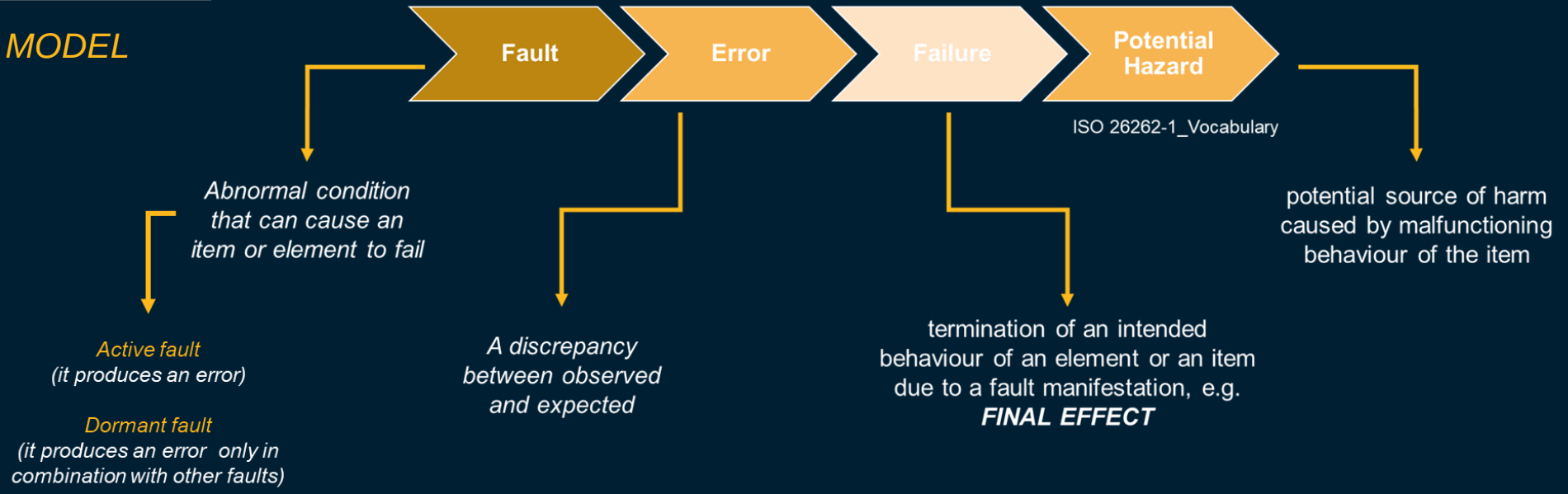
Model-Based Safety Analyses

The steps of the approach



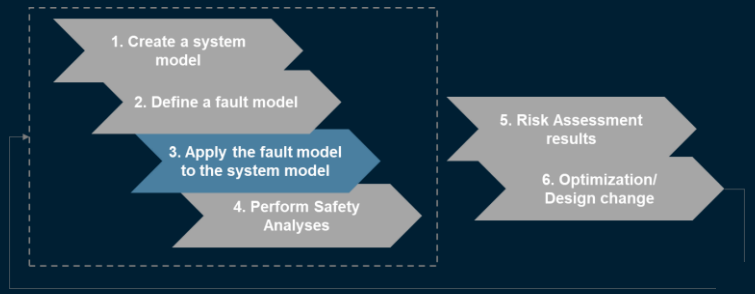
2. DEFINE A FAULT MODEL

The system model is augmented with the fault behavior of the system



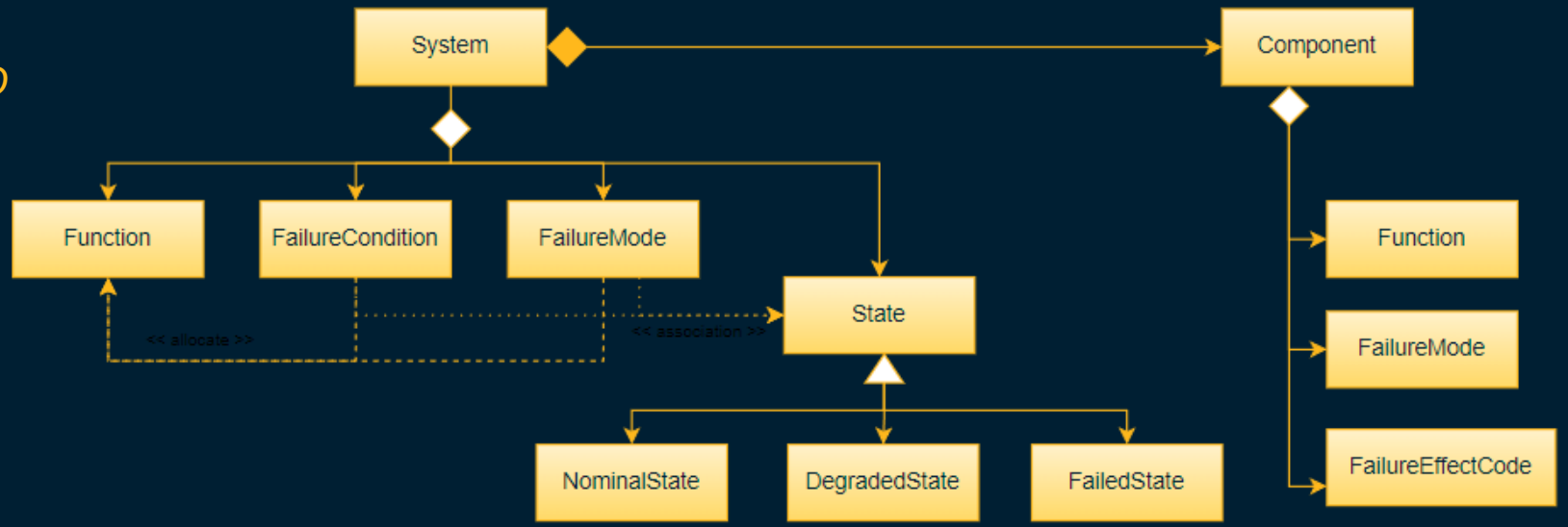
Model-Based Safety Analyses

The steps of the approach



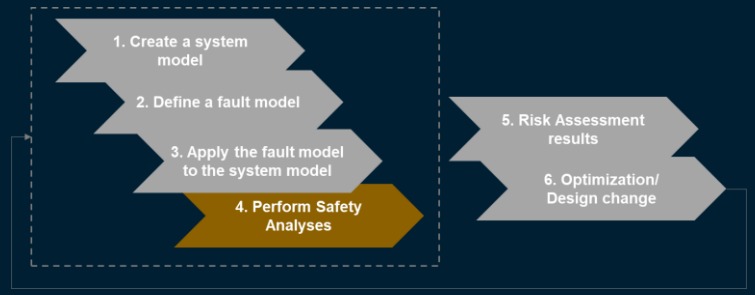
The fault model is automatically injected into the system model to to create a new extended model that foresee a degraded behaviour and understand the possible hazard

3. APPLY THE FAULT MODEL TO THE SYSTEM MODEL



Model-Based Safety Analyses

The steps of the approach



4. PERFORM SAFETY ANALYSES

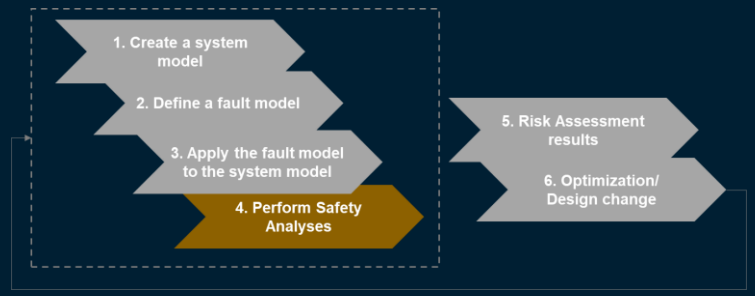
Once applied the fault model, the safety engineers uses formal analysis techniques to determine whether the proposed system architecture satisfies the safety properties (such as DFMEA, FTA).

Artifacts can be automatically generated from the model. This means:

- Fine-grained traceability between system model elements and elements of analysis models, such as FTA and FMEA
- Creation of FTA events directly from models
- Utilization of simulation for FMEA controlled fault injection

Model-Based Safety Analyses

System level Safety Analyses



4. PERFORM SAFETY ANALYSES

SYS Architectural Design

Safety Concept

- Definition of System Safety Concept
- Allocation of safety requirements onto preliminary architecture
- Trigger of safety analyses and collection of results

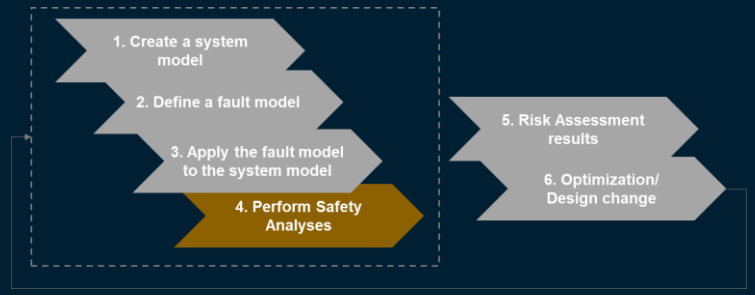
System Safety Analyses

- **DFMEA**
- **FTA**

The purpose of these analyses is to assist system engineer in the system design

Model-Based Safety Analyses

ISO 26262 requests for safety analyses



4. PERFORM SAFETY ANALYSES

Table 1 — System architectural design analysis

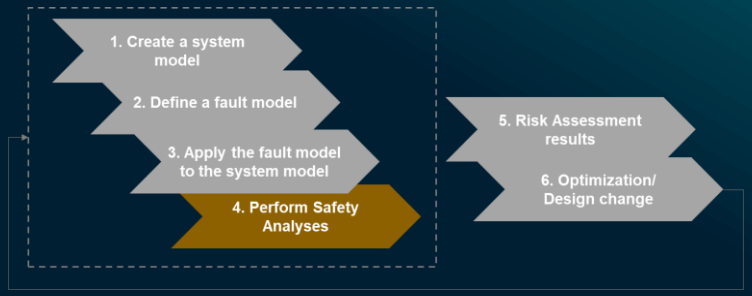
	Methods	ASIL			
		A	B	C	D
1	Deductive analysis	o	+	++	++
2	Inductive analysis	++	++	++	++

Highly recommended for all ASIL Levels (ASIL A to ASIL D)

Highly recommended for ASIL C and ASIL D

Model-Based Safety Analyses

Main techniques for Safety Analyses



4. PERFORM SAFETY ANALYSES

DFMEA

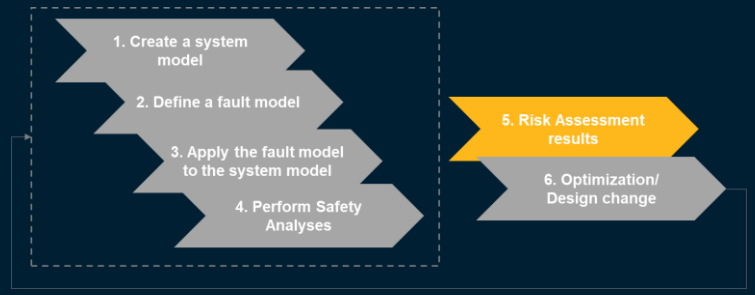
- ✓ Performed on architectural elements
- ✓ It is used to evaluate the completeness of Safety Mechanism against the design
- ✓ Action closure is used as a verification of SYS Design

FTA

- ✓ Performed on architectural elements
- ✓ It is used to evaluate the completeness of Safety Mechanism against the design

Model-Based Safety Analyses

The steps of the approach



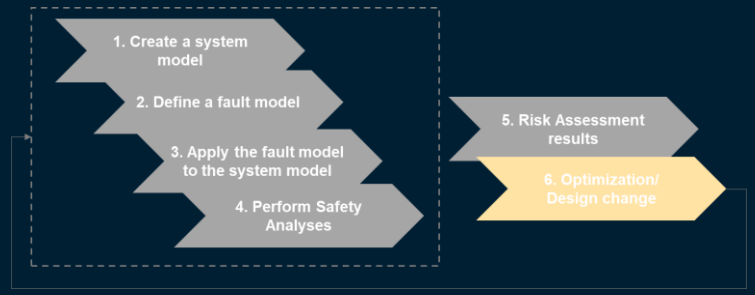
5. RISK ASSESSMENT RESULTS

Artifacts can be automatically generated from the model, including Risk Assessment Results

- Share a common model between system development and safety analyses ensures that safety analysis results are relevant and up-to-date as the system architecture evolves, and allows safety assessment early in the system design process.
- Moreover, the exploration of different architectures and design choices can be effortless

Model-Based Safety Analyses

The steps of the approach



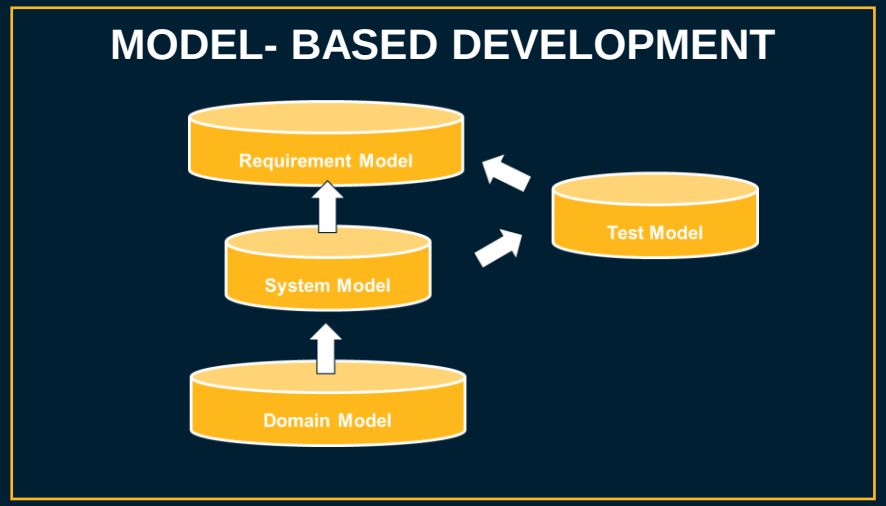
6. OPTIMIZATION AND DESIGN CHANGES

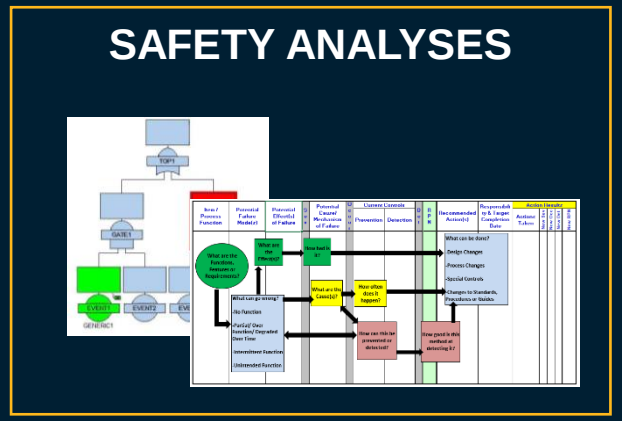
Optimization and design changes are managed by refining the system and the degraded models, or by reviewing the fault model

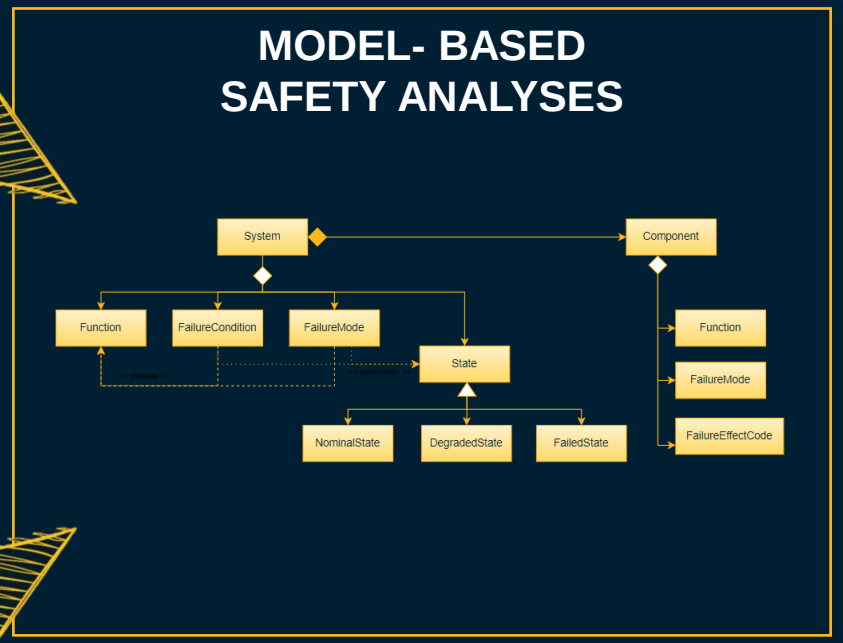
- Share a common model between system development and safety analyses ensures the traceability of changes
- Moreover, the automatic process helps the change process to be effortless

Model-Based Safety Analyses

Final Summary







Model-Based Safety Analyses

Benefits of the approach

INTEGRATION

Strong integration between systems and safety analysis based on common models of system architecture and failure modes

COMPLETE SIMULATION

Ability to simulate the behavior of system architectures early in the development process to explore potential safety hazards

Ability to exhaustively explore all possible behaviors of a system architecture with respect to some safety property of interest using automated analysis tools

TIME GAIN

The ability to automatically generate many of the artifacts that are manually created during a traditional safety analysis such as FTAs and FMEAs charts

FUSA & RAMS Delivery Unit

V-MODEL DESIGN & DEVELOPMENT

- Safety levels definition (SIL, ASIL, Plr)
- Safety Concept
- SYS/HW/SW Design and Development according to standard V-model cycle

SAFETY PROJECT MANAGMENT

- Management of a Functional Safety Project
- Customer Interface
- Safety Team coordination

SAFETY ANALISYS

- Hazard and Risk assessment
- RAMS Analysis
  - Reliability Analysis
  - DFMEA
  - FMEDA/FMECA
  - FTA
  - DFA
  - CMA / ZHA

STANDARD COMPLIANCE & SUPPORTING PROCESSES

- Gap Analysis
- Pre-assessment / Confirmation Measures
- Quality and FuSa pre-audit
- Process Implementation
- Quality/Safety Management
- Tool Evaluation
- Requirement Verification
- Technical Manual

TRAINING

- Technical and Methodological support via Classroom or on the job training.

Model-Based Safety Analyses

WHAT

System Design and Validation Delivery Unit

AKKODIS

Validation is the assessment of a planned or delivered system to meet the sponsor's operational need in the most realistic environment achievable

Systems Engineering is a **transdisciplinary** and **integrative** approach to enable the successful realization, use, and retirement of **engineered systems**, using **systems principles and concepts**, and scientific, technological, and management methods.

Main high reliability processes compliancy

ECSS | DO-178 | DO-254 | ISO26262 | CENELEC

SYSTEM MODELING is one the most cross functional engineering discipline which embraces a wide range of topics from the system physics modeling to control algorithm development.

TOOLS

MATLAB® python™ LAUTERBACH VECTOR CANTATA

Model-Based Safety Analyses

Thank you

Annunziata Fiorilli

FuSa & RAMS Delivery Unit Manager

annunziata.fiorilli@akkodis.com

Alessandro Badin

System Development Delivery Unit Manager

alessandro.badin@akkodis.com