

La tracciabilità delle safety analyses lungo il V-Model cycle

Annunziata Fiorilli – FuSa & RAMS Delivery Unit Manager

Bergamo, 30/05/2023

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



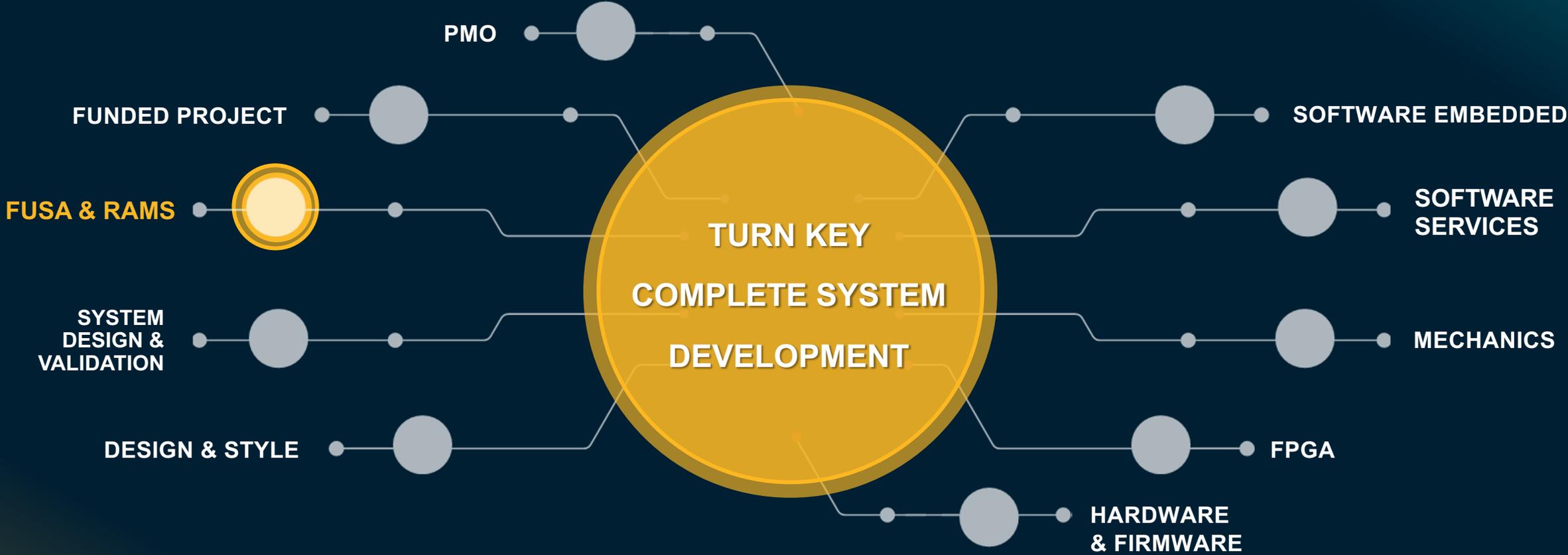
...and local, Akkodis in Italy

- 100+ M€ Revenues
- 1,500+ talents
- 16 offices
- **Leading Engineering, IT & R&D capabilities** across several industries:
Life Sciences & Healthcare, Automotive, Aerospace & Defence, Railway, Naval, Telecommunication & Media, Industrial, Oil&Gas, Energy, Financial Services & Banking, Fashion



Primo Meregalli







Safety Analyses

SAFETY ANALYSES

Lo sviluppo del progetto in 3 step



ANALISI DEI RISCHI

IDENTIFICAZIONE
FAILURE MODE PER LA
DEFINIZIONE
DELL'ARCHITETTURA DI
PROGETTO



IMPLEMENTAZIONE MISURE DI SICUREZZA

IMPLEMENTAZIONE HW
IMPLEMENTAZIONE SW



SAFETY VERIFICATION

FAULT INJECTION
VALUTAZIONE DELLE
METRICHE HW (FMEDA/FTA)

SAFETY ANALYSES

Lo sviluppo del progetto in 3 step



Lo sviluppo del progetto in 3 step: l'iterazione

ITERAZIONE

- revisione architettura
- identificazione ed implementazione delle modifiche
- Verifiche funzionali per garantire le performance
- Verifica sulla sicurezza funzionale (es, HW FMEDA)



Tempo sprecato nell'esecuzione della verifica della sicurezza

Necessità di ripetere l'iterazione attraverso l'analisi e l'inserimento della sicurezza

SAFETY ANALYSES

L'importanza di un approccio strutturato per la riduzione del rischio

STRUMENTO DI DESIGN
STRUMENTO DI VERIFICA

+ SAFETY DISPOSITIVO
- COSTI DI SVILUPPO

SAFETY ANALYSES

METODOLOGIE INDUTTIVE
METODOLOGIE DEDUTTIVE

ANALISI QUALITATIVE
ANALISI QUANTITATIVE

L'importanza di un approccio strutturato per la riduzione del rischio



- Prevenire/mitigare guasti sistematici introdotti dal processo di progettazione e sviluppo
- Prevenire/mitigare guasti randomici che possono verificarsi durante la vita operativa del sistema
- Inserire/valutare meccanismi e misure di sicurezza sufficienti
- Dimostrare che il progetto è sicuro

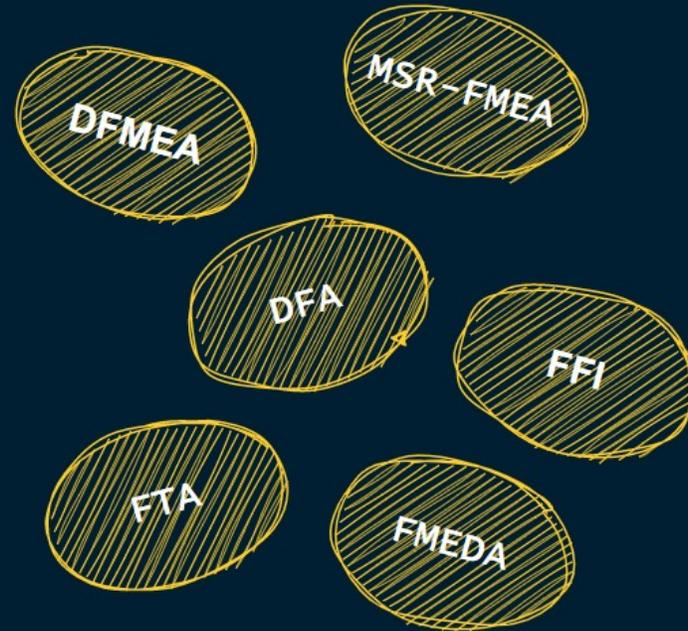
SAFETY ANALYSES

La tracciabilità delle safety analyses nel ciclo a V di sviluppo prodotto



SAFETY ANALYSES

La tracciabilità delle safety analyses nel ciclo a V di sviluppo prodotto



La tracciabilità delle safety analyses nel ciclo a V di sviluppo prodotto

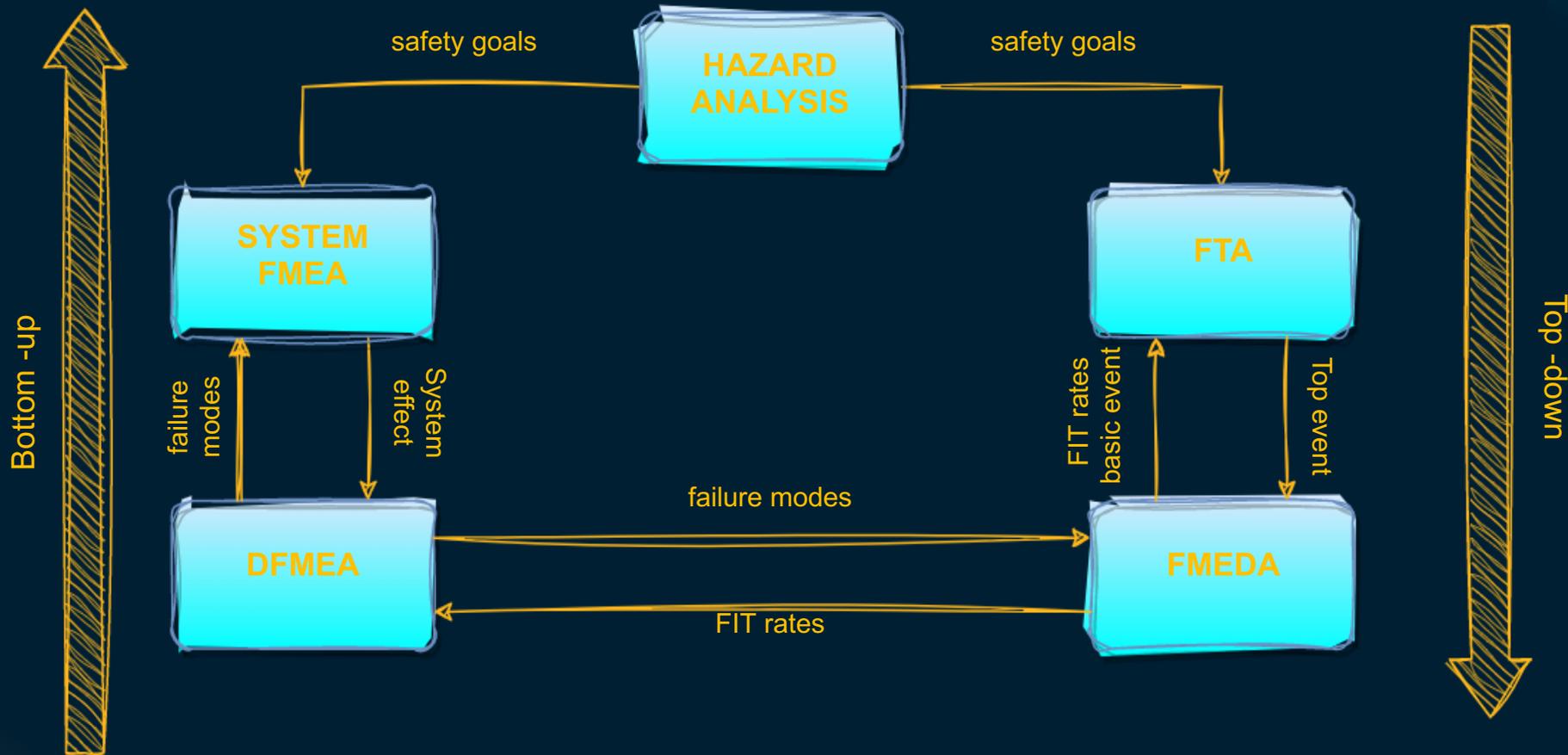
*«La **tracciabilità** è la proprietà di alcuni processi che producono un risultato di cui si vuole conservare la storia o le origini».*

Tale concetto è ben presente anche nella ISO 26262 lungo tutto il suo V-model.

*Realizzare la tracciabilità delle safety analyses significa integrare e gestire step by step con coerenza tutti i diversi tipi di analisi di sicurezza, garantendo con **semplicità** ed **efficacia** la massima copertura dei rischi nello sviluppo di un sistema.*

SAFETY ANALYSES

La tracciabilità delle safety analyses nel ciclo a V di sviluppo prodotto



Implementare la tracciabilità delle Safety Analyses

...per riassumere, raggiungere un processo tracciabile di safety analyses vuol dire:

-  Definire correttamente il sistema e i suoi livelli di sviluppo
-  Chiare le richieste del cliente finale
-  Identificare lo stato dell'arte, raccogliendo standard e linee guida
-  Ragionare sulle dimensioni dell'azienda
-  Scegliere i tool corretti

FUSA & RAMS Delivery Unit

The Team

15 Engineers

20+ YEARS OF
EXPERIENCE

- AEROSPACE
- AUTOMOTIVE
- MACHINERY
- RAILWAY



TECHNICAL FIELD

Functional Safety

STANDARD

- IEC 61508
- ISO 26262
- ISO 25119
- ISO13849
- ISO14971, IEC 62304
- EN50126/8/9

TOOLS

- Medini Analyze
- Reliability Workbench
- IQ RM Pro
- Doors

RAMS

- SN29500
- IEC 62380
- MIL-STD-217F
- ARP std
- FMEA Handbook

Quality Management

- ISO 9001
- IATF16949
- ISO 13485

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
 - FMEA (sys, sw, hw)
 - FMEDA/FMECA
 - FTA
 - DFA
 - FFE
 - CMA
 - ZHA

STANDARD COMPLIANCE & SUPPORTING PROCESSES

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

TRAINING

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



Thank you

Annunziata Fiorilli

M +39 344 039 9750

E annunziata.fiorilli@akkodis.com

