Sviluppare prodotti Safety Compliant

Nicola Bergamin
Bluewind Srl

Bluewind e Safety

About Bluewind

Bluewind, an independent engineering company, provides engineering and software solutions in the domains of electron , **Safety Critical** applications, **Cybersecurity** and **Artificial Intelligence**

Bluewind and Safety

Supporto allo sviluppo sistemi Safety Critical

Alcuni dati: 20 progetti /anno

- 40 % PMI
- 30% grande Industria
- 30% other

60% Industrial

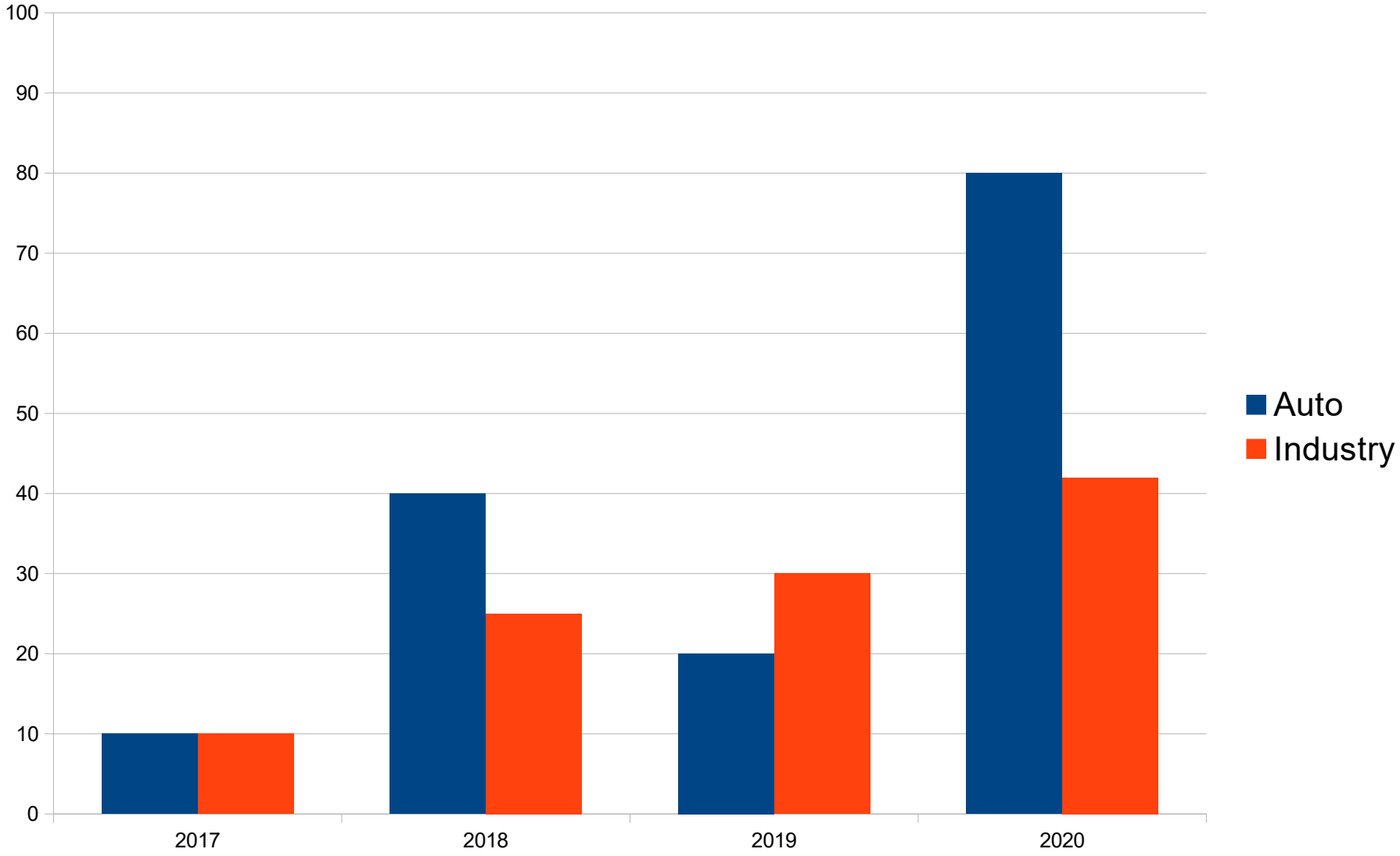
Commercial Construction Agriculture
Medical,
Drives,
Machinery

40% Automotive

BMS
Powertrain
Hybrid
Full electric
Steering

Safety: perchè adesso ?

R&D Sviluppo Safety/ Non Safety)
2017-2020



La richiesta di Safety: perché?

Attenzione maggiore alla Sicurezza dei prodotti e sistemi, richiesta di qualità e **tutela** più alta

Aumento della **complessità**: il software è ineludibile, e le implicazioni vanno considerate

Convergenza di tecnologie: AI, Cybersecurity sono già realtà, e sono essenziali alla Safety

Convergenza di settori: Industriale e Automotive stanno convergendo

Trasformazioni di settori: Meccanico –> Meccatronico –> Elettronico

Passo indietro……

Exemplary Tales

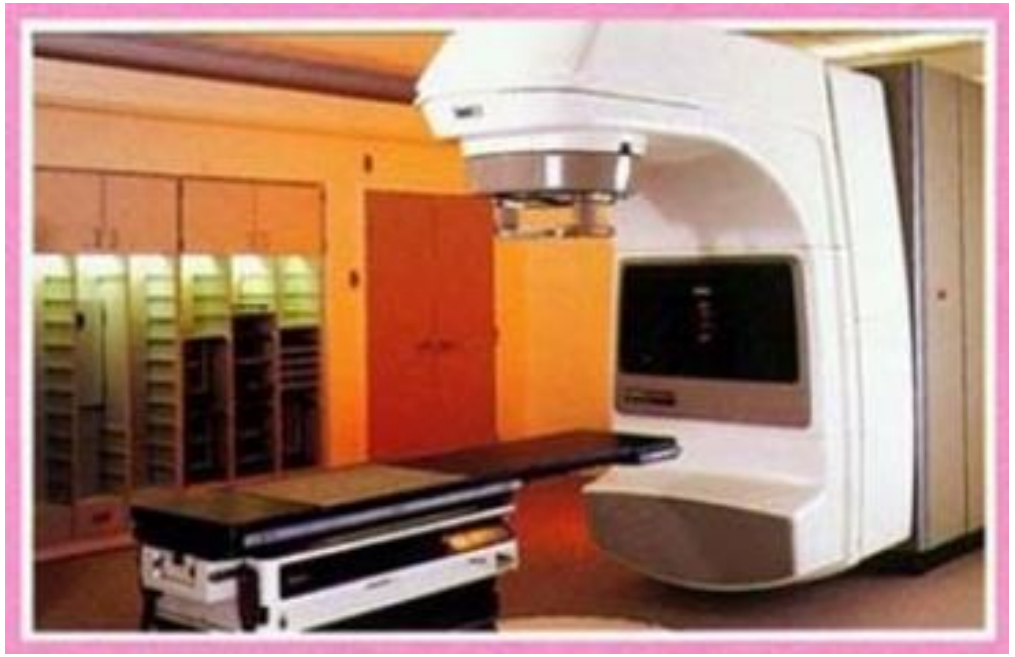
Therac-25 X-Ray failure (1985)

Atomic Energy of Canada Limited

One of the most well-documented failures in a safety-critical computer System

© By Philip Koopman, November 16, 2015 - “Critical Systems and Software Safety”

Images: https://hci.cs.siue.edu



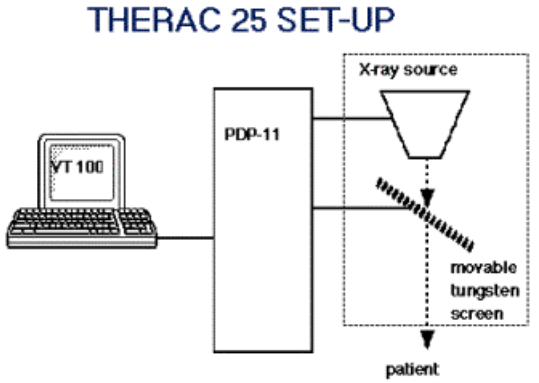
THERAC-25 X-RAY
Kennestone, 1985: apparently 15,000 - 20,000 rads instead of 200 rads

• (500 rads is fatal if delivered to the whole body, but this was focused)

These problems are not limited to the medical industry – they are generic problems in safety engineering and software engineering

Relying on software but:

- Not documented Software Specs
- No software test Plan
- Inadequate safety engineering
- Software not documented
- Simple programming errors
- Software excluded from Safety calculations...

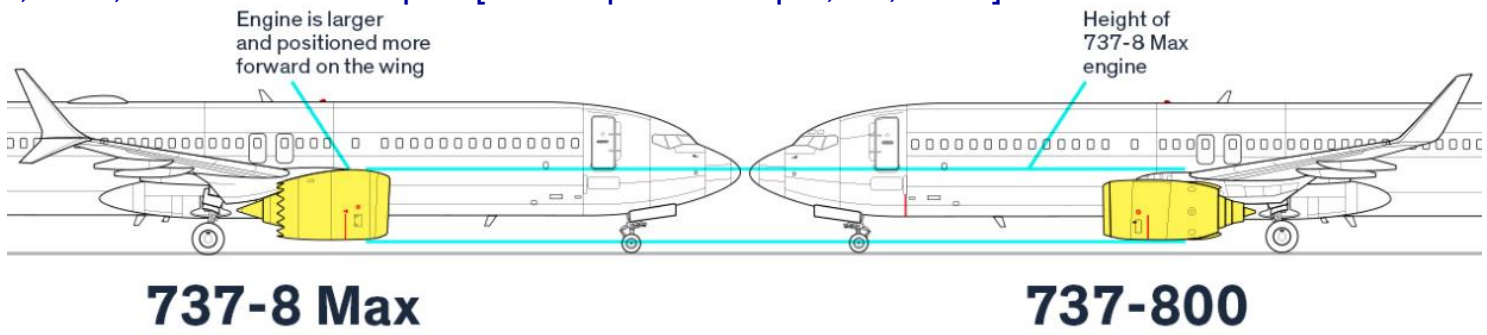


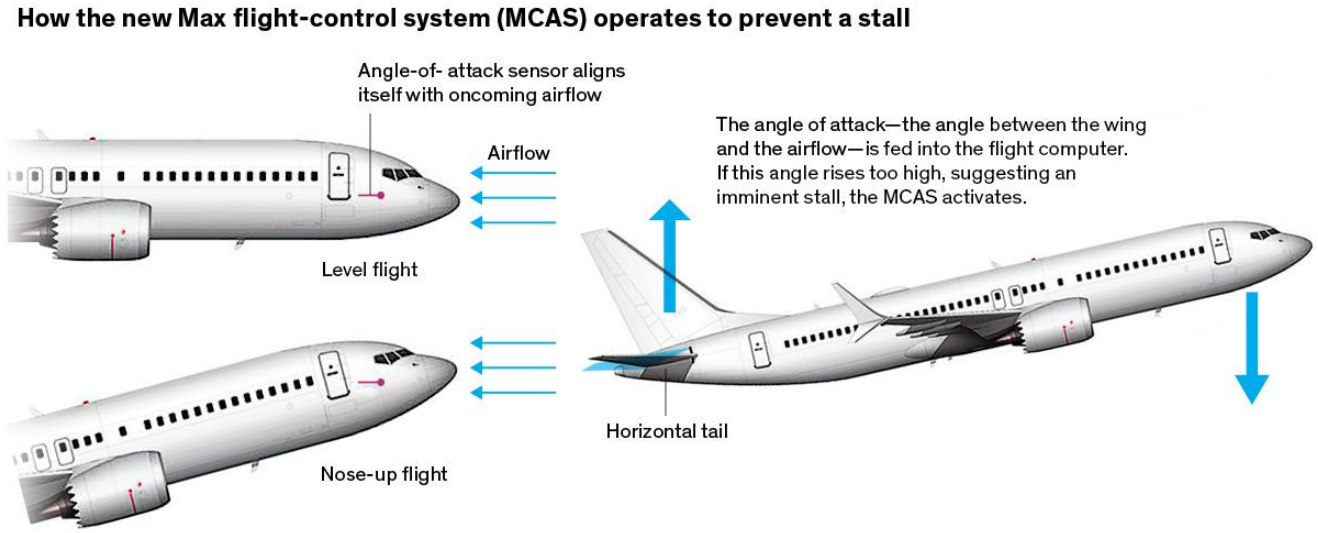
737 MAX (2018-2019), Boeing

How the Boeing 737 Max Disaster Looks to a Software Developer

Design shortcuts meant to make a new plane seem like an old, familiar one are to blame

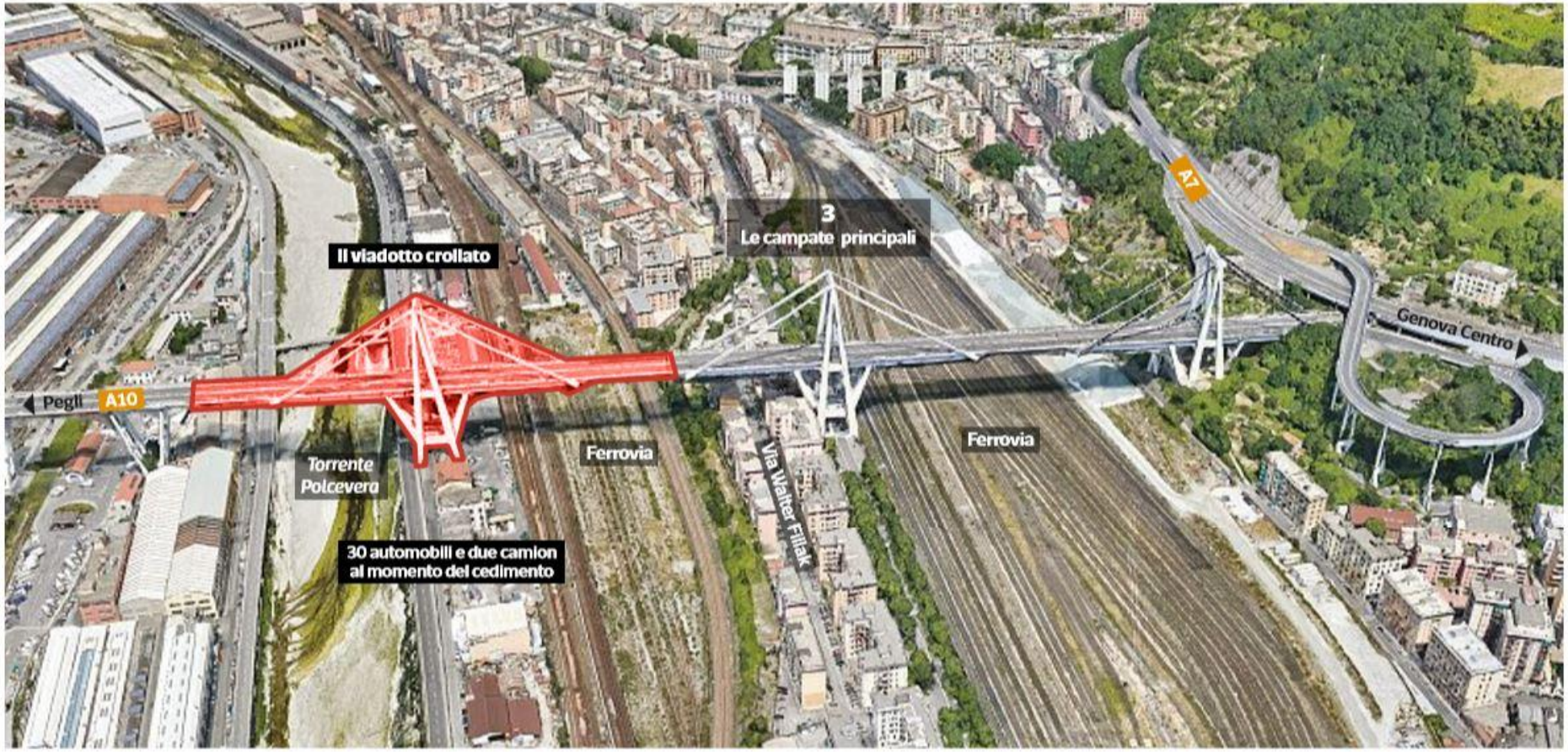
© By Gregory Travis, Pilot, Software developer. [IEEE Spectrum April, 18, 2019]





Ponte Morandi

(Lifecycle...)



Come funziona Safety

Functional Safety

Rischio tollerabile

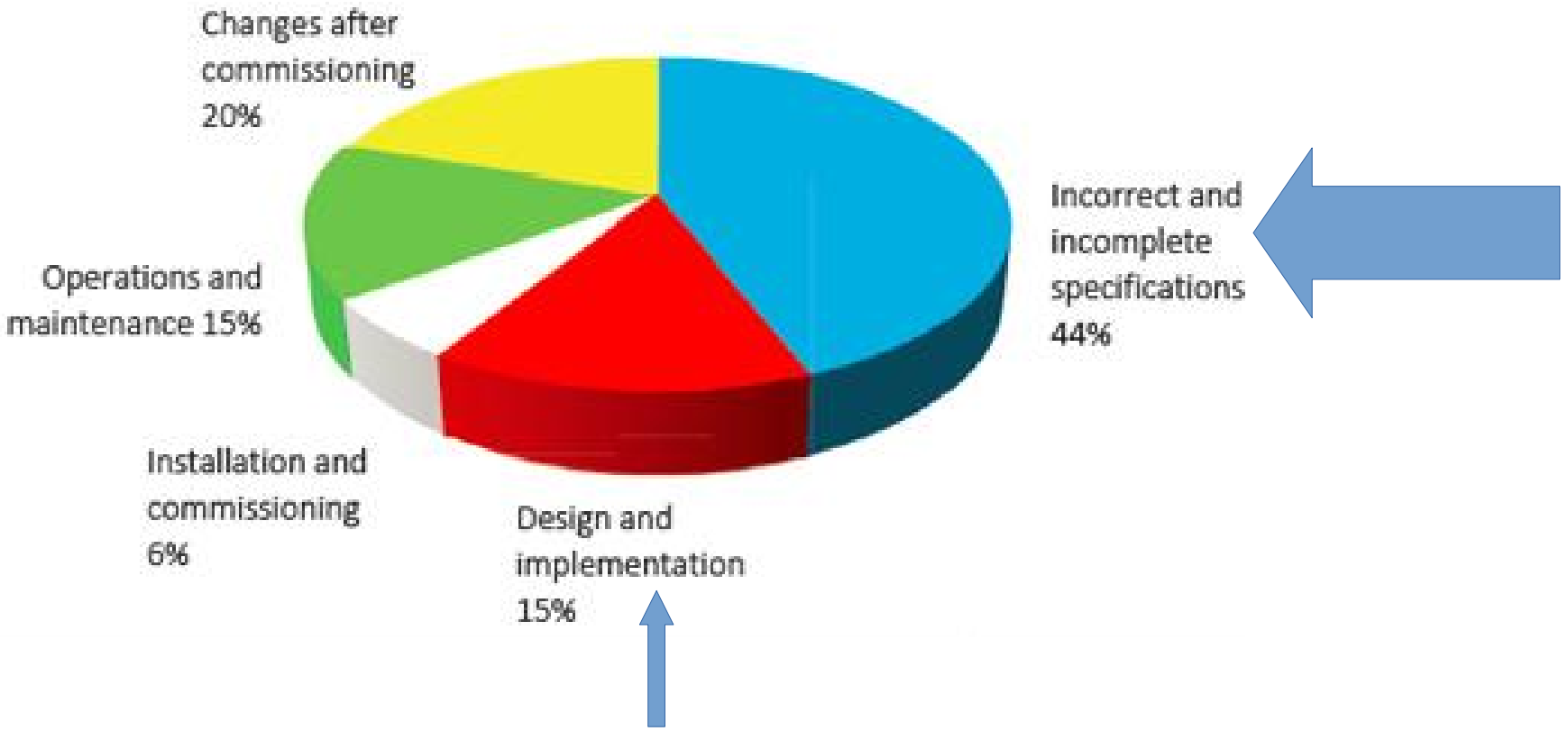
Safety Compliance

Adozione di procedure nella progettazione atte alla riduzione del rischio dovuto a malfunzionamenti, ad un livello di rischio definito **tollerabile**.

Rischio = Probabilità x Conseguenza

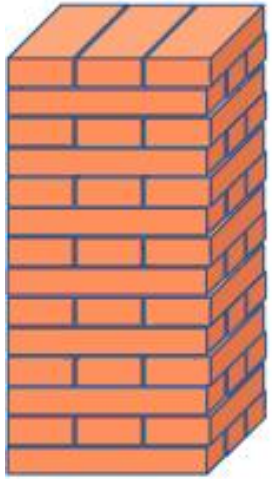
Layering concepts (ISA.org)

Causes of accidents involving control and safety systems.

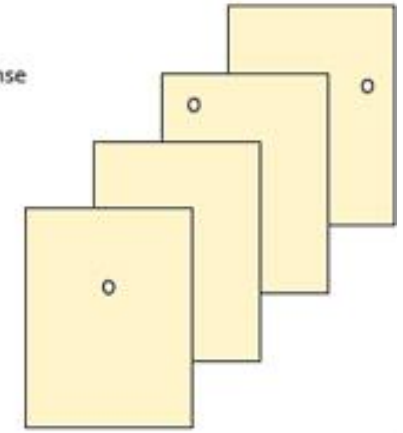


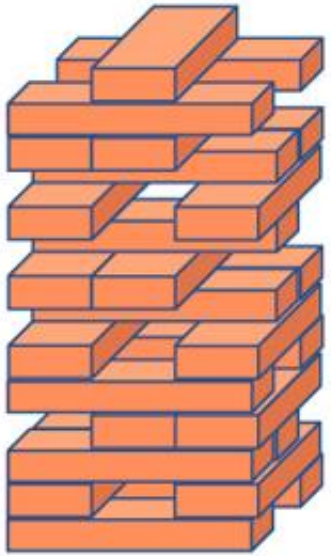
Layering concepts (ISA.org)

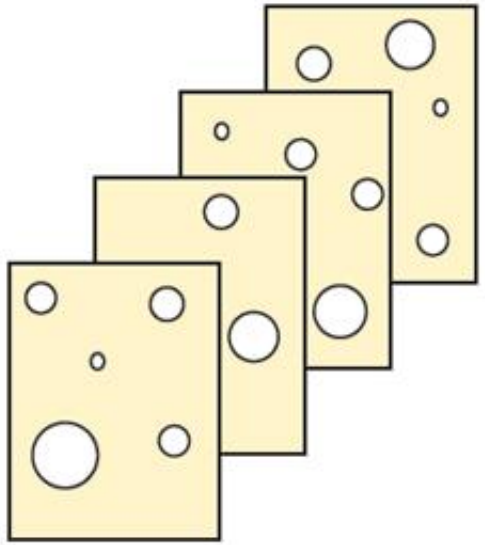
Protection and Mitigation layers



1. Trade secrets
2. Compliance audits
3. Emergency planning and response
4. Incident investigation
5. Management of change
6. Hot work permit
7. Mechanical integrity
8. Pre-startup safety review
9. Contractors
10. Training
11. Operating procedures
12. Process hazards analysis
13. Process safety information
14. Employee participation





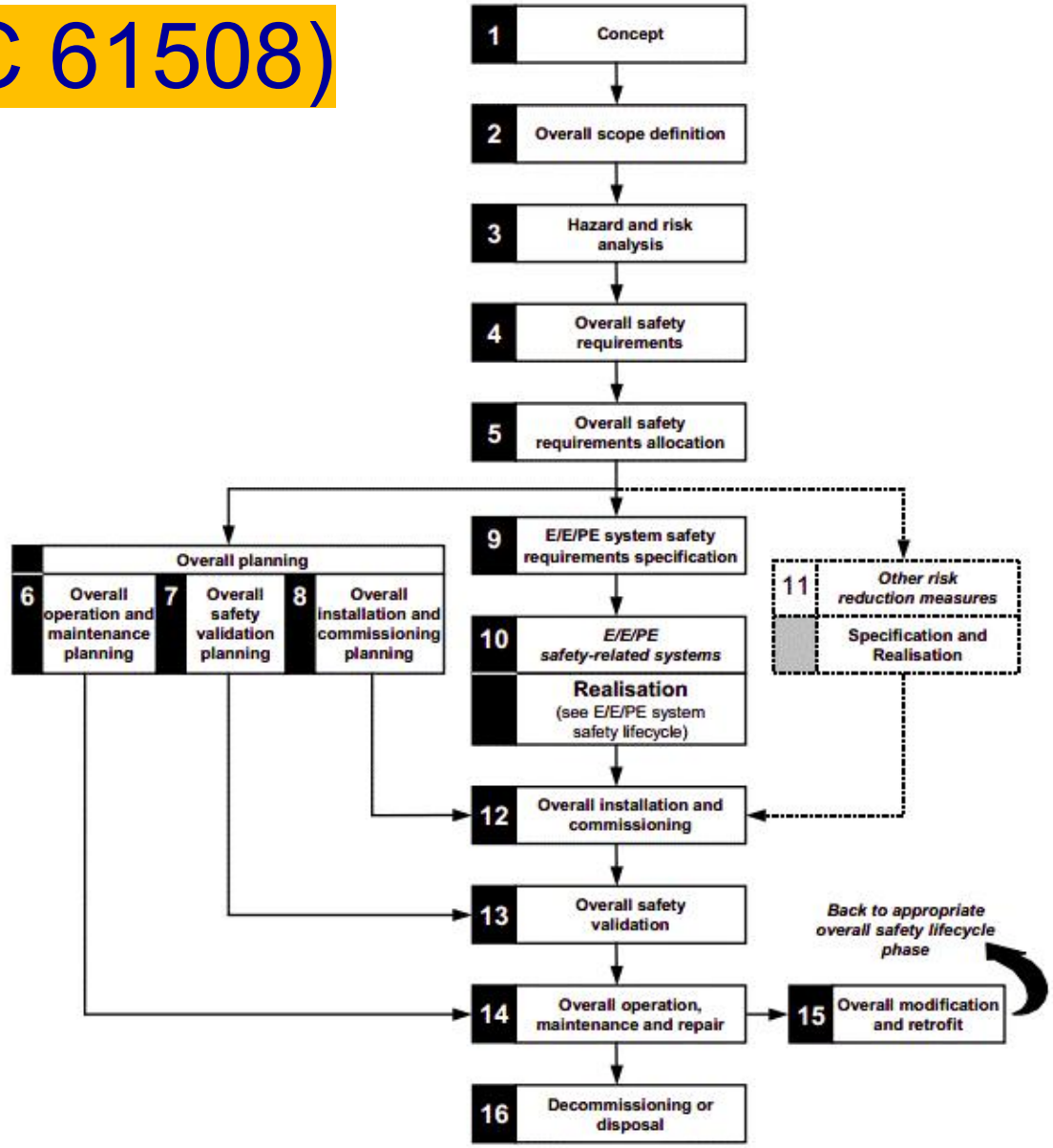


Description	Probability of failure
Stainless-steel construction	.01
Nitrogen purge	.1
Refrigeration system	.1
High-temperature alarm	.1
Empty reserve tank	.1
Diluting agent	.1
Vent gas scrubber and flare	.1
Rupture disk and relief valve	.1
All safety layers failing at the same time	**1E-9**

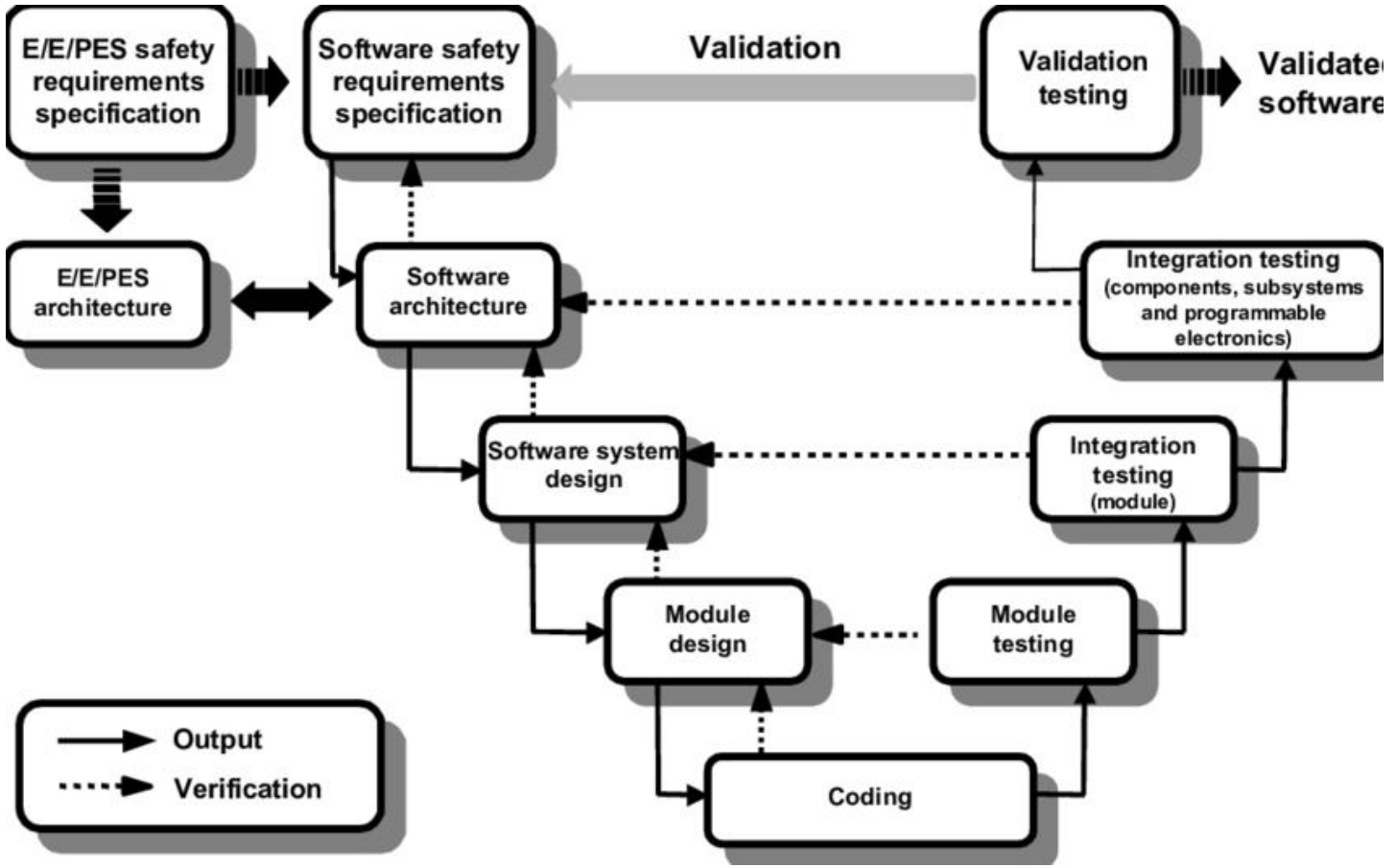
IEC EN 61508

is a core functional safety standard, applied widely to all types of safety critical E/E/PS and to systems with a safety function incorporating E/E/PS. (Safety Integrity Level – SIL)

Safety Lifecycle (IEC 61508)



Zoom sul ciclo di sviluppo (Software)



Functional Safety

Cosa è in pratica

Definire Safety Goals –> Safety **Functions**

Definire **SIL**

Attuare **Lifecycle** Design

ISA – **Independent** Safety Assessment

Functional safety

Ciclo di Sviluppo

- Architettura
- Approccio a ente certificatore (ISA - Independent safety Assessment)
- Safety Goals → Requisiti Safety Software, Hardware
- Sviluppo
- Testing
- Documentazione
- Assessment interno
- [Assessment ISA]

Come iniziare un processo Safety

Functional Safety

Valutare la introduzione di un processo Safety

Adeguamento ad una norma di settore o di legge (i.e. medicale)

Tutela aziendale (best practice)

Competitività e qualità del prodotto

Richiesta dal mercato (competitività commerciale)

Entrata in nuovo mercato, o cambio di modello

Da dove inizio?

Processo di sviluppo unitario: gli ingredienti

Formazione generale

Trovare le competenze: il Safety Expert

Formazione tecnica

Assessment Iniziale di progetto

Investimenti nella Safety

In generale, il costo puo essere x1.5 - x 2.5 - x3.0
(a seconda del livello SIL1..SIL4)

Per Industriale (IEC-61508), si riscontra la maggior differenza tra SIL2 e SIL3

Gli investimenti si spiegano con :

Tools,
R&D,
controllo formale del processo,
testing,
certificazione

Safety Process vs Standard (QM)

Perche Safety è piu complesso e costoso?

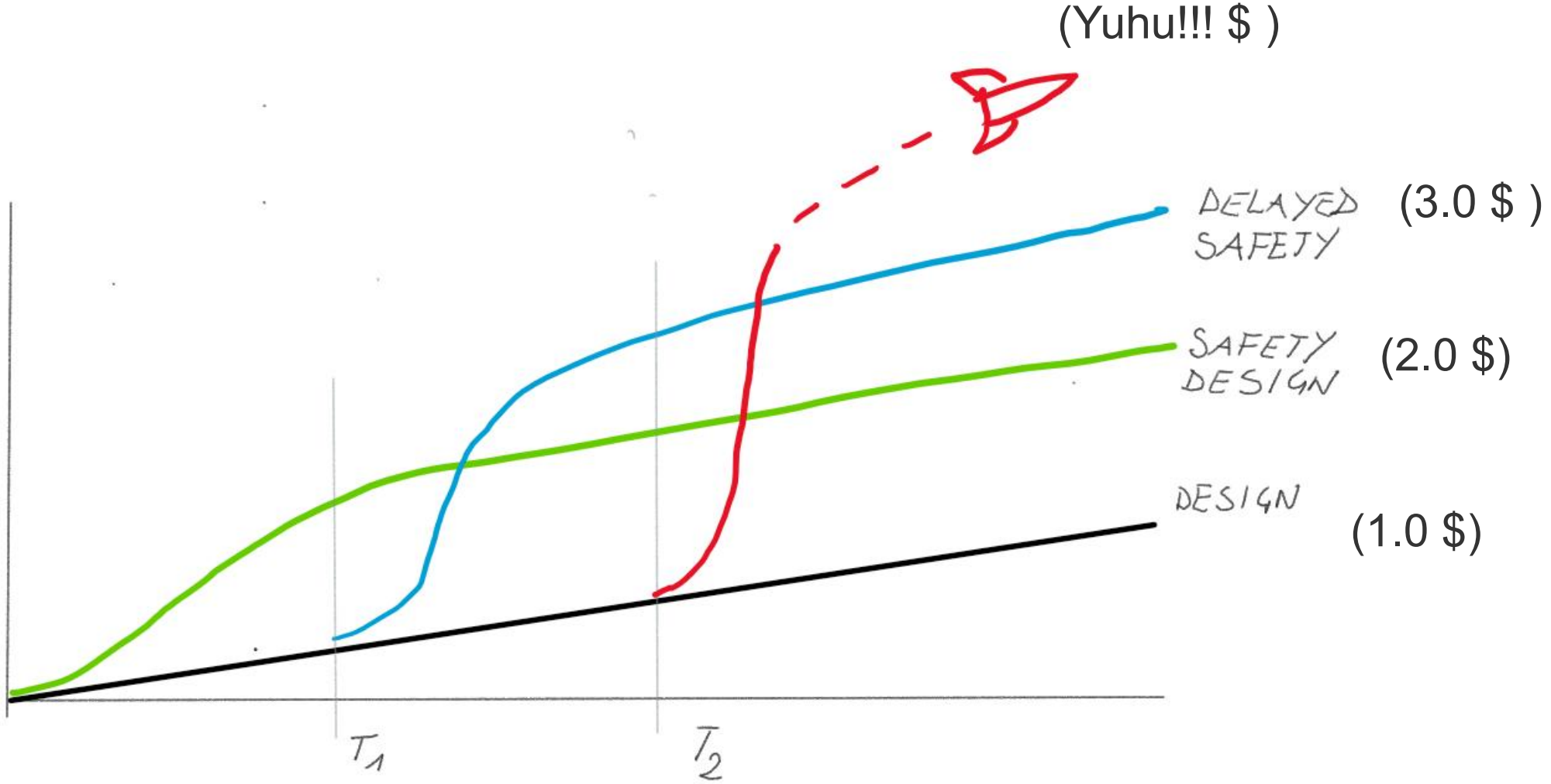
- processo di qualità stringente, in cui hardware, software e documentazione sono normati

- testing dei sottosistemi va documentato

- vanno simulate e testate anche le situazioni di guasto

Safety Design patterns

How delay impacts over performance and cost



Impatti positivi

Crescita di prodotto e aziendale

Il criterio di testing e documentazione determina crescita della qualità del sistema, indipendentemente dalla safety

Crescita astronomica della qualità e mentalità in R&D e in azienda, per tutti i i tipi di progetto

Impatti positivi

Competenze emergenti

Le competenze che emergono (interne o esterne)

Safety Manager (specific professional)
Software Safety expert (developers)
Hardware Safety expert (developers)
Testing Team (developers,..)

La Safety è additiva?

= si puo applicare ad un progetto già in corso?

Risposta sintetica: NO
(perché è strutturale)

Tuttavia: ad un progetto in corso è possibile valutare contromisure, mediante strumenti Safety Assessment e successivo Gap Analysis

Potrebbe avere un costo piu elevato, oppure fornire livello SIL inferiore)

La Certificazione

Quando è necessaria? Il famoso ISA

What is Independent Safety Assessment (ISA)?
A Guidance document provided by the Independent Safety Assurance Working Group, © ISA Working Group 2011

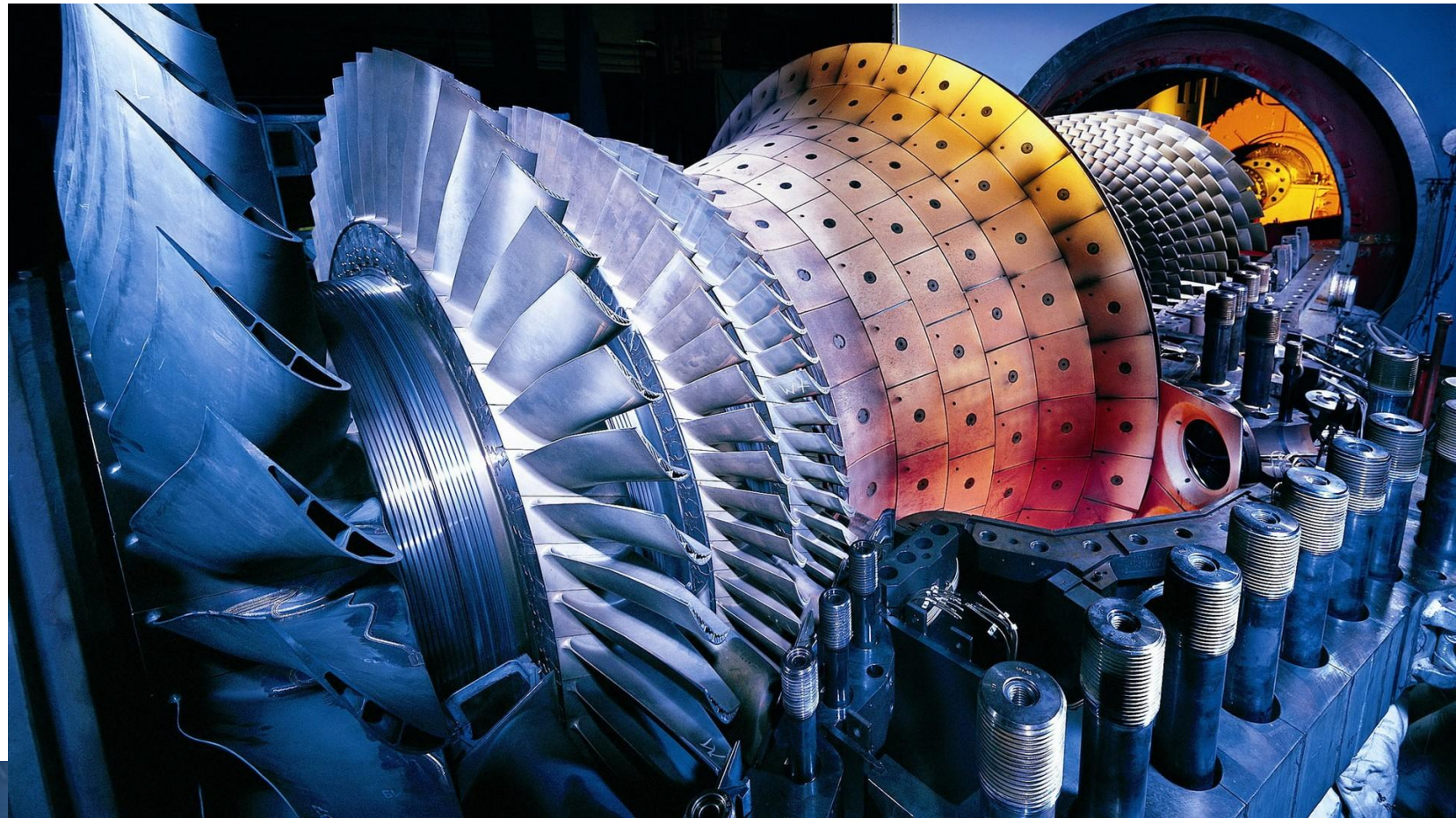
Who uses Independent Safety Assessors?

Anyone who needs or wants an independent assessment of safety. Reasons include:

- To comply with a standard that requires an ISA
- To be assured that a contractor's product is safe
- To assure your customer that what your product is safe
- To assure yourself that your product is safe
- To demonstrate to a regulator that your product is safe

Because the safety assessment provided by the ISA is independent of existing safety analysis and assessment, it can provide confidence that safety claims are justified and that any weaknesses that are identified have been dealt with appropriately.
In some situations an ISA is mandatory. For instance, when carrying out work on safety critical systems for the UK railway industry.

Industrie e casi reali



Succede sempre

“Noi dobbiamo fare il prodotto! ...la safety serve, **ma verrà dopo**...”

“Eh, noi facciamo una cosa semplice. **Non è che dobbiamo fare un missile**, è solo un [es: macchinario,... trattore,... dispositivo,... ascensore,…etc]”

“Lo testiamo noi **a mano**”

“Dobbiamo andare in produzione e fare una Safety **semplificata**”

“Abbiamo gia fatto un progetto **quasi** Safety.

“Safety la conosciamo, ci abbiamo dato **un occhio**”

“L’hardware **è gia fatto**”

“**Intanto iniziamo** e ci studiamo, poi faremo formazione se abbiamo bisogno”

Non esiste “un po' di” safety.
E’ un processo unitario

Industrial (Marine Application)

Grande Industria

Safety Standard		IEC 61508
Safety manager		Partial (Hardware Only)
Hardware Safety		Parziale
Competenze Software		NO
Certificazione Finale (ISA)		Ready
Decisione		Gap Analysis + Assessment Hardware Progetto Completo Affiancamento Safety Expert

CAV- Commercial, Construction, Agricultural

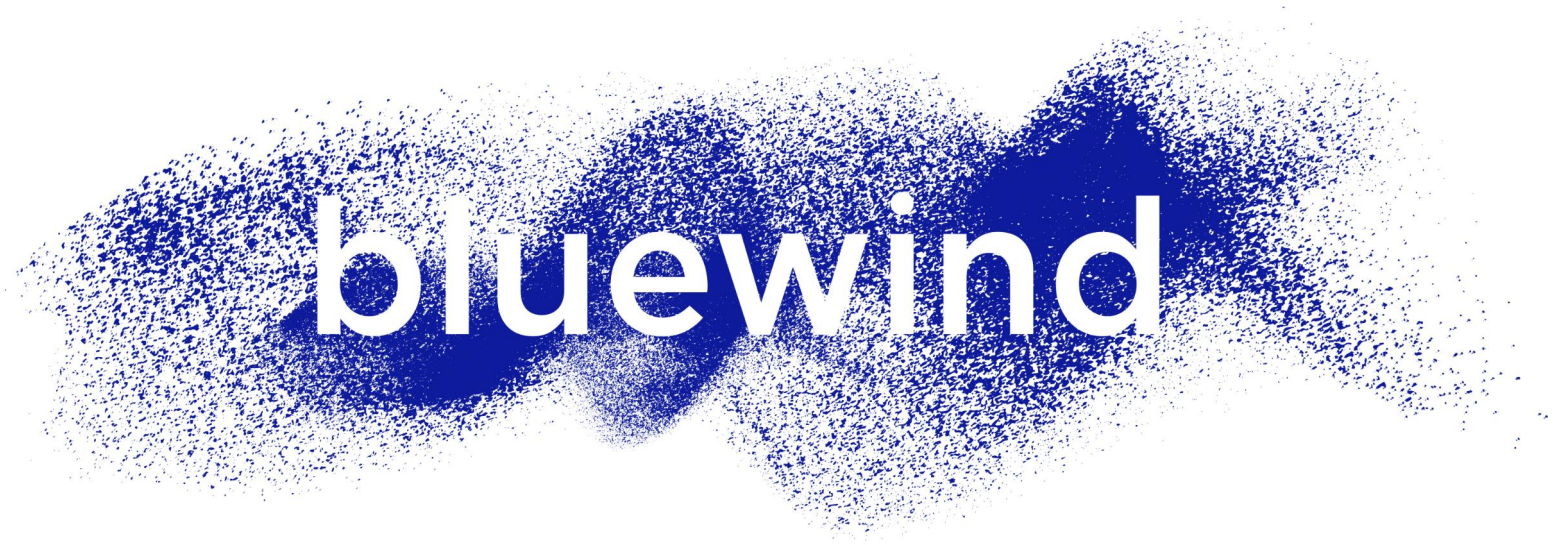
PMI

Safety Standard	To Be defined fare il minimo possibile, ma pronto per la safety" .	Not mandatory- Different Concurrent norms possible
Safety manager	(was sucbontracted to supplier)	NO
Hardware Safety		NO
Competenze Software Safety		NO
Certificazione (ISA)		To be defined
Decisione		-Assessment on applicable standards -Market requirements and cost/benefits

Industrial Electrical Drives -eMotorbykes

PMI

Safety Standard	To Be defined	Possible norms: EN 26262, IEC 61508
Safety manager		NO
Hardware Safety		In Corso
Competenze Software Safety		Incomplete
Certificazione (ISA)		Ready
Decisione		Assessment on Standard applicability



Nicola Bergamin
nicola.bergamin@bluewind.it
linkedin.com/in/nicolabergamin

www.bluewind.it/safety