Metodi di Progettazione - 4

FACOLTÀ DI INGEGNERIA
CIVILE E INDUSTRIALE

SAPIENZA
UNIVERSITÀ DI ROMA

Costanzo Pietrosanti

IL PROCESSO DI PROGETTAZIONE
ISO 9001 e Risk Analysis

Fonte: Austin Howard, University of Idaho, Mechanical Engineering Dept.,Idaho Space Grant Consortium, “Introduction to Risk Assessment in Engineering: With Application to Heat Shield Reliability Modeling”

ISO 9001: 2015 e Risk Analysis

- Con la revisione 2015 la Normativa ISO 9001 adotta un l'approccio sistematico alla **gestione del rischio** integrato nei processi che vengono analizzati, in particolare nel processo di progettazione.
- L'obbiettivo consiste nel rendere l'organizzazione proattiva, prevenendo o riducendo gli effetti indesiderati e promuovendo il miglioramento continuo.

http://www.bsigroup.com/LocalFiles/it-IT/ISO%20REVISION/2-9001_importanza%20del%20rischio%20nella%20gestione%20della%20qualit%C3%A0.pdf

Concetto di approccio basato sul rischio - 1

Requirement 4

All'organizzazione è richiesto di **determinare i rischi** che possano influenzare la sua capacità di raggiungere gli obiettivi e le conseguenze specifiche e generali sull'impresa.

A seconda della natura dell'Impresa, le conseguenze di erogare un servizio o lanciare un prodotto non conforme possono essere limitate, per altre posso essere fatali.

Un sistema basato su rischi implica la valutazione sia ***qualitativa*** che ***quantitativa*** del rischio in base al contesto del business.

Tale approccio mette in luce anche le ***opportunità,*** qualora esistano.

Concetto di approccio basato sul rischio - 2

Requirement 5

Il Top Management deve essere coinvolto e deve esercitare la sua leadership nell'assicurare che i rischi e le opportunità che possono effettivamente interessare la conformità del prodotto o del servizio siano state determinate e affrontate.

A che cosa?

Ai **Requirement** espressi esplicitamente ed implicitamente dal **Cliente** e dagli **Stakeholders** (gli interessati, es. conformità a normative, alle norme di buona Ingegneria ecc.)

Concetto di approccio basato sul rischio - 3

Requirement 6

Le organizzazioni devono intraprendere azioni per identificare rischi e opportunità e pianificarne la gestione.

Requirement 8

L'organizzazione deve pianificare, implementare e controllare i suoi processi e di indirizzare le azioni di gestione identificate nel Requirement 6.

Requirement 9

L'organizzazione deve monitorare, misurare, analizzare e valutare i rischi e le opportunità.

Il ciclo di Deming ed il Rischio

Identificare rischi e opportunità – in relazione al contesto dell'organizzazione e alla sua attitudine ad assumersi rischi.

Analizzare **e stabilire le priorità di** rischi e opportunità. Cosa è accettabile, cosa non lo è? Quali vantaggi e quali svantaggi comporta un processo piuttosto che un altro?

Pianificare le azioni per indirizzare i rischi. Come i rischi possono essere evitati, mitigati o eliminati?

Implementare il piano. Intraprendere le azioni necessarie. Controllare l'efficienza delle azioni. Questo processo funziona?

Verificare l'approccio, imparare dall'esperienza, migliorare continuamente e considerare opportunità innovative.

Act
Implementare i cambiamenti nell'approccio e continuamente rivedere le opportunità di miglioramento

Plan
Aumentare l'impegno della leadership.
Identificare e valutare i rischi.
Creare un piano per indirizzare rischi e opportunità

Check
Monitorare i piani attraverso la misurazione, gli audit interni e la reportistica

Do
Implementare il piano per mitigare i rischi. Attraverso la comunicazione, il training e i controlli

Concetto di approccio basato sul rischio

Obbiettivi:

- Descrivere l'importanza del Risk Assessment
- Introdurre concetti, strumenti e processi connessi con la Risk Analysis

Concetto di approccio basato sul rischio

Definizione di Rischio:

- La combinazione di frequenza (o probabilità) di accadimento e le conseguenze di specifici eventi pericolosi
- Un modo per calcolarlo consiste nel semplice prodotto tra I fattori:

$$R = P_a \times S$$

R = Rischio
P_a = Probabilità di accadimento
S = Gravità delle conseguenze

Rischio e Affidabilità

Il Rischio è spesso confuso con la mancanza di Affidabilità

Affidabilità

Probabilità che un Manufatto o un Sistema funzioni senza rotture o malfunzionamenti per uno specifico intervallo temporale o numero di cicli

- L'Affidabilità è uno dei fattori che contribuiscono alla determinazione del Rischio
- L'Analisi di Affidabilità è spesso usata al posto dell'Analisi del Rischio ma i due concetti sono differenti; ciò è dovuto alla difficoltà nella misura e quantificazione della severità delle conseguenze di un accadimento pericoloso

Rischio e Sicurezza

Il Rischio è spesso confuso con la mancanza di Affidabilità

La valutazione del Rischio è quantitativa *e si basa sulle prove e sulla modellazione fisica*

La valutazione dei ***Rischi legati alla Sicurezza*** *si avvale spesso dell'esperienza e della sensibilità degli analisti risultando talvolta qualitativa; l'approccio sui grandi numeri (es. casistica incidentale) non rende spesso ragione della specificità di alcune situazioni.*

Tuttavia, con riferimento all'HS&E (Health, Safety and Environment), la valutazione gode di approcci Big Data con le relative analisi di valutazione e validazione (vedi OHSAS (Occupational Health and Safety Assessment Series) 18001.

Failure

Failure = Fallimento (è un Evento)

Es. FAILURE: La valvola non funziona in quella situazione ed in quel momento

1. ***La parola Failure Mode definisce uno stato del Sistema in analisi***
   Es.: non è possibile raffreddare il componente, il rubinetto della valvola è bloccato

2. ***Un Failure Mechanism è il processo con cui la Failure avviene***
   Es.: la valvola non si apre perché lo stelo si è corroso nel tempo

Descrizione dell'Evento	Sistema	Sotto-Sistema	Valvola	Attuatore
Nessun flusso arriva dai sotto-sistemi quando è richiesto	Meccanismo	Modo	Effetto	
Valvola bloccata		Meccanismo	Modo	Effetto
Bloccaggio dello stelo dell'attuatore			Meccanismo	Modo
Corrosione dello stelo dell'attuatore				Meccanismo

Modello Deterministico e Non-Deterministico

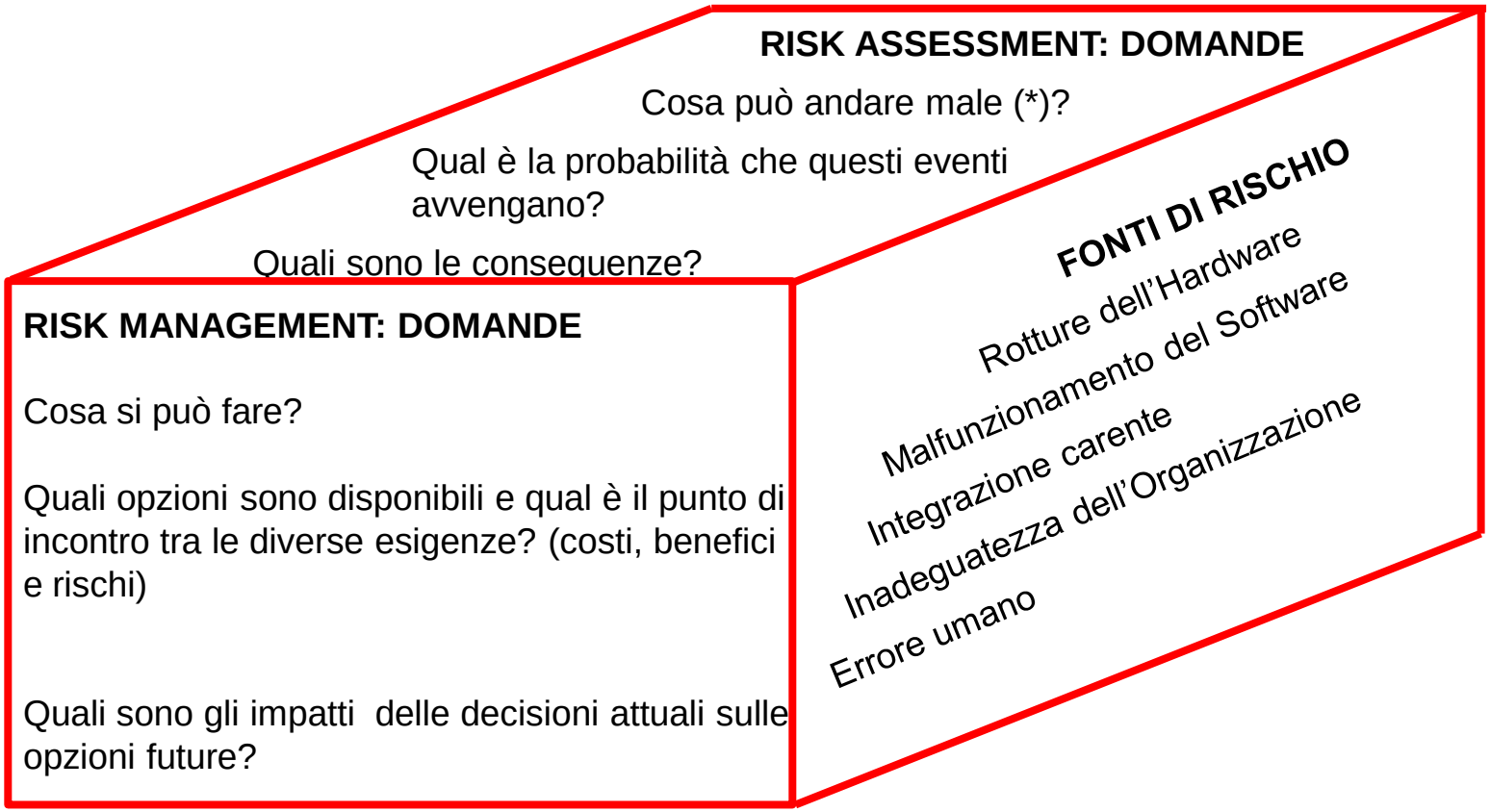
Un Modello di Rischio o di Affidabilità è deterministico quando consente di fare predizioni quantitative univoche

(ad uno stesso input corrisponde uno ed un solo output)

Un modello è non-deterministico quando presenta uno o più punti di scelta dopo i quali più strade risultano percorribili

(ad uno stesso input corrispondono più output; es. elaborazione on line di set di dati rilevati da sistemi affetti da errori dipendenti da cause diverse)

Concetto di Total Risk Management - TRM



Haimes, Yacov Y. *Risk Modeling, Assessment, and Management.* Hoboken, NJ, USA: John Wiley & Sons, Incorporated, 2005. p 23. http://site.ebrary.com/lib/uidaho/Doc?id=10114200&ppg=47

(*) Occorre aprire una parentesi sul principio di Murphy

Alcuni ulteriori fattori

Per effettuare un buon Risk Assessment occorre avere presenti il seguente principio fondamentale ed il suo lemma:

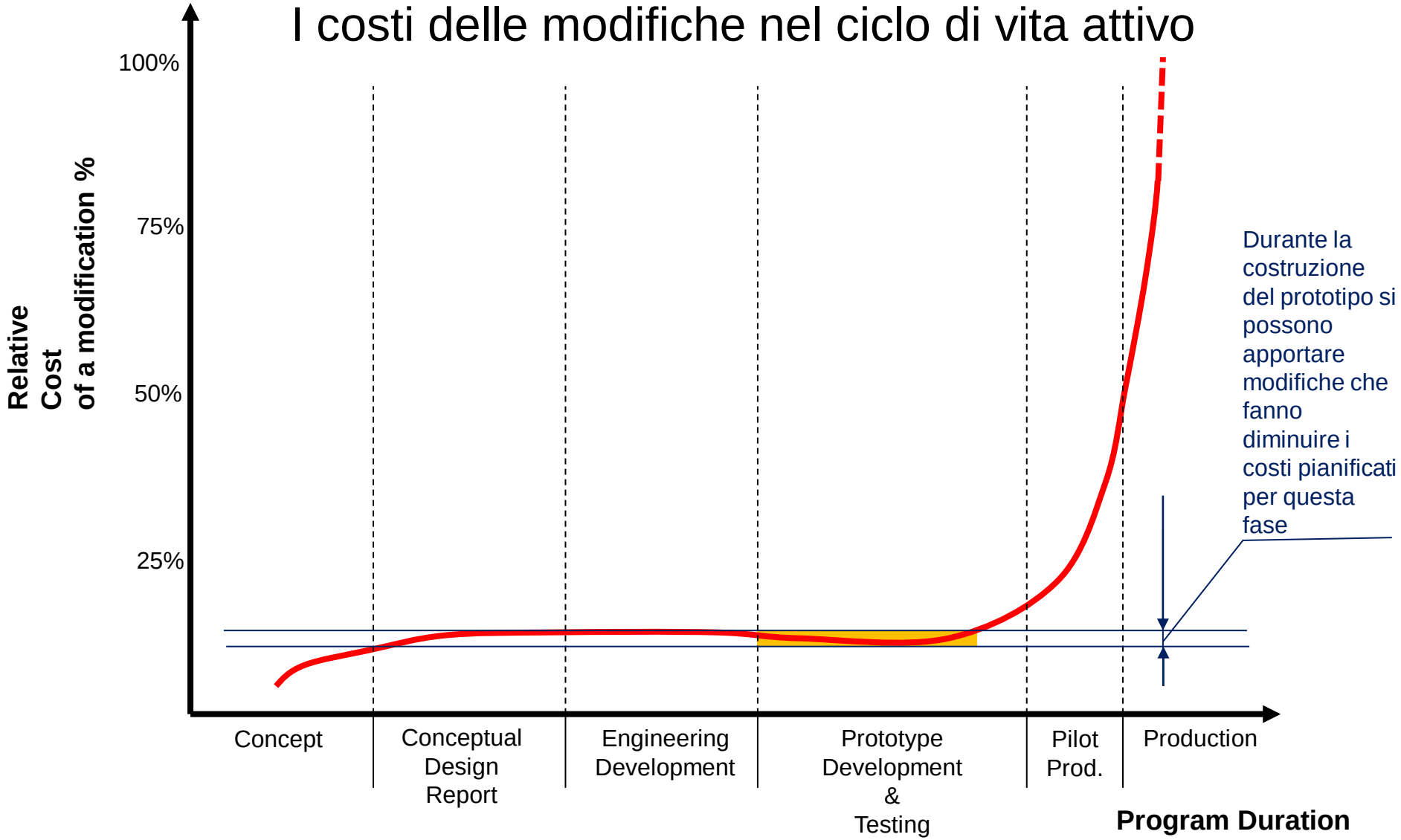
Il Principio di Murphy
Se qualcosa può andare storto, sicuramente lo farà.

Il Primo Lemma
Se esistono due modi per fare una cosa, quello giusto e quello sbagliato, qualcuno nel team adotterà sicuramente il secondo.

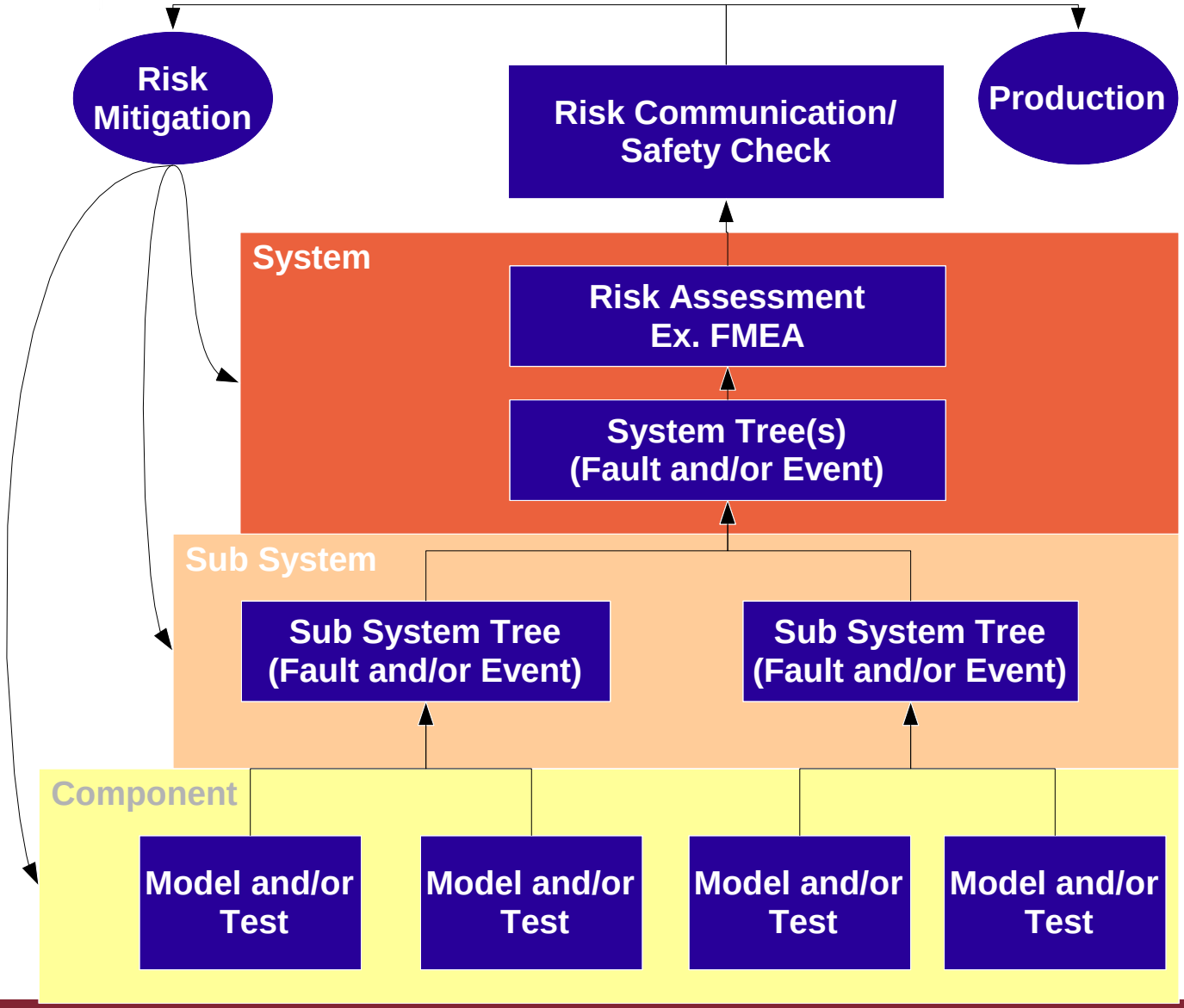
Murphy – Ingegnere Aeronautico, 1949

L'importanza della Valutazione del Rischio

I costi delle modifiche nel ciclo di vita attivo



Sequenza di Processo



Failure Mode and Effect Analysis (DFMEA)

- Concetti della stessa famiglia:
  - Failure Mode & Effect Analysis (FMEA)
  - Design Failure Mode & Effect Analysis (DFMEA)
  - Process Failure Mode & Effect Analysis (PFMEA)
- Scopo
  - Definire e guidare la logica del processo di progettazione
  - Identificare, quantificare e ridurre I rischi in fase di progettazione
  - Predisporre la tracciabilità del processo di Progettazione e sviluppo
  - Documentare e motivare le attività di progettazione
  - Predisporre I documenti per il continuo miglioramento del prodotto
- L'FMEA è un metodo induttivo (Forward Analysis)

Failure Mode and Effect Analysis (DFMEA)

Fase 1: definizione di una **metrica** (scala di valutazione delle variabili)

- Severity (es. rate 1-10) — Gravità delle conseguenze
- Occurrence (es. rate 1-10) — Numero di Accadimenti
- Detectability es. (rate 1-10) — Modalità di rilevamento

- Il prodotto dei parametri considerati è chiamato **RPN**, questo valore descrive il rischio globale di ogni *meccanismo di failure (fonte di rischio)*

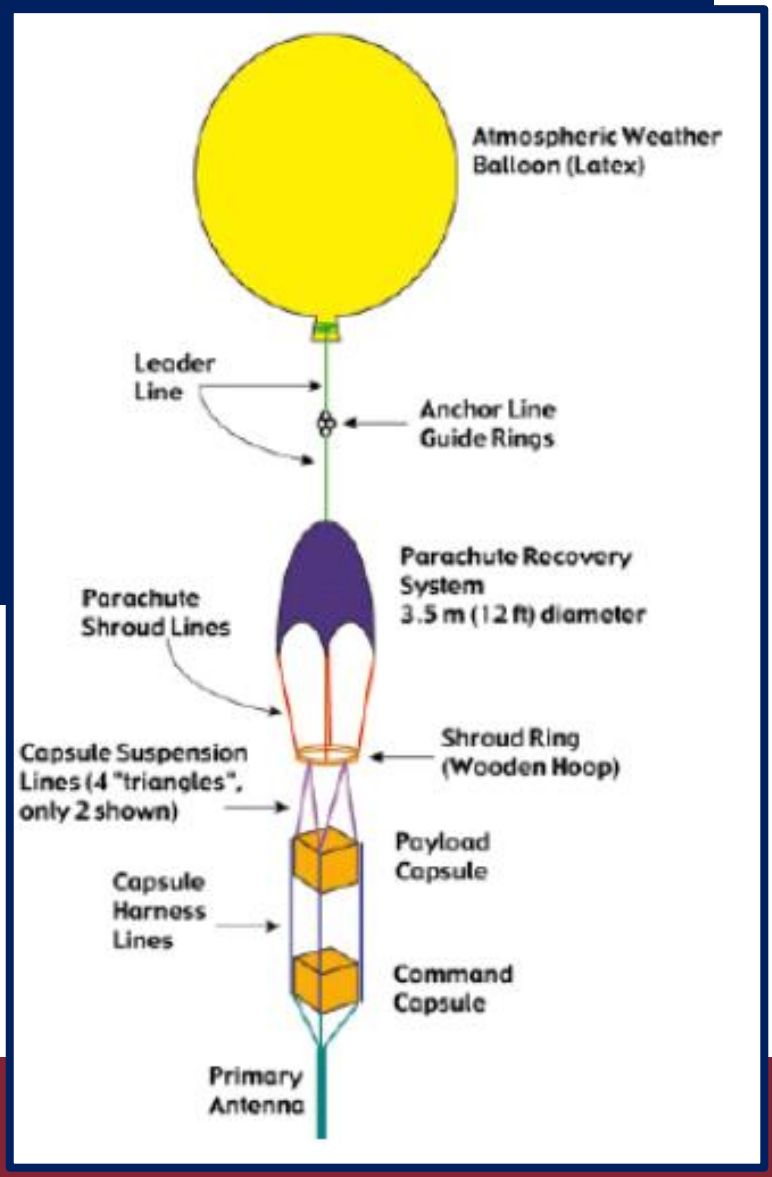
- Alti RPN = Rischi elevati
- Inizio del processo di mitigazioni di rischio con la focalizzazione dei meccanismi di *failure* più importanti

Failure Mode and Effect Analysis (DFMEA)

Fase 2: identificazione dei possibili incidenti e delle variabili per la determinazione dell'RPN

- Definizione del Team di esperti per l'effettuazione dell'FMEA
- Preparazione della tabella FMEA riportando le Funzioni del Sistema e dei sotto-sistemi e componenti

CASE STUDY
Balloon-Sat for
Weather Data Collection



Failure Mode and Effect Analysis (DFMEA)

Fase 3

Analisi e Valutazione per mezzo di una Round Table del Team di Progetto = Team di Valutazione FMEA

Identificazione delle:

1. Potenziali modalità di incidente (Potential failure Modes - cosa può andare male?)
2. Potenziali cause di rottura (Potential cause modes – cosa si è rotto all'origine?)
3. Potenziali conseguenze

Failure Mode and Effect Analysis (DFMEA)

Fase 4

Identificazione delle:

1. Azioni previste e sistemi per la mitigazione del rischio
2. Valutazione di Severity, Occurrence, Detectability in accordo alla metrica predeterminata.

Fase 5

1. Predisposizione di ulteriori eventuali misure
2. Valutazione della nuova situazione.

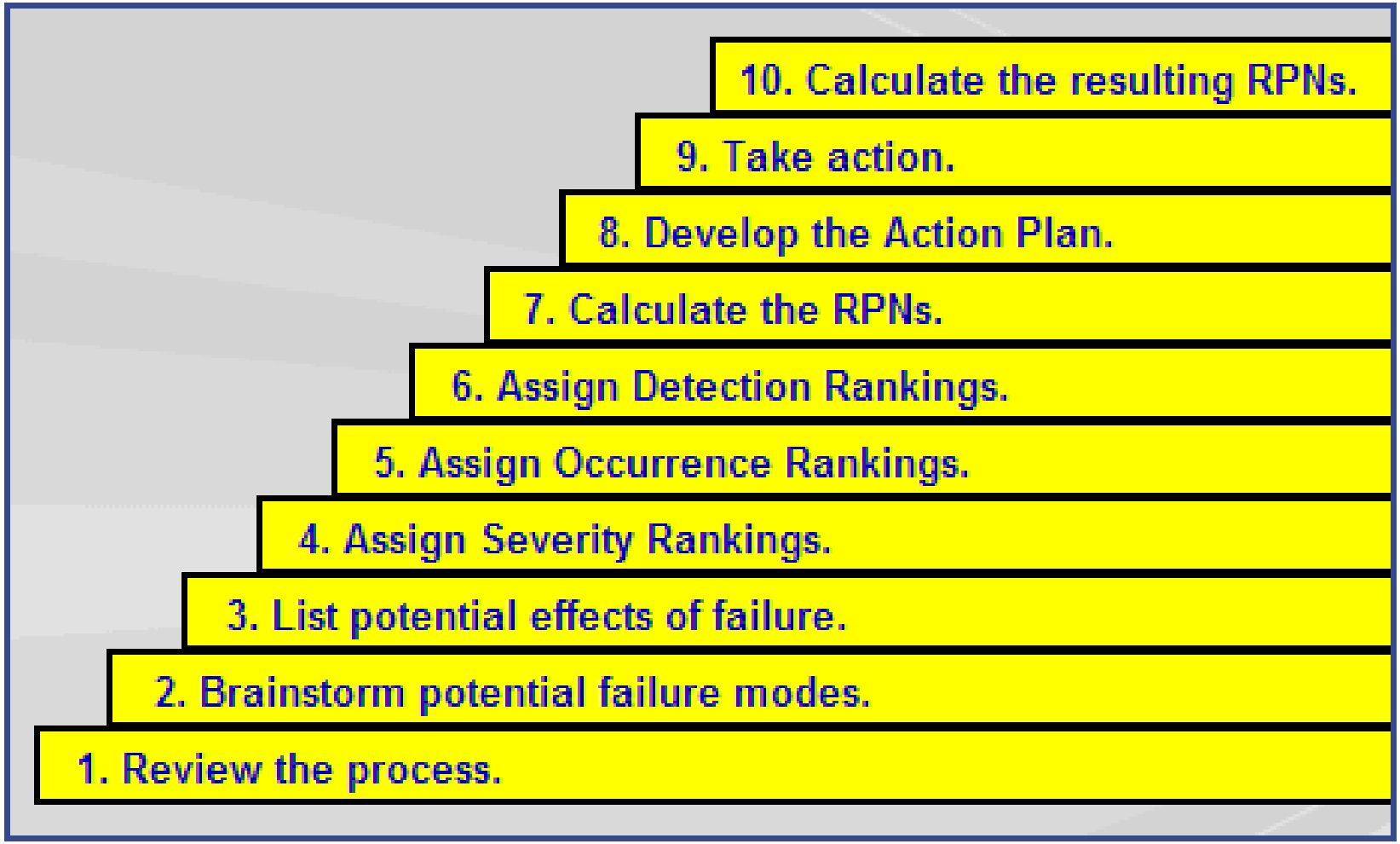
Failure Mode and Effect Analysis (DFMEA)

Tabella FMEA e individuazione delle possibili modalità di incidente

ITEM AND FUNCTION	POTENTIAL FAILURE MODE(S	POTENTIAL EFFECT(S) OF FAILURE	SEV	POTENTIAL CAUSE(S) OF FAILURE	OCCUR	CURRENT DESIGN CONTROLS	DETECT	RPN	RECOMMENDED ACTIONS	ACTION RESULTS				
										ACTION TAKEN	SEV	OCCUR	DETECT	RPN
Balloon	Premature Burs	Unreliable data	7	Bad Balloon	2	Notifying FAA	10	140	Buy newly made balloon/ write code to detect and deploy parachute	Buy newly made balloon, don't touch	7	1	10	70
Data Collection	Sensors fail	Unreliable data	8	Low Temperature, Power Failure, faulty sensor	2	Redundancy, Insulation/ Heating Pads, Testing	2	32	Add Insulation, replace bad sensors, calibrate	Moored testing	8	2	1	16
	Memory fails	No stored data	5	Short/ Programming error	2	Testing	2	20	Fix short, Test	Bench testing	5	1	2	10
	Radios fail	No telemetry/ loose redundant tracking	9	Power, Signal Blockage, Weak signal	2	Redundancy, Testing	5	90	Change antenna position	None	9	2	5	90
Tracking	GPS Failure	Cannot find probe	9	Power, Low Temp, Shorts, Programming, Poor reception	3	Redundancy, Testing	4	108	Increase Insulation, fix shorts, repsoition antenna	None	9	3	4	108
	Radios	Cannot find probe	10	Power, Low Temp, Shorts, Programming, Signal failure	3	Redundancy, Testing	5	150	Increase Insulation, fix shorts	Testing	10	2	5	100

Radios = Comunicazioni in radiofrequenza e relativo apparato

Summary: Failure Mode and Effect Analysis (DFMEA) Sequence



Fault Tree Analysis (Analisi con l'Albero dei Guasti)

La FTA è una tecnica che correla, usando collegamenti logici (porte logiche), gli eventi che provocano un determinato malfunzionamento.

L'analisi che ne consegue è detta FMECA (Failure Mode, Effect, and Criticality Analysis.

L'FTA è un metodo deduttivo (Backward Analysis)

Lo avete già visto in altri corsi, qui ci interessa metterne in luce gli aspetti procedurali rilevanti per la progettazione e richiesti dalla ISO9001:2015

L'FTA - 2

La FTA genera un modello di eventi di tipo gerarchico, permettendo di individuare i percorsi degli eventi che possono provocare malfunzionamento o rotture dei sistemi meccanici e valutarne le probabilità. Si adotta una procedura *Top-Down* a partire da un evento considerato.

- In cima all'albero dei guasti c'è un evento (*top failure, top event*) che comporta la completa rottura e uscita dal servizio di un Sistema.
- Al di sotto ci sono tutti i possibili eventi che conducono alla *top failure.*
- L'FTA è utilizzata per avere una visione del Sistema e delle interazioni tra eventi di *failure* ed i possibili percorsi che portano al *top event*.
- L'FTA può essere utilizzato per generare un modello probabilistico per la stima quantitativa dell'affidabilità.

Failure vs. Fault

- **Gli eventi di base o primari sono chiamati FAILURES se si riferiscono a componenti**
- **Gli eventi intermedi in un FT sono chiamati FAULTS**
- **Nel caso di FAULT di un COMPONENTE, questo ha ricevuto un comando che non ha soddisfatto**
- **Nel caso di FAULT di un SISTEMA questo può anche non averlo ricevuto.**

L'FTA - 3

I cammini percorribili dal basso alla cima (*bottom to top*) dell'albero sono detti ***cutset***, il più corto ***cutset minimo.***

ESEMPIO

Contesto: Eventi pericolosi (*Hazard*) legati alla guida di una vettura

Top Events:

1. Ribaltamento del veicolo a seguito di fuoriuscita dalla strada (svio)
2. Impatto contro un albero a seguito di svio

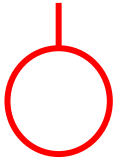
Elementi dell'analisi:

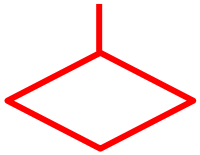
1. Condizioni sulla strada
2. Condizioni fuori dalla carreggiata
3. Veicolo
4. Guidatore

L'FTA – 4: Costruire il Fault Tree - Simbologia

Top Event l'evento primario indesiderato di interesse dell'FTA

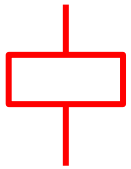
Basic Event un evento che non richiede ulteriori sviluppi





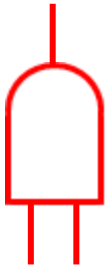
Undeveloped Event un evento che non ha ulteriori sviluppi e di limitate conseguenze oppure di cui si hanno pochi dati disponibili

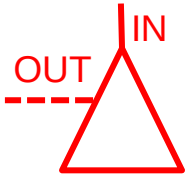
Intermediate Event un evento indesiderato che ha ulteriori sviluppi.



Porta OR indica che gli eventi in output accadono soltanto se accade uno o più eventi di quelli indicati in input

Porta AND la porta AND indica che l'evento in input accade se tutti gli eventi in input si verificano.

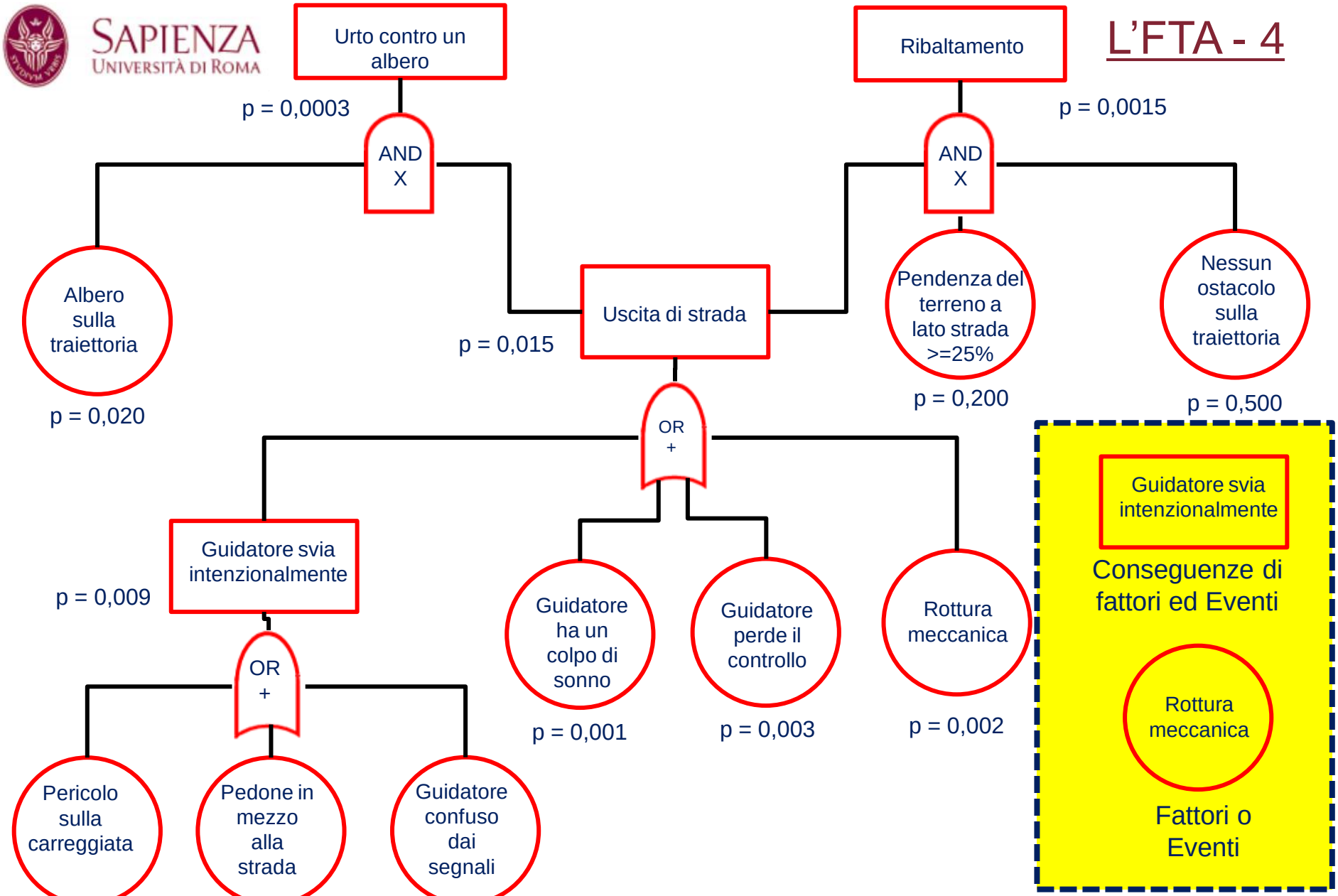




Porta TRANSFER (IN o OUT) trasferisce a/da un'altra parte dell'albero

Haimes, Yacov Y. *Risk Modeling, Assessment, and Management.* Hoboken, NJ, USA: John Wiley & Sons, Incorporated, 2005. p 530. http://site.ebrary.com/lib/uidaho/Doc?id=10114200&ppg=554

L'FTA - 4


Urto contro un albero
p = 0,0003
AND X
Albero sulla traiettoria
p = 0,020
Uscita di strada
p = 0,015
Ribaltamento
p = 0,0015
AND X
Pendenza del terreno a lato strada >=25%
p = 0,200
Nessun ostacolo sulla traiettoria
p = 0,500
OR +
Guidatore svia intenzionalmente
p = 0,009
OR +
Pericolo sulla carreggiata
p = 0,002
Pedone in mezzo alla strada
p = 0,006
Guidatore confuso dai segnali
p = 0,001
Guidatore ha un colpo di sonno
p = 0,001
Guidatore perde il controllo
p = 0,003
Rottura meccanica
p = 0,002
Guidatore svia intenzionalmente
Conseguenze di fattori ed Eventi
Rottura meccanica
Fattori o Eventi

Outline: FTA – Event Tree - 5

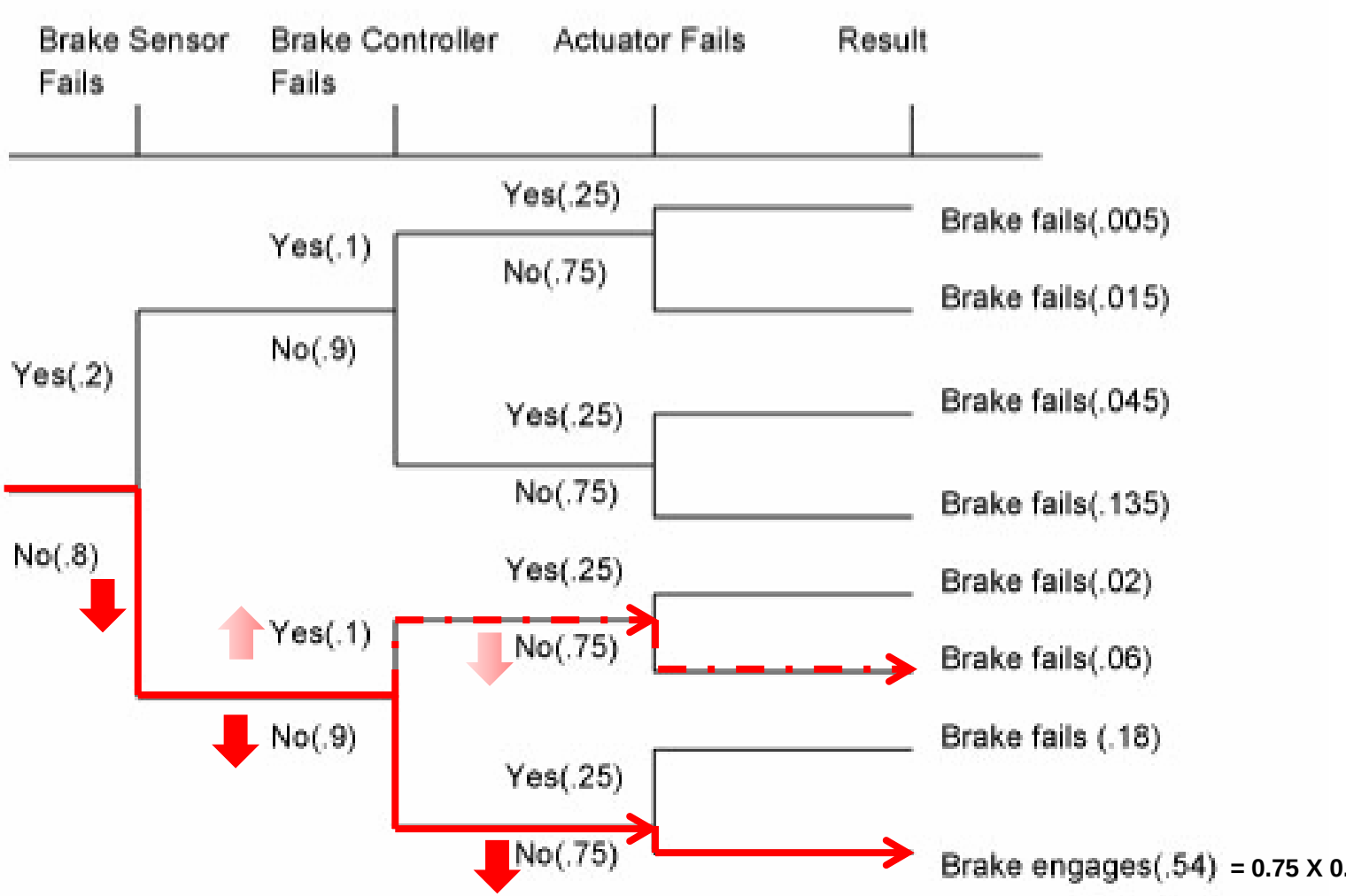
Obbiettivi dell'Albero degli Eventi

Determinare la probabilità di un evento principale a partire dalla probabilità di ogni evento di base nella sequenza degli eventi che portano a quello di più alto livello.

Determinare le sequenze degli eventi che conducono ad un risultato accettabile scegliendo la soluzione ottimale

L'Albero degli Eventi può essere costruito utilizzando un modello che permetta la stima dell'affidabilità.

Outline: FTA – Event Tree - Esempio

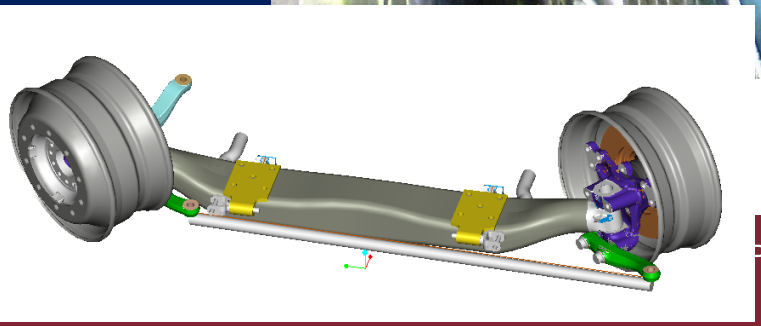


= 0.75 X 0.9 X 0.8

Le condizioni sono tutte di OR, quindi la probabilità totale è data dal prodotto della probabilità dei singoli eventi

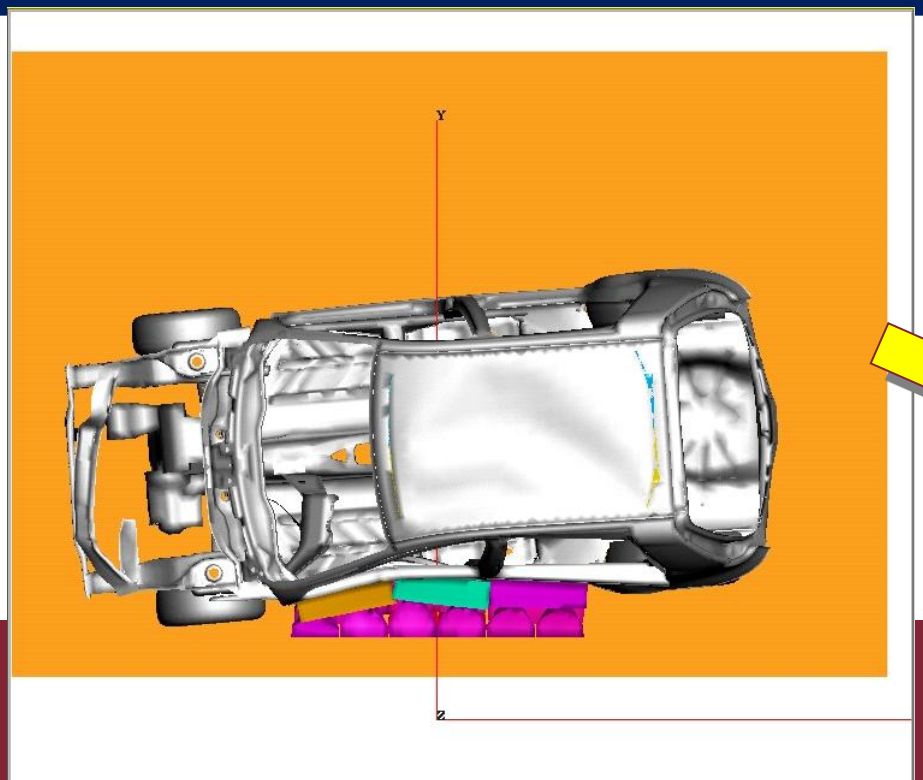
Valutazione dell'affidabilità: approccio sperimentale

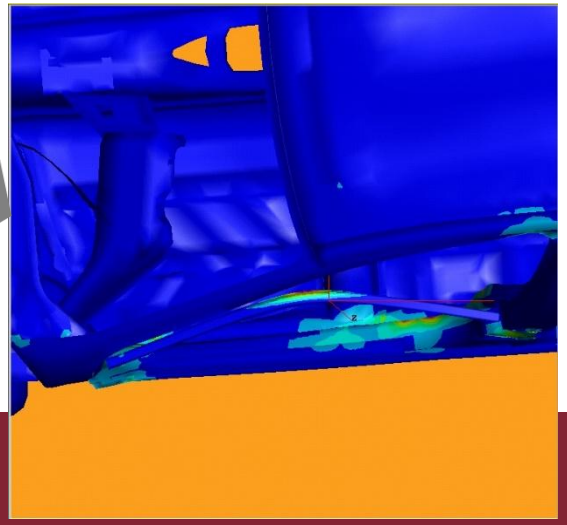
- **Vantaggi**
  - Può evidenziare cause di rottura trascurate
  - Alcune situazioni possono essere modellate solo dopo aver compreso accuratamente la fisica del fenomeno in studio
    - Es. Turbolenza
- **Limiti**
  - Costoso
  - Time consuming
  - Richiede una grande massa di data per poterne comprendere il significato



Valutazione dell'affidabilità: approccio modellistico

- **Vantaggi**
  - È veloce e poco costoso
- **Limiti**
  - È facile fare assunzioni imprecise o scorrette
  - Alcuni fenomeni non possono essere modellizzati

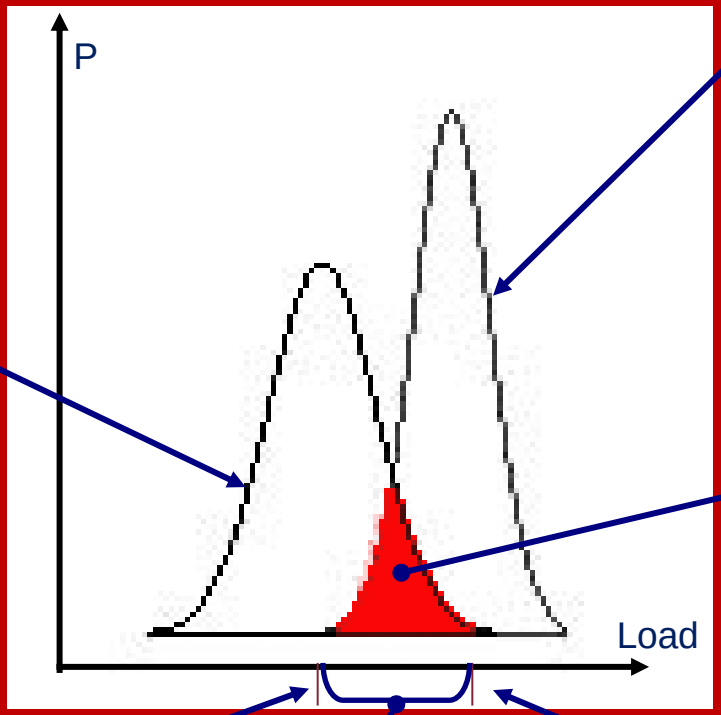




Come la modellistica fisica può produrre inaffidabilità

Curva di probabilità della progettazione (Design Probability Curve)

Incertezza sui carichi e sui vincoli (Load Probability Curve)



Area = Probabilità di rottura (Failure Proability Area)

Carico medio

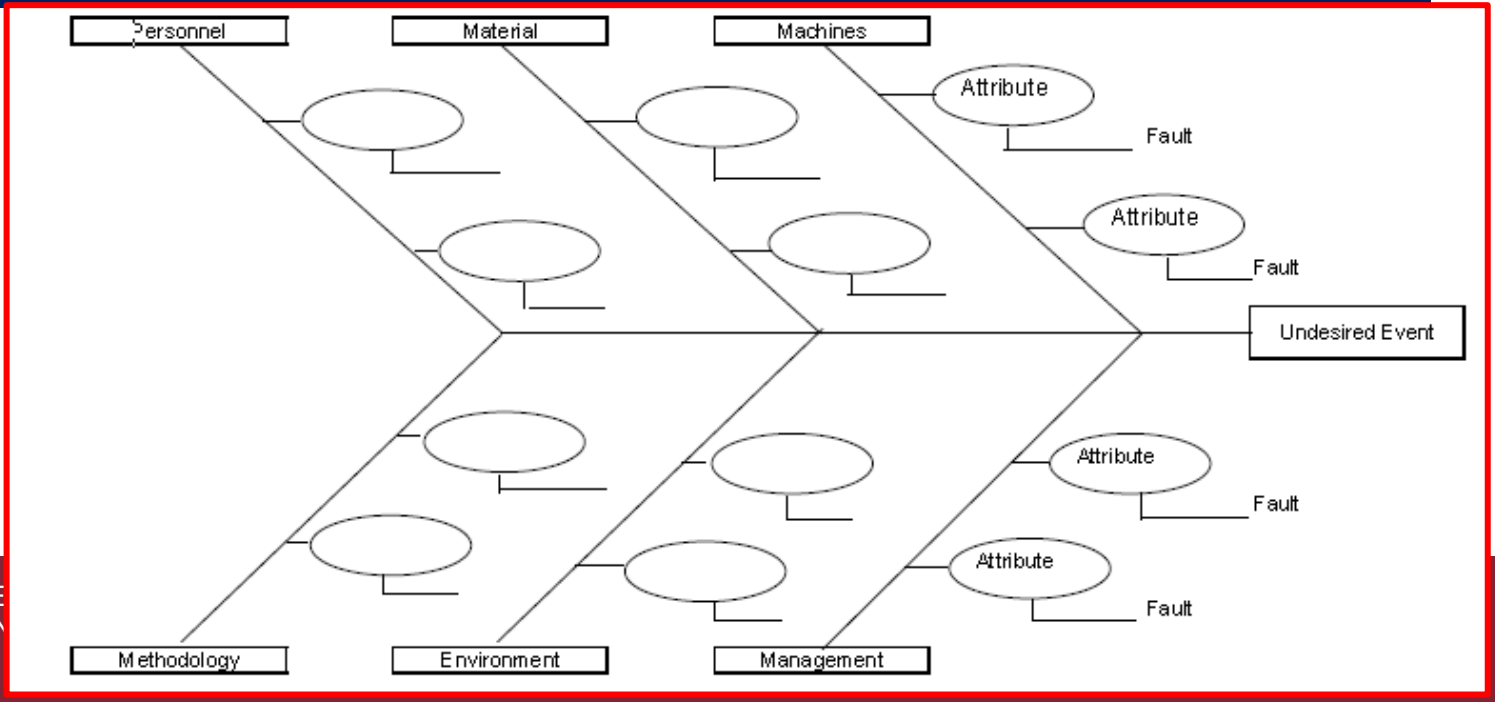
Fattore di sicurezza della Progettazione

Mean Design Spec Load

Alcuni fraintendimenti

Fault Tree vs. Ishikawa Fishbone Diagram

- Qualcuno si riferisce erroneamente all'albero dei guasti come ad un esempio di Ishikawa Fishbone Model
- Il Fishbone Diagram è un metodo di basso livello di strutturazione frutto di un brain storming per elencare le potenziali cause che possono dare luogo ad un incidente.
- L'FTA è un processo formale di individuazione graduale delle cause direttamente collegate ad un evento indesiderato.
- L'FTA mostra la progressive individuazione delle cause di guasto mediante una logica simbolica.



Esempio di Fishbone Diagram - 1

Il metodo consiste nell'individuazione ed elencazione delle categorie concettuali afferenti al problema.

ESEMPIO: Malfunzionamento del compressore di un motore aeronautico scoperto dal Ground Engineer.

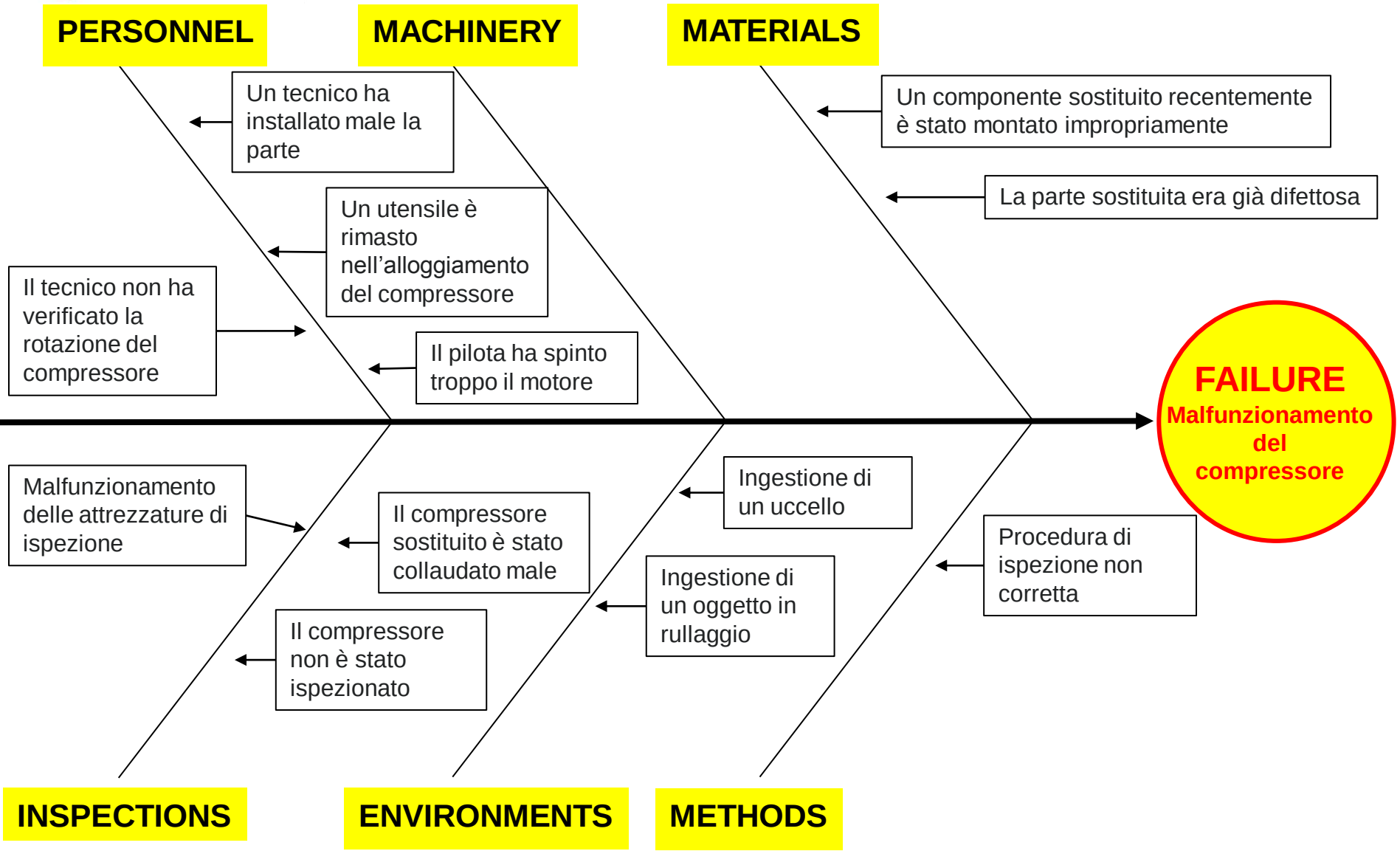
- Individuiamo dapprima le categorie principali riconducibili al problema (breakdown):
- **Personnel**: Tutti coloro che possono aver avuto un ruolo nella manutenzione dell'aereo
- **Machinery**: Le tecnologie coinvolte ed utilizzate
- **Materials**: I component coinvolti dell'aeromobile
- **Measurements**: Le ispezioni
- **Environment**: Fattori climatici, geografici e ambientali, tutti I fattori riconducibili a "*Madre Natura*"
- **Methods**: I processi di manutenzione adottati

Esempio di Fishbone Diagram - 2

Fattori al contorno:

- **Personnel**: Recentemente personale nuovo è stato inserito nelle Squadre di Manutenzione
- **Machinery**: -
- **Materials**: Alcuni componenti dei motori sono stati sostituiti nell'ultimo ciclo di manutenzione
- **Measurements**: -
- **Environment**: -
- **Methods**: -

Esempio di Fishbone Diagram - 3



Metodo Monte Carlo

- Il metodo consiste nel raccogliere una serie di output a partire da input generati in modo random o pseudo-random
- Questo metodo viene applicato molto bene quando è disponibile un modello affidabile del fenomeno in esame e si lavora all'interno dell'intervallo di stabilità e robustezza del modello stesso
- Gli output hanno presentano caratteristiche simili a quelle rilevabili da una serie di esperimenti*
  - Scattering simile dei dati
  - Più sono i "runs" del modello, più significativi ed evidenti risultano I trends.

*se gli input sono corretti – la qualità dell'output del modello dipende dalla qualità delle informazioni in input

Metodo Monte Carlo

- Il metodo Monte Carlo si presta alla progettazione di strutture e fenomeni di grande complessità e costo dove sia disponibile una buona modellistica e si lavori all'interno dell'intervallo di stabilità e robustezza del modello stesso

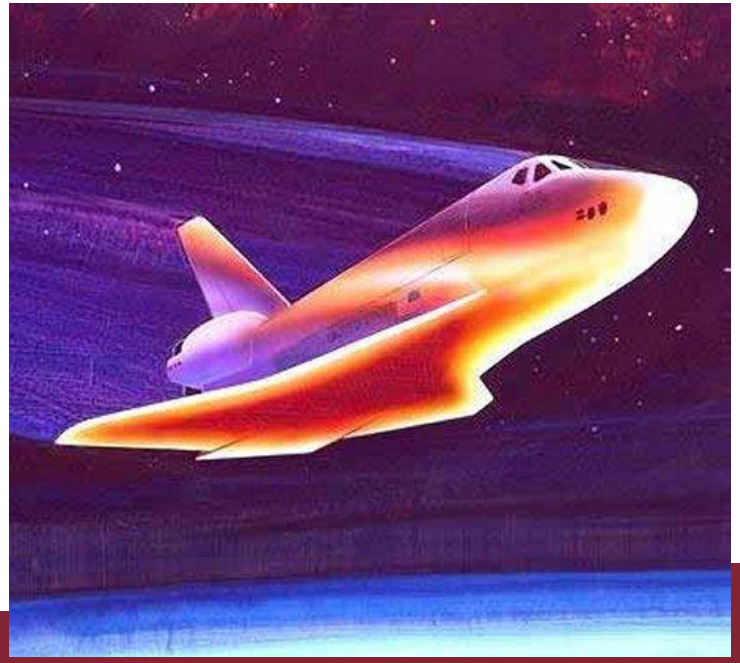
- e dove la progettazione probabilistica sia adottata come metodologia di lavoro.

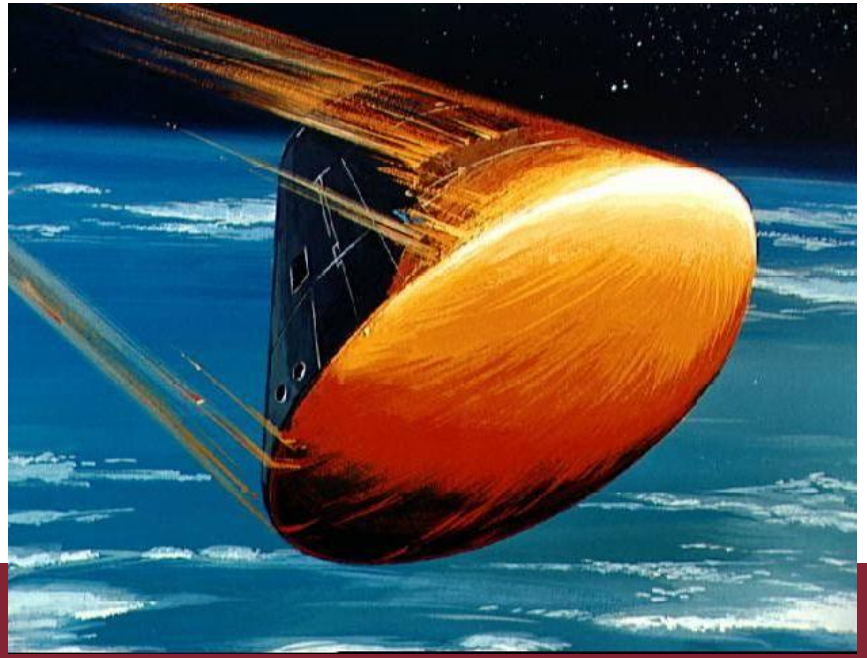
- Ciò accade quando le strutture sono soggette ad alti rischi (es. Pipeline con gas in pressione), dove la struttura non può essere facilmente sostituita (stazioni spaziali), dove l'incidente ha un forte impatto sull'opinione pubblica (Space Shuttle).

- L'elaborazione dei dati è abbastanza complessa; richiede uno specialista con sensibilità di progettazione e dei fenomeni coinvolti.

Esempio: affidabilità di uno scudo termico spaziale

- Energia Cinetica: $\frac{1}{2}mV^2$ + Energia Potenziale: $\int mgdy$ → Energia Termica (calore)
  - Velocità di rientro tra 7 km/s (LEO) e 11 km/s (rientro da un volo lunare),
  - Altitudine ~400 km (di più nel caso di rientro da un volo lunare)
- Vantaggio di una forma avviata (blunt body)
- Shuttle vs Apollo

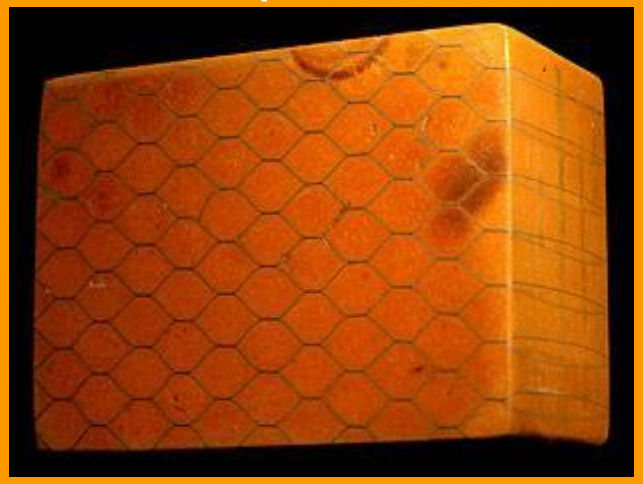




Le “mattonelle” della protezione termica

Apollo

Before



After

Shuttle

TPS Failure Modes

1. Il materiale dello scudo si brucia durante il rientro
   - Difetto strutturale (Crack)
   - Danneggiamento (Damage)
   - Scollamento (De-bonding)
   - Punto caldo (Hot spots)
   - Ablazione (Flowthrough)

2. Surriscaldamento della linea di bordo dell'incollaggio (Bondline)
   - Conducibilità troppo alta
   - Assorbimento di energia radiante
3. Cedimento dell'interfaccia
   - e.g. Interferenza elettromagnetica, interferenza con il Sistema di atterraggio

Obbiettivi della Valutazione di Rischio per lo scudo termico del veicolo Orion:

- Ottenere una stima dell'affidabilità globale del sistema
- Identificare I componenti/eventi con più alta probabilità di provocare un incidente
- Identificare I sotto-sistemi troppo conservativi
- Determinare gli aspetti relativi a progettazione, modellazione, parametri in gioco che abbiano più effetto sull'affidabilità

- Determinare dove allocare risorse per ridurre in modo più efficiente I rischi

Esempio di interazione dei rischi

Urto con Micro-Meteoriti e detriti orbitali (MMOD)

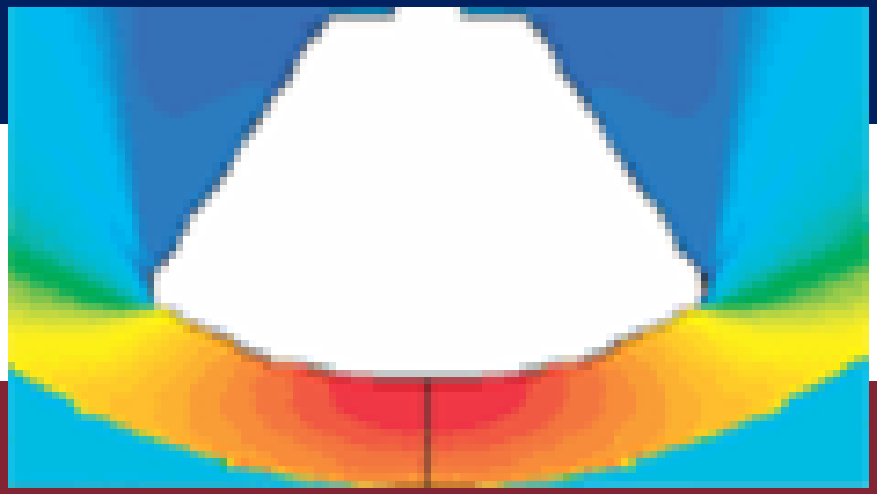
- Rischio che parti di dimensioni significativa colpiscano lo scudo termico con velocità tale da provocare un danno

- Rischio che il danno da MMOD possa causare il cedimento del TPS

Esempio: Dimensionamento del TPS

Modellazione dell'ambiente di rientro

- Alla base occorre valutare accuratamente le condizioni di rientro (energia da dissipare, temperature all'interfaccia sulla base del *Drag Coefficient* globale, della superficie di prima stima, dell'andamento della densità dell'aria in relazione alle condizioni atmosferiche e all'orientazione verso il sole nell'arco orario del rientro stesso ecc.
- Sviluppo di un modello di recessione ottenuto imponendo le condizioni di rientro selezionate in modo random come condizioni al contorno del modello termico ablative
- Selezionare il materiale e lo spessore sulla base del modello di recessione



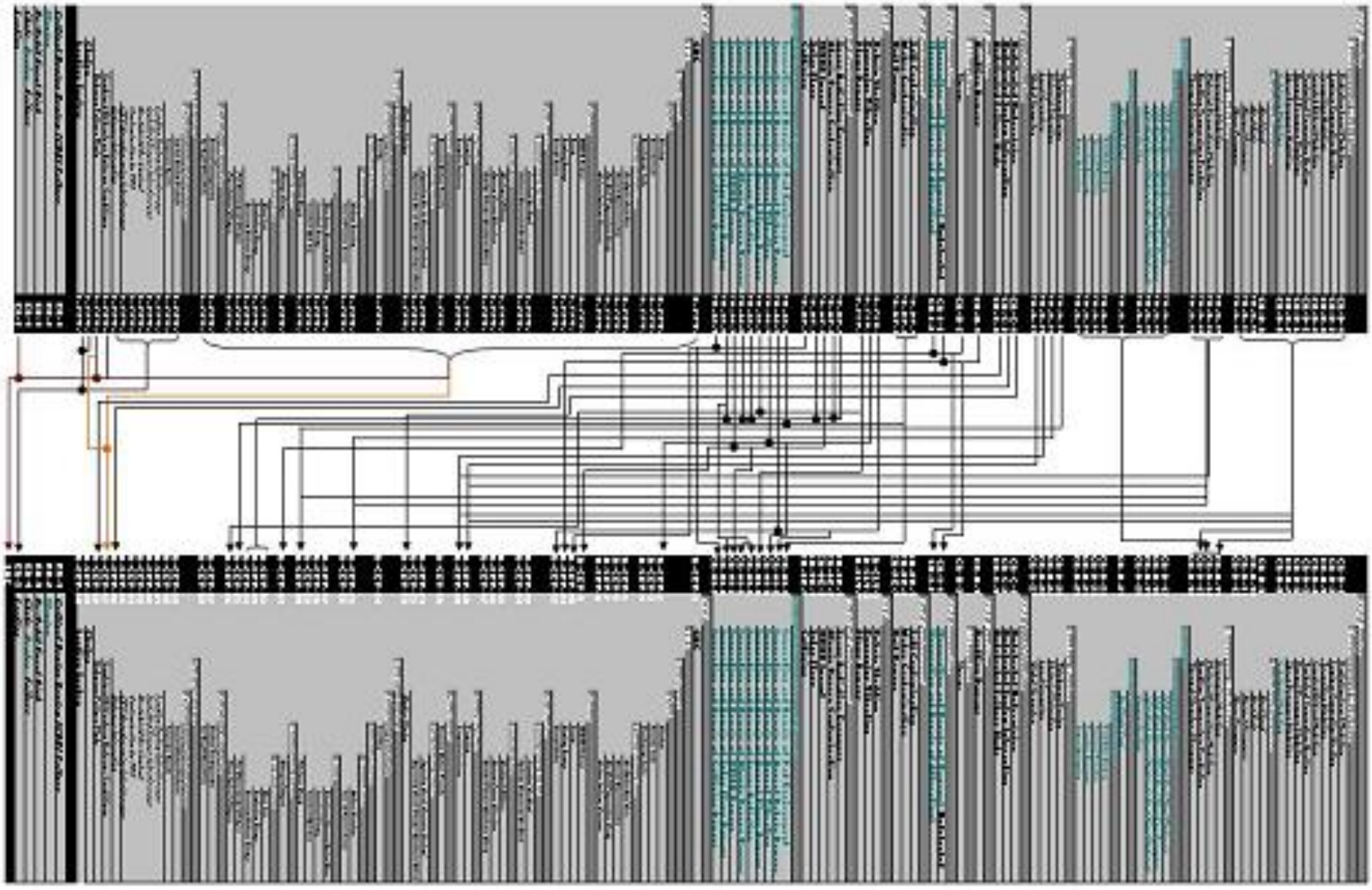
SAPIENZA
UNIVERSITÀ DI ROMA

Organizzare I Rischi con il SW SAFE

No.	Material	Dependancy	Influencing	Risk	Description	Benign Failure Description	Benign Consequence	Catastrophic Failure Description	Catastrophic Consequence
					Risks associated with active components	-	-	-	-
				TPS Design	Risks inherent to the thermal protection system	-	-	-	-
				Environment Modeling	Risks of failing to accurately predict the	-	-	-	-
CR-D-1			•	Radiation Level Modeling	Risk of failing to accurately predict radiative heading during entry	Failure to predict extreme radiation levels resulting in an insufficient design	CR-D-13 B CR-D-15 B CR-CEV-19 B	Failure to predict nominal radiation levels resulting in an insufficient design	CR-D-13 C CR-D-15 C
CR-D-2			•	Laminar Convective Heating	Risk of failing to accurately predict convective heating during entry	Failure to predict extreme laminar heating resulting in an insufficient design	CR-D-13 B CR-D-15 B CR-CEV-19 B	Failure to predict nominal laminar heating resulting in an insufficient design	CR-D-13 C CR-D-15 C
CR-D-3			•	Transition Modeling	Risk of failing to accurately predict the heating gradients in transition zones during entry	Failure to predict extreme transition heating resulting in an insufficient design	CR-D-13 B CR-D-15 B CR-CEV-19 B	Failure to predict nominal transition heating resulting in an insufficient design	CR-D-13 C CR-D-15 C
CR-D-4			•	Coupled Effect Modeling	Risk of failing to accurately predict coupled effects during entry	Failure to predict extreme coupled effects resulting in an insufficient design	CR-D-13 B CR-D-15 B CR-CEV-19 B	Failure to predict nominal coupled effects resulting in an insufficient design	CR-D-13 C CR-D-15 C
CR-D-5			•	Turbulent Convective Heating	Risk of failing to accurately predict turbulence/turbulent heating during entry	Failure to predict extreme turbulent heating resulting in an insufficient design	CR-D-13 B CR-D-15 B CR-CEV-19 B	Failure to predict nominal turbulent heating resulting in an insufficient design	CR-D-13 C CR-D-15 C
CR-D-6			•	Normal Pressure Modeling	Risk of failing to accurately predict the normal pressure loads during entry	Failure to predict extreme normal pressures resulting in an insufficient design	CR-D-13 B CR-D-15 B CR-CEV-19 B	Failure to predict nominal normal pressures resulting in an insufficient design	CR-D-13 C CR-D-15 C
CR-D-7			•	Shear Pressure Modeling	Risk of failing to accurately predict the shear pressure loads on the vehicle	Failure to predict extreme shear pressures resulting in an insufficient design	CR-D-13 B CR-D-15 B CR-CEV-19 B	Failure to predict nominal shear pressures resulting in an insufficient design	CR-D-13 C CR-D-15 C
CR-D-8			•	Catalysis Modeling*	Risk of failing to accurately predict heating due to chemical reactions on the TPS surface	Failure to predict extreme catalytic heating resulting in an insufficient design	CR-D-13 B CR-D-15 B CR-CEV-19 B	Failure to predict nominal catalytic heating resulting in an insufficient design	CR-D-13 C CR-D-15 C
				Trajectory Dispersions	Risks of failing to anticipate changes in the	-	-	-	-
CR-D-9			•	*Heat Load*	Risk of trajectory dispersions causing unanticipated heat loads during entry	Unanticipated heat loads caused by extreme trajectory dispersions resulting in insufficient design	CR-D-13 B CR-D-15 B CR-CEV-19 B	Unanticipated heat loads caused by nominal trajectory dispersions resulting in insufficient design	CR-D-13 C CR-D-15 C
CR-D-10			•	*Heat Rate*	Risk of trajectory dispersions causing unanticipated heat rates during entry	Unanticipated heat rates caused by extreme trajectory dispersions resulting in insufficient design	CR-D-13 B CR-D-15 B CR-CEV-19 B	Unanticipated heat rates caused by nominal trajectory dispersions resulting in insufficient design	CR-D-13 C CR-D-15 C
CR-D-11			•	*Normal Pressure*	Risk of trajectory dispersions causing unanticipated normal pressures during entry	Unanticipated normal pressure caused by extreme trajectory dispersions resulting in insufficient design	CR-D-13 B CR-D-15 B CR-CEV-19 B	Unanticipated normal pressure caused by nominal trajectory dispersions resulting in insufficient design	CR-D-13 C CR-D-15 C
CR-D-12			•	*Shear Pressure*	Risk of trajectory dispersions causing unanticipated shear pressures during entry	Unanticipated shear pressure caused by extreme trajectory dispersions resulting in insufficient design	CR-D-13 B CR-D-15 B CR-CEV-19 B	Unanticipated shear pressure caused by nominal trajectory dispersions resulting in insufficient design	CR-D-13 C CR-D-15 C
				Response Modeling	Risks of failing to accurately predict material	-	-	-	-
CR-D-13		X	•	Recession Modeling	Risk of failing to accurately predict material recession rates during entry	Failure to predict recession rates in extreme conditions	CR-CEV- B CR-CEV-18 B CR-CEV-19 B	Failure to predict recession rates in nominal conditions	CR-CEV- C CR-CEV- C CR-CEV- C
CR-D-14		X	•	Material Properties Modeling	Risk of failing to accurately predict material properties during entry	Failure to predict material properties in extreme conditions	CR-CEV- B CR-CEV-18 B CR-CEV-19 B	Failure to predict material properties in nominal conditions	CR-CEV- C CR-CEV- C CR-CEV- C
CR-D-15		X	•	Bondline Temperature Prediction	Risk of failing to accurately predict the temperature at the bondlines during entry	Failure to predict bondline temperature in extreme conditions	CR-CEV- B CR-CEV-18 B CR-CEV-19 B	Failure to predict bondline temperature in nominal conditions	CR-CEV- C CR-CEV- C CR-CEV- C
CR-D-16		X	•	Thermal-Structural Response	Risk of failing to accurately predict the thermal and structural response during entry	Failure to thermal-structural response in extreme conditions	CR-CEV- B CR-CEV-18 B CR-CEV-19 B	Failure to thermal-structural response in nominal conditions	CR-CEV- C CR-CEV- C CR-CEV- C
				Testing	Risks of failing to properly test TPS materials in entry conditions	-	-	-	-
				Arc Jet Response Testing	Risks of failing to properly ground test TPS materials in entry conditions	-	-	-	-
CR-D-17			•	*LDR-High Shear/High Heat Flux/Moderate Pressure*	Risk of failing to ground test materials in high shear/high heat/moderate pressure	Failure to collect enough arc jet test data to understand material behavior in environment described	CR-CEV- B CR-D-13 B CR-D-14 B CR-D-15 B CR-D-16 B	Failure to collect any arc jet test data to understand material behavior in environment described	CR-CEV- C CR-D-13 C CR-D-14 C CR-D-15 C CR-D-16 C
CR-D-18			•	*LDR-High Shear/High Heat Flux/Low Pressure*	Risk of failing to ground test materials in high shear/high heat/low pressure	Failure to collect enough arc jet test data to understand material behavior in environment described	CR-CEV- B CR-D-13 B CR-D-14 B CR-D-15 B CR-D-16 B	Failure to collect any arc jet test data to understand material behavior in environment described	CR-CEV- C CR-D-13 C CR-D-14 C CR-D-15 C CR-D-16 C
CR-D-19			•	*LEC-High Shear/Moderate Heat Flux/Moderate Pressure*	Risk of failing to ground test materials in high shear/moderate heat/moderate pressure	Failure to collect enough arc jet test data to understand material behavior in environment described	CR-CEV- B CR-D-13 B CR-D-14 B CR-D-15 B CR-D-16 B	Failure to collect any arc jet test data to understand material behavior in environment described	CR-CEV- C CR-D-13 C CR-D-14 C CR-D-15 C CR-D-16 C
CR-D-20			•	*Coupon Scaling*	Risk of failing to ground test materials to scale	Failure to collect enough arc jet test data with large scale coupons	CR-CEV- B CR-D-13 B CR-D-14 B CR-D-15 B CR-D-16 B	Failure to collect any arc jet test data with large scale coupons	CR-CEV- C CR-D-13 C CR-D-14 C CR-D-15 C CR-D-16 C
				Flight Test	Risks of failing to properly flight test TPS materials in entry conditions	-	-	-	-
CR-D-21			•	*No Flight Test*	Risk of not flight testing the TPS	-	-	Failure to conduct a flight test	CR-CEV- B,C CR-D-13 B,C CR-D-14 B,C CR-D-15 B,C CR-D-16 B,C
				Flight Test Failure	Risks of performing a flight test an having a failure	-	-	-	-
CR-D-22			•	Test Vehicle Burn up	Risk of performing a flight test and getting misleading data due to TPS scaling factors	Collecting partially misleading flight data or good data that contains gaps resulting in poor response	CR-CEV- B CR-D-13 B CR-D-14 B CR-D-15 B CR-D-16 B	Collecting fully misleading flight data resulting in insufficient response modeling	CR-CEV- C CR-D-13 C CR-D-14 C CR-D-15 C CR-D-16 C
CR-D-23			•	Incorrect Trajectory	Risk of performing a flight test and getting misleading data due to an incorrect trajectory	Collecting partially misleading flight data or good data that contains gaps resulting in poor response	CR-CEV- B CR-D-13 B CR-D-14 B CR-D-15 B CR-D-16 B	Collecting fully misleading flight data resulting in insufficient response modeling	CR-CEV- C CR-D-13 C CR-D-14 C CR-D-15 C CR-D-16 C
CR-D-24			•	Trajectory Dispersions	Risk of performing a flight test and getting misleading data due to trajectory dispersions	Collecting partially misleading flight data or good data that contains gaps resulting in poor response	CR-CEV- B CR-D-13 B CR-D-14 B CR-D-15 B CR-D-16 B	Collecting fully misleading flight data resulting in insufficient response modeling	CR-CEV- C CR-D-13 C CR-D-14 C CR-D-15 C CR-D-16 C
CR-D-25			•	Sensor Malfunction	Risk of performing a flight test and getting misleading data due to sensor/instrumentation	Collecting partially misleading flight data or good data that contains gaps resulting in poor response	CR-CEV- B CR-D-13 B CR-D-14 B CR-D-15 B CR-D-16 B	Collecting fully misleading flight data resulting in insufficient response modeling	CR-CEV- C CR-D-13 C CR-D-14 C CR-D-15 C CR-D-16 C

SAPIENZA
UNIVERSITÀ DI ROMA

Visualizzare le interazioni tra i rischi

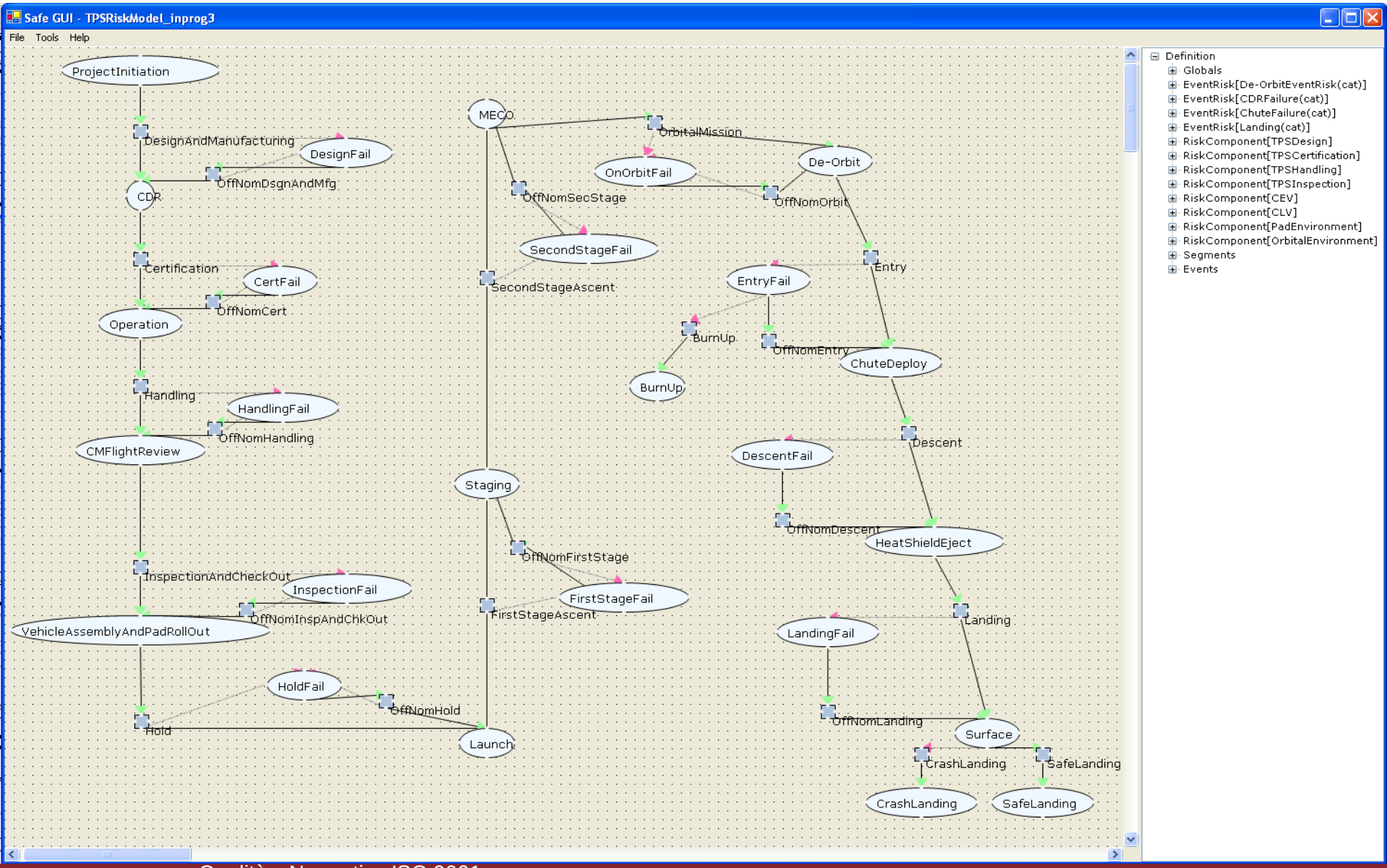


SAPIENZA
UNIVERSITÀ DI ROMA

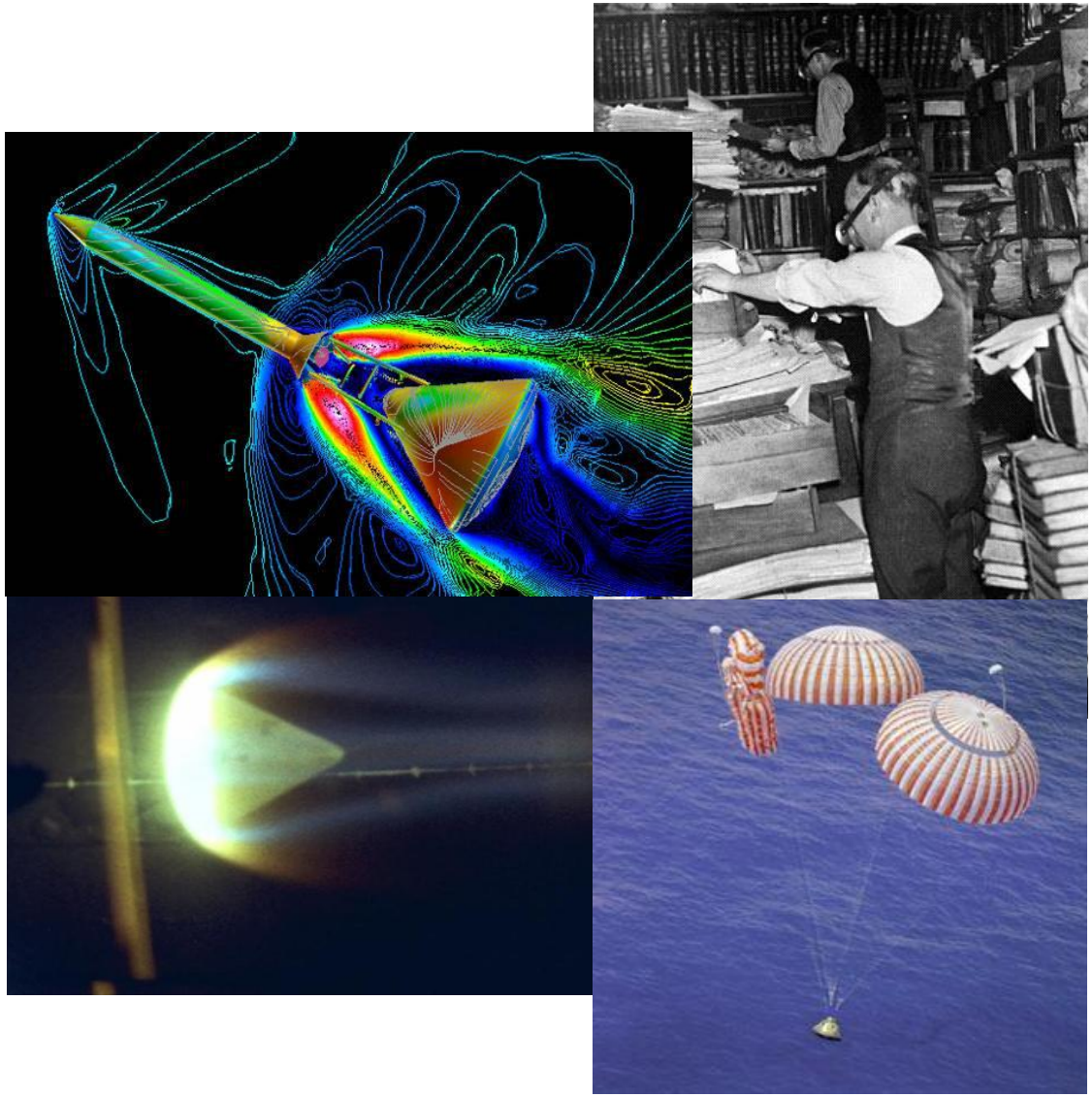
Calcolare i valori di rischio

ID	Material dependant	Influencing	Risk	Active Segment(s)/ Event(s), [Time Active]	Benign Probability (1,2,3)	Benign Consequence (1,2,3,4)	Benign Risk (L,M,H)	Cat Probability (1,2,3)	Cat Consequence (1,2,3,4)	Cat Risk (L,M,H)	Prediction Confidence Level (N,L,M,H)	Material Sensitivity (N,L,M,H)				
												AVCOAT	ACC	PhenC-t	PICA	3DQP
			CEV	-	-	-	-	-	-	-	-	-	-	-	-	-
CR-CEV-1		•	GNC	Entry [80-30]	?	?	?	?	?	?	?	?	?	?	?	?
			TPS	Entry [80-30]	-	-	-	-	-	-	-	-	-	-	-	-
			Burnthrough	Entry [80-30]	-	-	-	-	-	-	-	-	-	-	-	-
			Crack	Entry [80-30]	-	-	-	-	-	-	-	-	-	-	-	-
CR-CEV-2	x	X	•	Vibration	Entry [80-30]	?	?	?	?	?	?	?	?	?	?	?
CR-CEV-3	x		•	Acoustic Loads	Entry [80-30]	?	?	?	?	?	?	?	?	?	?	?
CR-CEV-4	x		•	Aerodynamic Loads	Entry [80-30]	?	?	?	?	?	?	?	?	?	?	?
				Thermal-Mechanical Stress	Entry [80-30]	-	-	-	-	-	-	-	-	-	-	-
CR-CEV-5	x		•	*Re-Entry Heat Pulse*	Entry [80-30]	?	?	?	?	?	?	?	?	?	?	?
CR-CEV-6	x	X	•	*Ascent Depressurization*	Entry [80-30]	?	?	?	?	?	?	?	?	?	?	?
CR-CEV-7	x		•	*On-Orbit Temperature Cycling*	Entry [80-30]	?	?	?	?	?	?	?	?	?	?	?
CR-CEV-8	x		•	*Material Internal Pressure*	Entry [80-30]	?	?	?	?	?	?	?	?	?	?	?
			Damage	Entry [80-30]	-	-	-	-	-	-	-	-	-	-	-	-
CR-CEV-9	x	X	•	MMOD Damage	Entry [80-30]	?	?	?	?	?	?	?	?	?	?	?
CR-CEV-10	x	X	•	Collision	Entry [80-30]	?	?	?	?	?	?	?	?	?	?	?
CR-CEV-11	x	X	•	Handling Damage	Entry [80-30]	?	?	?	?	?	?	?	?	?	?	?
CR-CEV-12	x	X	•	Ascent Debris	Entry [80-30]	?	?	?	?	?	?	?	?	?	?	?
			De-Bonding	Entry [80-30]	-	-	-	-	-	-	-	-	-	-	-	-
				Ablator Internal De-Bond	Entry [80-30]	-	-	-	-	-	-	-	-	-	-	-
CR-CEV-13	x		•	*Facesheet De-Bond*	Entry [80-30]	?	?	?	?	?	?	?	?	?	?	?	?
CR-CEV-14	x		•	*Internal Honeycomb De-Bond*	Entry [80-30]	?	?	?	?	?	?	M	M	N	M	N	N
				Attachment Failure	Entry [80-30]	-	-	-	-	-	-	-	-	-	-	-	-
CR-CEV-15			•	*Insufficient Adhesive*	Entry [80-30]	?	?	?	?	?	?	?	?	?	?	?	?
CR-CEV-16		?	•	*Uneven Carrier Structure*	Entry [80-30]	?	?	?	?	?	?	?	?	?	?	?	?
CR-CEV-17			•	*Bondline Thermal-Mechanical Strain*	Entry [80-30]	?	?	?	?	?	?	?	?	?	?	?	?
				Local Hot Spots	Entry [80-30]	-	-	-	-	-	-	-	-	-	-	-	-
CR-CEV-18		X	•	Transition	Entry [80-30]	?	?	?	?	?	?	?	?	?	?	?	?
CR-CEV-19		X	•	Geometric Features	Entry [80-30]	?	?	?	?	?	?	?	?	?	?	?	?

Il Modello di interazione



Calcolare l'Affidabilità



Esempio - Risultati

Modello di Affidabilità

- Incorpora oltre 90 potenziali rischi di cedimento della TPS
  - Ogni rischio può esitare sia positivamente che negativamente
- Molteplici cedimenti non distruttivi possono condurre ad un evento catastrofico
- Tutti I fattori relative alla fase di incipiente rientro possono influire sui rischi durante il rientro e nella fase di atterraggio

Documenti di Risk Analysis

- Descrizione dettagliata delle interazioni tra I sotto-sistemi
- Può essere utilizzata per analizzare le modifiche e capire come impostare il modello
- Può essere utilizzata per capire le relazioni tra la scelta dei materiali, i rischi sottesi e le altre variabili di progettazione

Summary - 1

- **La Risk Analysis è un argomento vasto** e di fatto copre un'intera branca dell'Ingegneria. Il nuovo orientamento della ISO 9001:2015 ne amplia ancora di più le applicazioni.

- **La Risk Analysis è un processo iterativo**
  - Se usata correttamente, può contribuire significativamente a salvare vite….e denaro!
  - È di aiuto nelle decisioni in genere e quelle progettuali in particolare; contribuisce a documentare le azioni intraprese, giustificandone i motivi. In questo senso costituisce una potente spinta alla **capitalizzazione del Know How**

- Ci sono moltissimi tool di aiuto disponibili per gli Ingegneri

Summary - 2

- L'output del Risk Assessment è buono se è buono l'input
  - Gli ingegneri devono avere moltissimi dati sperimentali a disposizione e modelli validati prima che un Modello di Rischio venga sviluppato.
- L'output del Modello di Rischio non ha significato senza averne stabilito I limiti di validità della soluzione

END OF PART 4