SIA - Società Italiana Avionica S.p.A.

# Fasi del ciclo di vita
# Overview

# Perché un Ciclo di Vita nel *System Engineering* …

# Introduzione del ciclo di vita nel *System Engineering* finalità:

Modularità

Individuazione più agevole delle componenti riutilizzabili

Ciclo di vita

Esaustività

Certezza di coprire tutte le fasi necessarie

Rapid prototyping

Analisi precoce di carenze e punti di forza del sistema

Dimostrabilità

Possibilità di documentare agevolmente il processo in sede di certificazione

# Fasi del ciclo di vita – *overview*

Ciclo di vita

Modularità *Individuazione più agevole delle componenti riutilizzabili*

la presenza, per ogni componente sistemistica, al minimo di:

- REQUISITI
- INTERFACCE ESTERNE
- ARCHITETTURA E DOCUMENTAZIONE DI SVILUPPO
- TEST DEI REQUISITI

consente di incrementare la **modularità** del sistema

# Fasi del ciclo di vita – *overview*

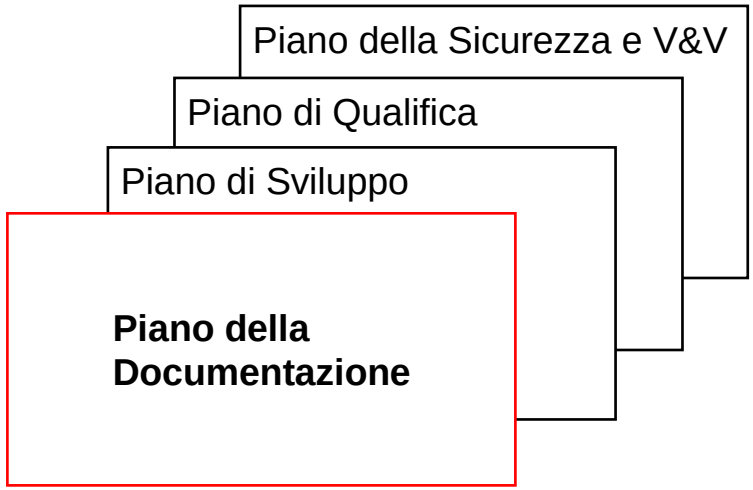
Ciclo di vita

**Esaustività** — *Certezza di coprire tutte le fasi necessarie*

Analisi del ciclo di vita →
- Vantaggi (modularità, dimostrabilità del processo, ecc)
- Costi (tempo e risorse per analisi e documentazione)

Individuazione delle versione *più idonea alla particolare applicazione*

Dalla definizione del ciclo di vita discendono:



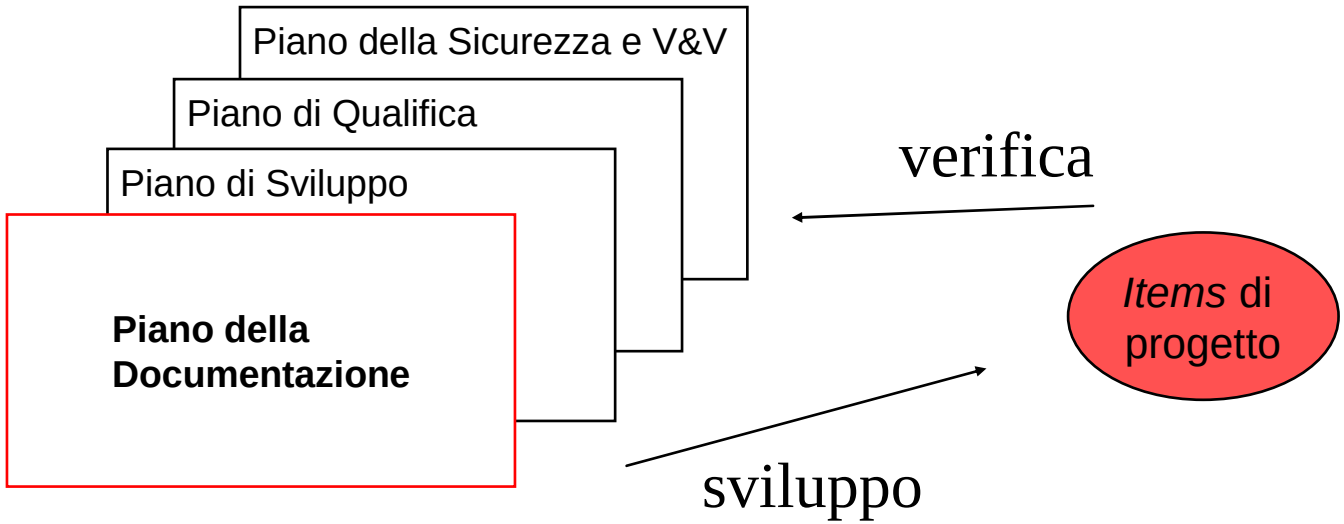
# Fasi del ciclo di vita – *overview*

Ciclo di vita

Esaustività

*Certezza di coprire tutte le fasi necessarie*

La garanzia della **esaustività** del processo discende dal confronto tra il **Piano della Documentazione** e i prodotti, confermato dalle attività di V&V



# Fasi del ciclo di vita – *overview*

Ciclo di vita

*Rapid prototyping* — *Analisi precoce di carenze e punti di forza del sistema*

Capitolato cliente

Altri requisiti iniziali (*standard*, condiz operative, sistemi esistenti in Azienda, ecc)

Analisi funzionale di sistema

Requisiti di sistema (funzionali / prestazionali)

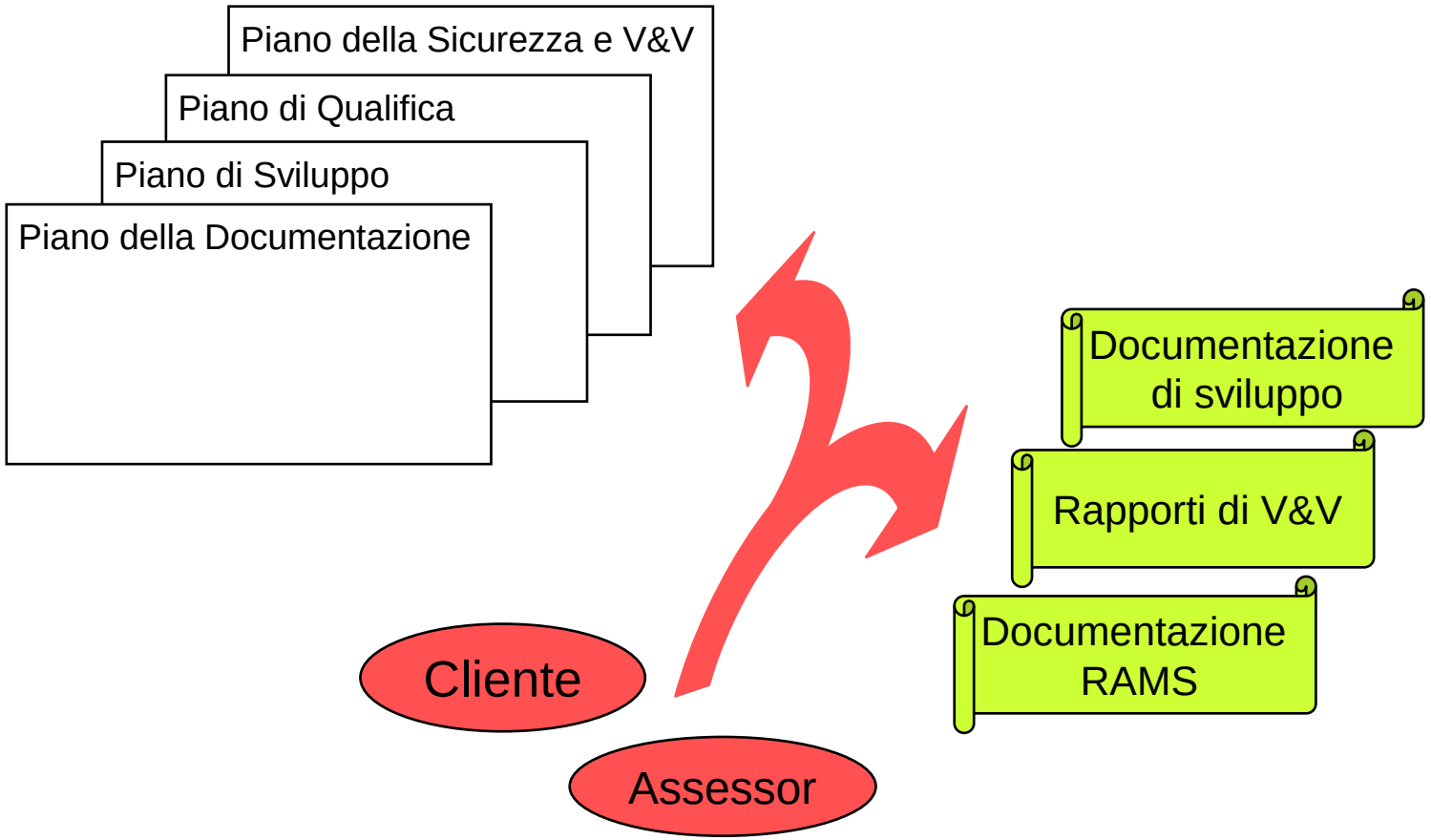
*Validazione analitica del requisito, simulazione, confronto con sistemi esistenti*

# Fasi del ciclo di vita – *overview*

Ciclo di vita

Dimostrabilità

*Possibilità di documentare agevolmente il processo in sede di certificazione*

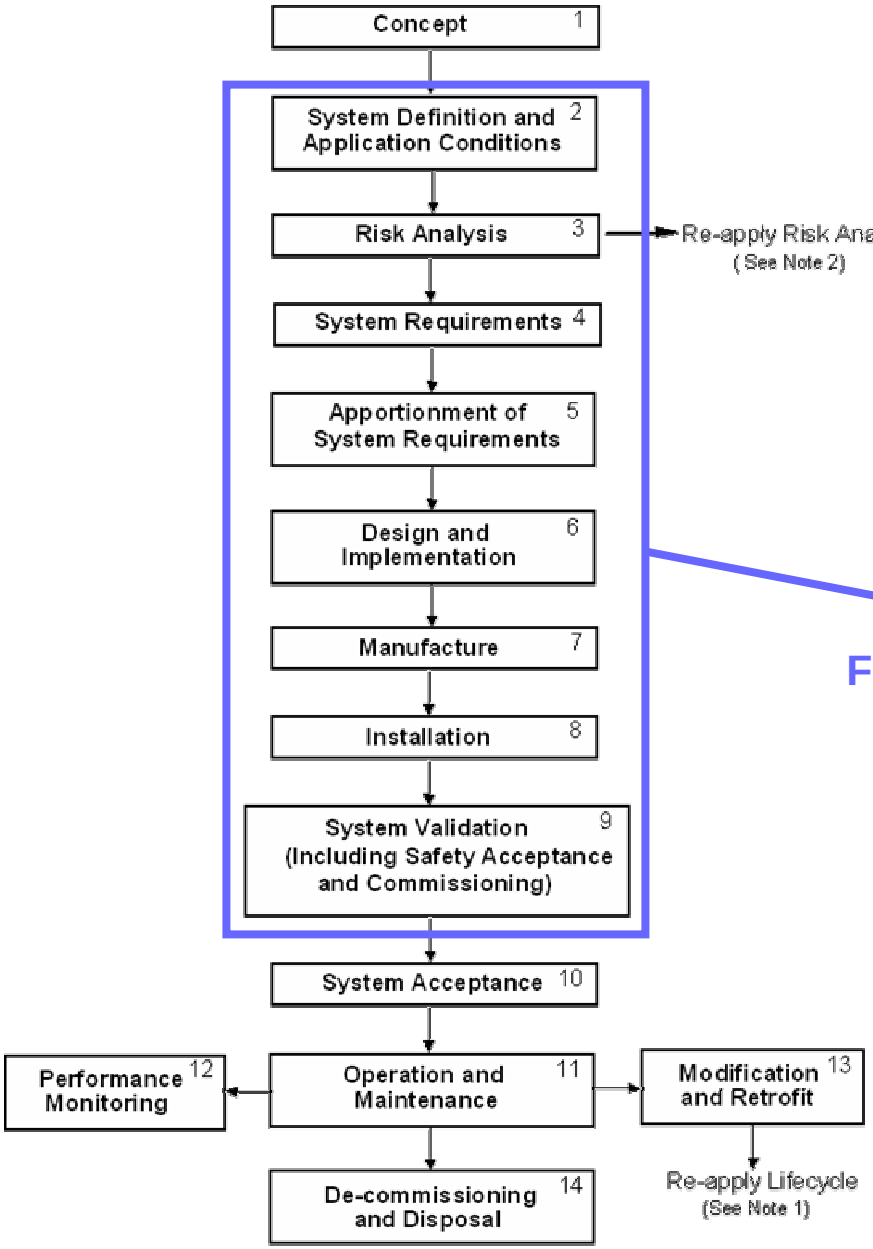


# Fasi del ciclo di vita – *overview*

## NORMATIVE di RIFERIMENTO:

- **CENELEC EN 50126** - ***Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety*** **(RAMS)**
- **CENELEC EN 50128** - ***Railway applications - Software for railway control and protection systems***
- **CENELEC EN 50129** - ***Railway Applications - Safety related electronic systems for signalling***
- **CENELEC EN 50124-1** ***Railway application - Insulation coordination - Part 1: Basic requirements - clearances and creepage distances for all electrical and electronic equipment***
- **CENELEC EN 50121** ***Railway application - emc***

# Fasi del ciclo di vita – *overview*



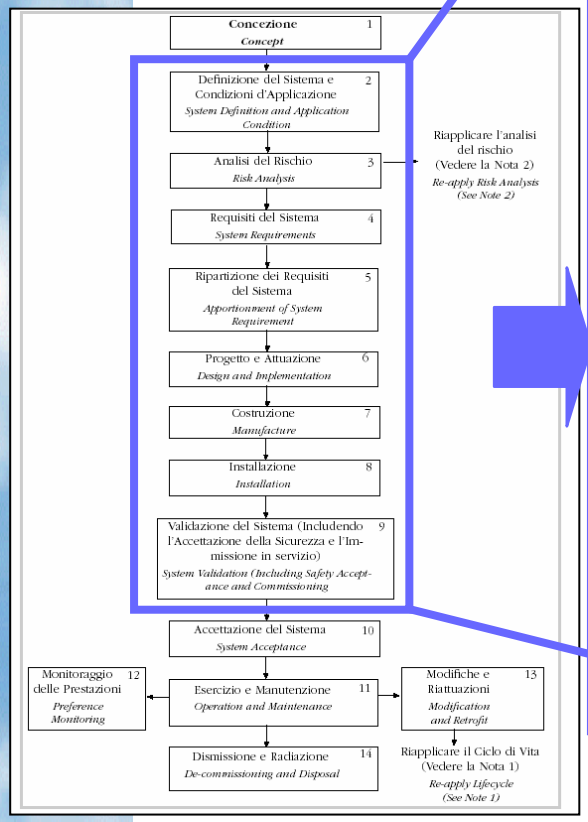

Sequenza logica delle fasi
(CENELEC 50126)

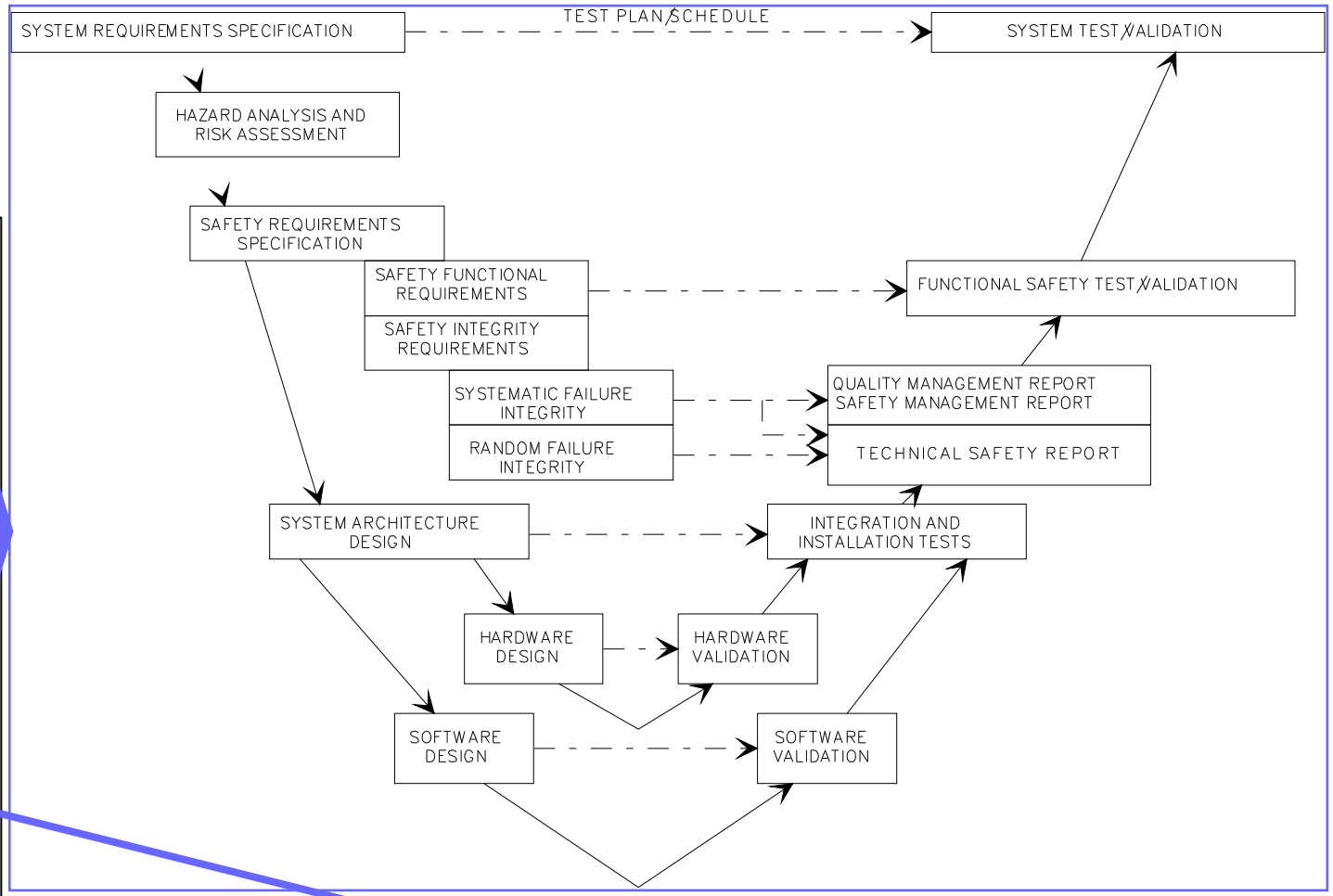
**Fasi di Sviluppo e Validazione**

# Fasi del ciclo di vita – *overview*



Sequenza logica delle fasi
(CENELEC 50126)



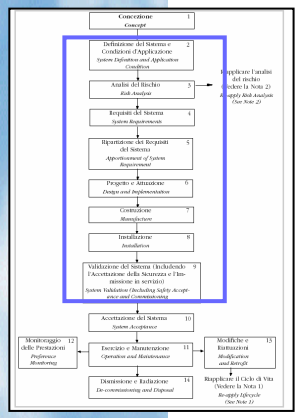




**Fasi di Sviluppo e Validazione (dettaglio)**

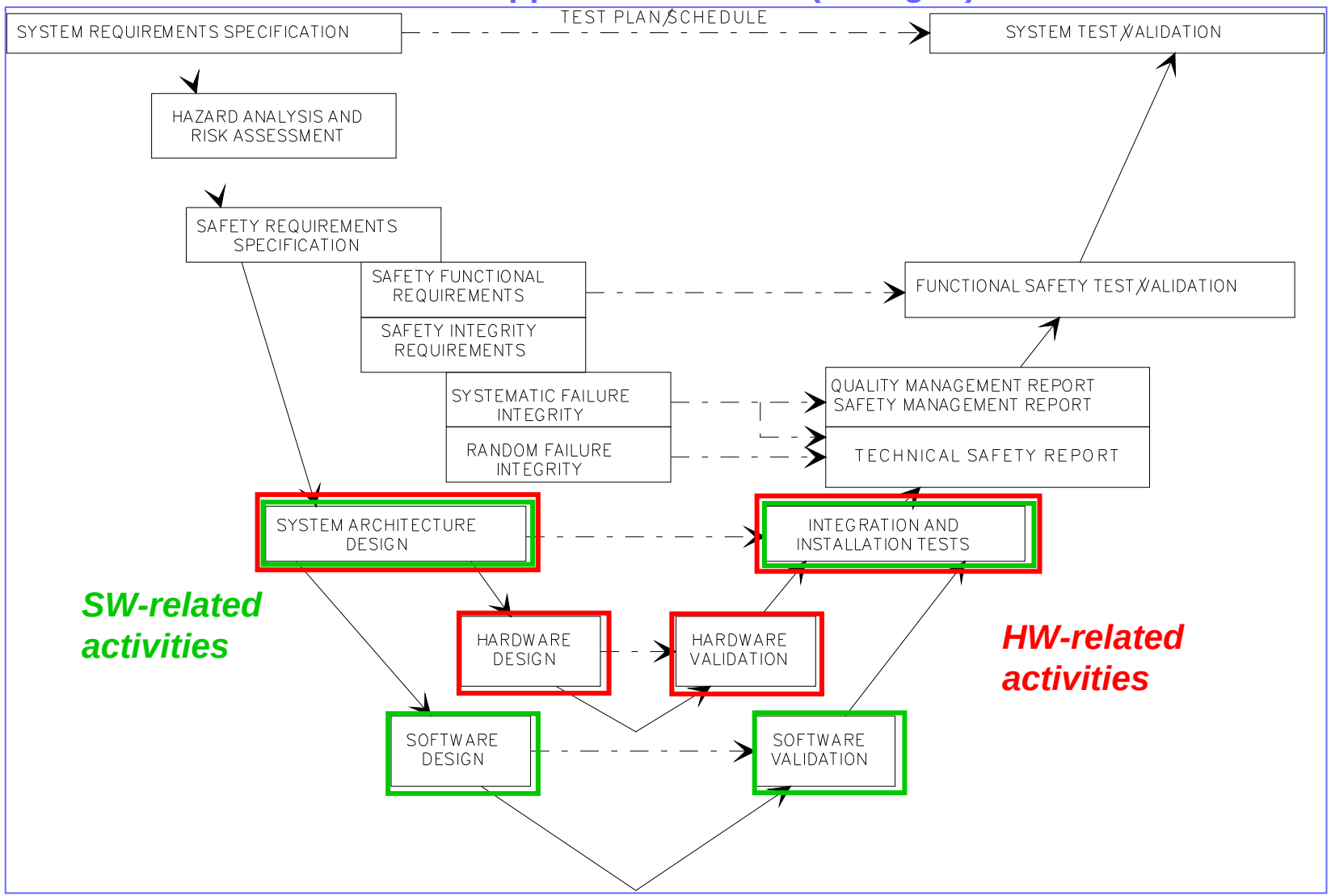
# Fasi del ciclo di vita – *overview*



Sequenza logica delle fasi (CENELEC 50126)

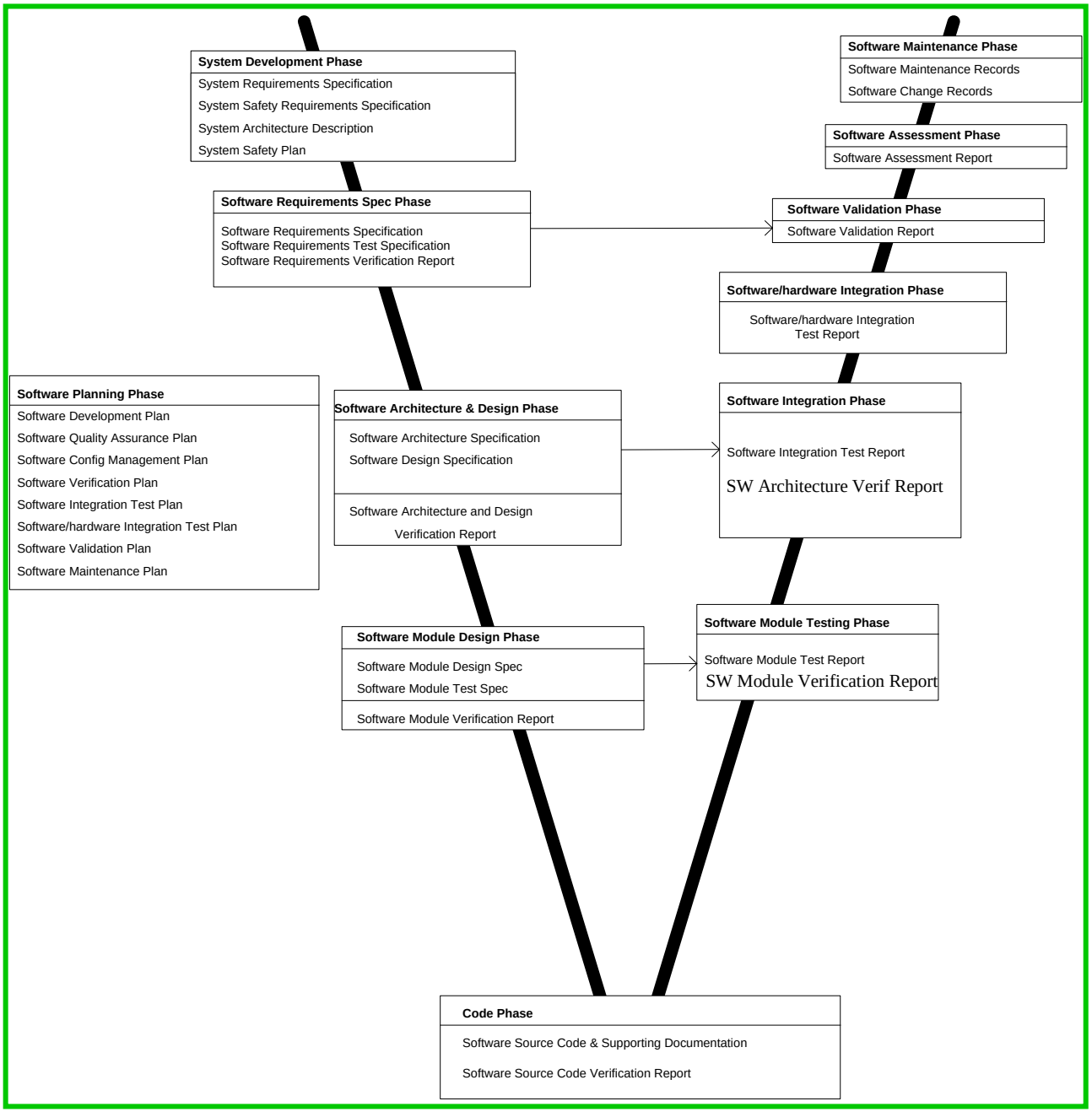


## Fasi di Sviluppo e Validazione (dettaglio)



# Fasi del ciclo di vita – *overview*

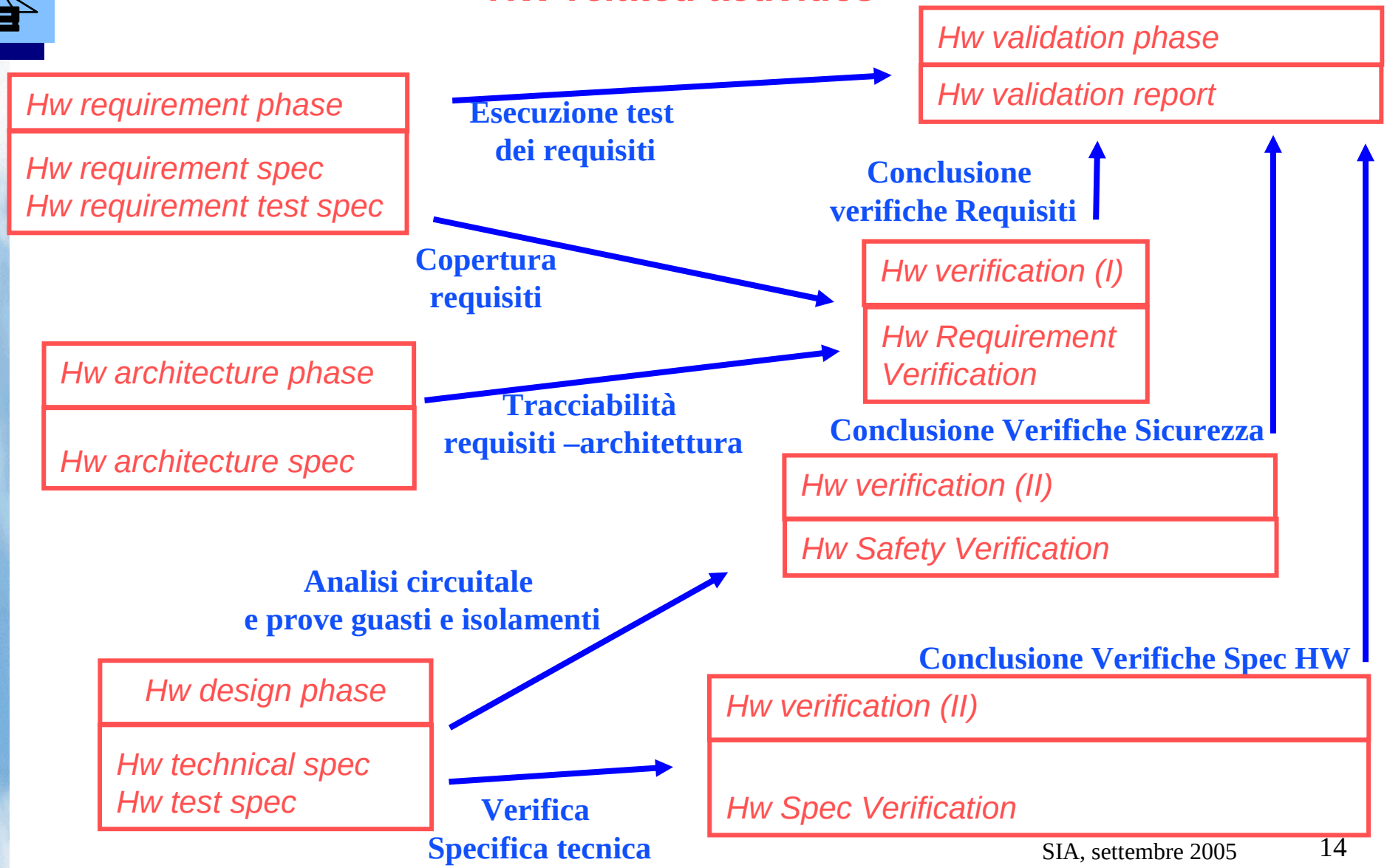





***SW-related activities***
**(CENELEC 50128)**

# Fasi del ciclo di vita – *overview*

## *HW-related activities*



SIA - Società Italiana Avionica S.p.A.

# Fasi del ciclo di vita
# fase 1 - Concezione

# Fase 1 - Concezione



Concezione del sistema

Studio di fattibilità tecnica

Valutazione commerciale e di programma

SIA - Società Italiana Avionica S.p.A.

# Fasi del ciclo di vita
# fase 2 – Definizione di Sistema

# Fase 2 – Definizione di Sistema

Studio di fattibilità tecnica

Valutazione commerciale e di programma

Definizione del sistema

Profilo di missione

Piano di *Safety*

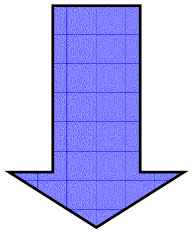
Condizioni applicative

SIA - Società Italiana Avionica S.p.A.

# Fasi del ciclo di vita
# Fase 3 - Analisi di rischio

## Concetti generali

- **Il rischio dipende da:**
  1. ***Frequenza di accadimento di situazioni pericolose***
  2. ***Conseguenze derivanti dalle situazioni pericolose***



**Criteri di Classificazione per:**

***Frequenza di accadimento***

***Conseguenze***

## Concetti generali

# Classificazione della frequenza di accadimento (CENELEC 50126)

| Livello | Frequenza di accadimento | Definizione |
|---|---|---|
| **A** | **Frequente** | Probabile che accada frequentemente. La situazione pericolosa si presenterà continuamente |
| **B** | **Probabile** | Accadrà parecchie volte. Ci si può aspettare che la situazione pericolosa si presenti spesso |
| **C** | **Occasionale** | Probabile che accada parecchie volte. Ci si può aspettare che la situazione pericolosa si presenti parecchie volte |
| **D** | **Remoto** | Probabile che accada qualche volta nella vita del sistema. Ci si può ragionevolmente aspettare che la situazione pericolosa si presenti |
| **E** | **Improbabile** | Improbabile che accada ma possibile. Si può assumere che la situazione pericolosa possa presentarsi eccezionalmente |
| **F** | **Incredibile** | Estremamente improbabile che accada. Si può assumere che la situazione pericolosa possa non presentarsi |

# Classificazione delle conseguenze

| Classe | Livello di gravità | Definizione |
|---|---|---|
| 4 | Catastrofico | Morte e/o parecchie persone ferite e/o danni maggior all'ambiente |
| 3 | Critico | Morte di una persona e/o lesione grave di una persona e/o importante danno all'ambiente |
| 2 | Marginale | Ferite leggere e/o importante minaccia per l'ambiente |
| 1 | Trascurabile | Possibile leggera ferita |

# Matrice di classificazione del rischio

| Frequenza di accadimento | Categoria di gravità | | | |
|---|---|---|---|---|
| | 4 Catastrofico | 3 Critico | 2 Marginale | 1 Trascurabile |
| A – Frequente | 4A | 3A | 2A | 1A |
| B – Probabile | 4B | 3B | 2B | 1B |
| C – Occasionale | 4C | 3C | 2C | 1C |
| D – Remoto | 4D | 3D | 2D | 1D |
| E – Improbabile | 4E | 3E | 2E | 1E |
| F – Incredibile | 4F | 3F | 2F | 1F |

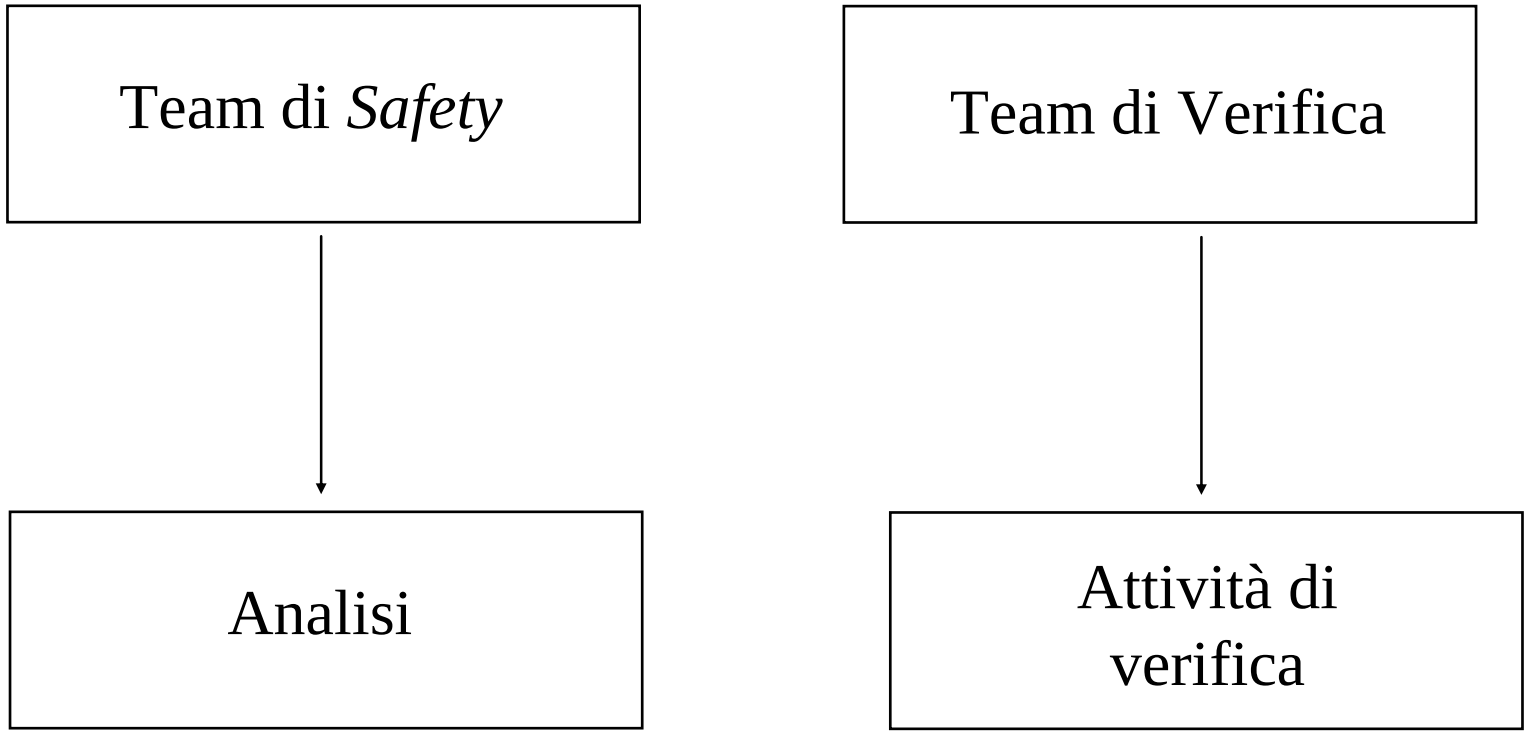
| Hazard Risk Index | Severity – Probability | Suggested Criteria |
|---|---|---|
| 1 | 4A, 4B, 4C, 3A, 3B, 2A | Unacceptable |
| 2 | 4D, 3C, 3D, 2B, 2C | Undesirable (Management Decision Required) |
| 3 | 4E, 4F, 3E, 2D, 2E, 1A, 1B | Acceptable with Review by Management |
| 4 | 3F, 2F, 1C, 1D, 1E, 1F | Acceptable without Review |

# Descrizione della fase

- **Attori**
- **Elementi di ingresso**
- **Attività**
- **Elementi di uscita**
- **Verifica**

# Attori

- **Gruppo di Verifica e Validazione**



# Elementi di ingresso

- **Elementi di ingresso per la fase**
  1. **Indicazioni generali sulle funzionalità del sistema**
  2. **Indicazioni generali sull'ambiente operativo**

# Attività

- ***Preliminary Hazard Analysis* (PHA)**
- ***Hazard Analysis***
- ***Hazard Log***

# *Preliminary Hazard Analysis*

- **Obiettivi**
  1. **Identificazione degli *hazard***
  2. **Identificazione delle cause**
  3. **Determinazione del rischio associato alle situazioni pericolose (FMEA) e delle misure di riduzione**

**FMEA**: *Failure Mode and Effects Analysis*

# PHA - Identificazione degli *hazard*

- **L'identificazione degli *hazard* avviene mediante**

1. **Utilizzo di *checklist* di natura ferroviaria (PHL)**
2. **Indagini mirate alla funzionalità del sistema in esame (HAZOp)**
3. **Utilizzo di informazioni derivanti dall'esperienza dell'analista**
4. **Utilizzo di informazioni derivanti da standard e normative**

Risultato di queste attività è la *Hazard List*

# PHA - Identificazione delle cause

- **Viene eseguita effettuando una analisi FMEA del sistema, nella quale sono evidenziate:**
  1. **Cause esterne (materiali particolari, condizioni ambientali, fattori umani, ecc.)**
  2. **Malfunzionamenti propri del sistema**
  3. **Malfunzionamento delle interfacee di connessione**
- **I risultati sono riportati in forma tabellare (tabella Id delle Cause)**

| | | | Causa | | Effetto sul sistema |
|---|---|---|---|---|---|
| I.D. | Funzione/ Interfaccia | Deviazione | Tipo | Categoria | |

# Determinazione e riduzione del rischio

- **Raccogliendo solo le cause di *hazard* della tabella (ID delle Cause) si compone una nuova tabella (rapporto PHA) in cui viene**
  1. **Identificata la classe di rischio (RC) iniziale**
  2. **Identificate le misure per la riduzione del rischio**
  3. **Identificata la classe di rischio finale (accettabilità del rischio)**

| *Sub-Hazard* | | | *Hazard* sistema | Classi rischio e contromisure | | | |
|---|---|---|---|---|---|---|---|
| I.D. | Rif. AC. | Descr. | Descr. *(da Hazard list)* | RC Iniziale | Contromisure | RC Finale | Raccomandazioni |

Analisi delle cause (tabella precedente)

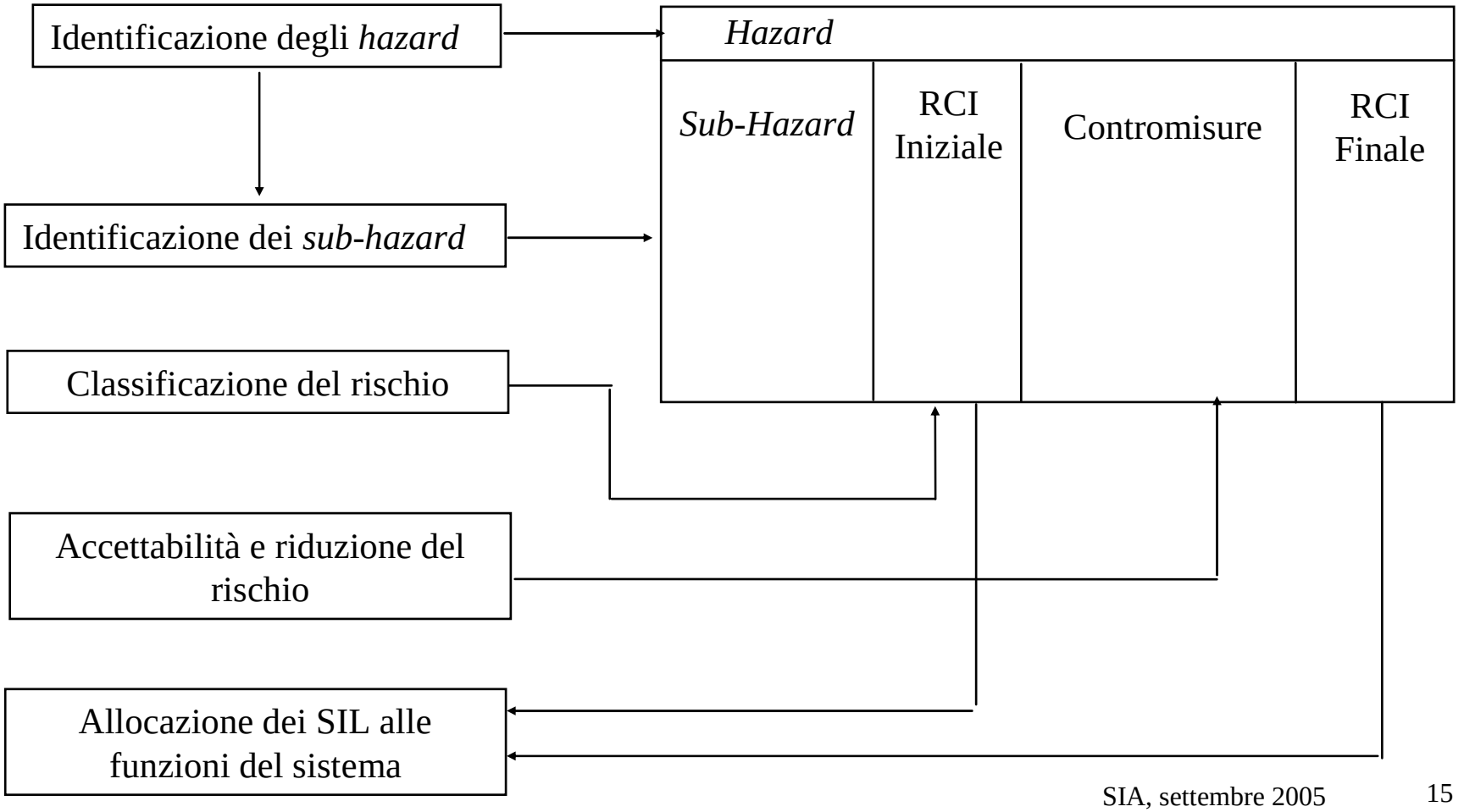
Requisiti di sicurezza

# Assegnazione del SIL

- **Safety Integrity Level (SIL)**
  1. **È relativo a funzioni del sistema**
  2. **È relativo a una soglia probabilistica di frequenza di eventi pericolosi**
  3. **Viene assegnato in funzione della classe rischio da raggiungere**
  4. **Riduce la frequenza di accadimento ma non muta la gravità**

# *Preliminary Hazard Analysis*

- **Riassumendo si ha il seguente processo**



# *Hazard Analysis*

- **Obiettivi**
  1. **Analisi delle condizioni operative del sistema**
  2. **Identificazione di nuove cause (*sub-hazard*)**
  3. **Identificazione di nuove misure di riduzione del rischio (contromisure)**

# *Hazard Log*

- **Il registro contiene**
  1. **L'evidenza di cause ed effetti delle situazioni pericolose**
  2. **Le misure utilizzate per la mitigazione del rischio**
  3. **La definzione di un criterio per il riesame della tollerabilità del rischio**
  4. **I limiti di ogni analisi svolta**
  5. **I metodi, gli strumenti e le tecniche utilizzate**

# Elementi di uscita

- **Elementi di uscita della fase**
  1. ***Hazard* legati al sistema e cause che li generano**
  2. **Misure prese per la mitigazione delle cause**
  3. **Registro delle situazioni pericolose**

# Verifica

- **Le attività di verifica permettono di valutare**
  1. **La completezza delle valutazioni effettuate**
  2. **L'adeguatezza della classificazione del rischio**
  3. **L'adeguatezza delle modalità di registro delle attività**
  4. **La correttezza dei metodi e delle tecniche utilizzate**