Fasi del ciclo di vita – *overview*

Finalità del ciclo di vita nel *System Engineering*

Ciclo di vita

Modularità

Individuazione più agevole delle componenti riutilizzabili

Esaustività

Certezza di coprire tutte le fasi necessarie

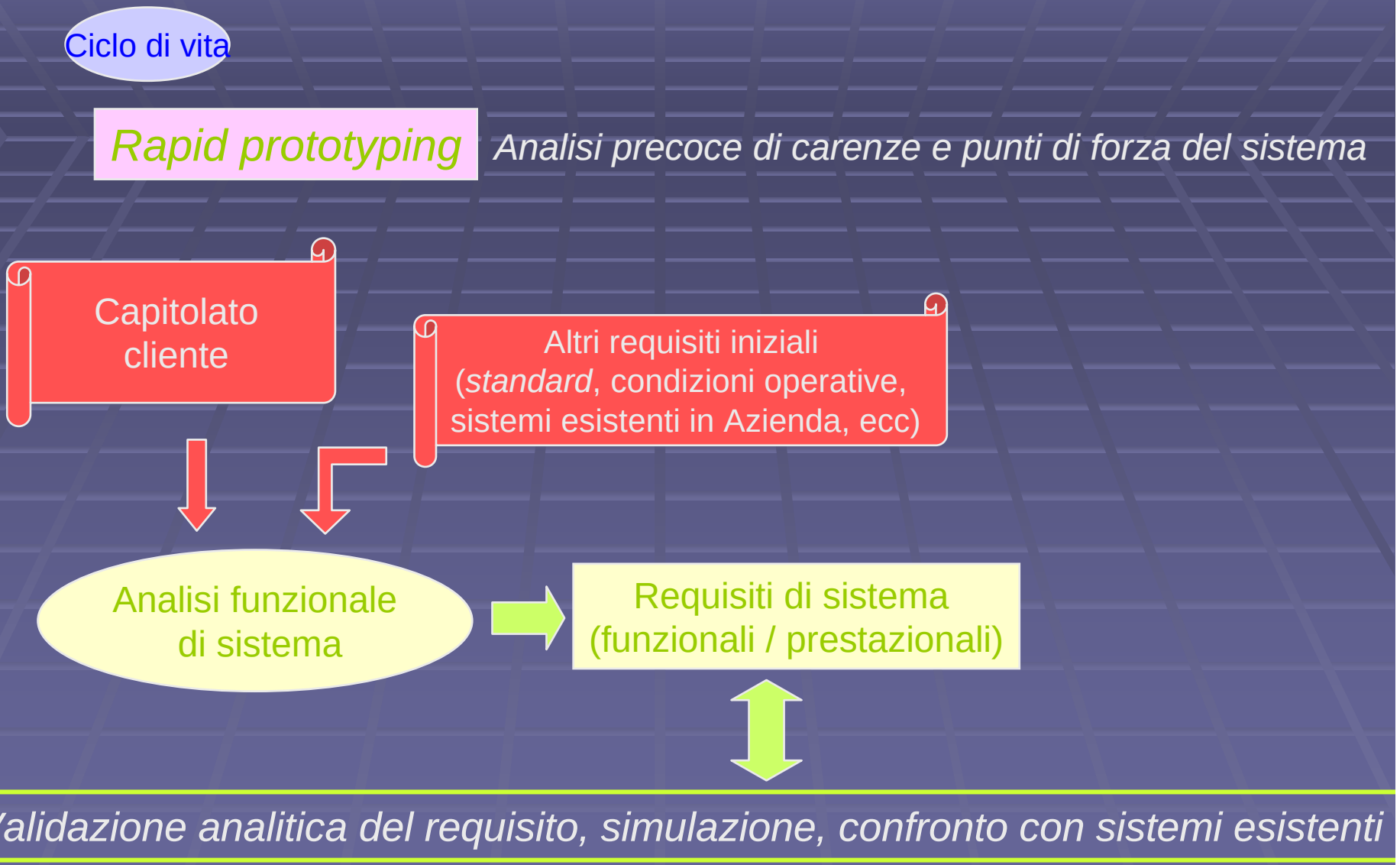
Rapid prototyping

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*

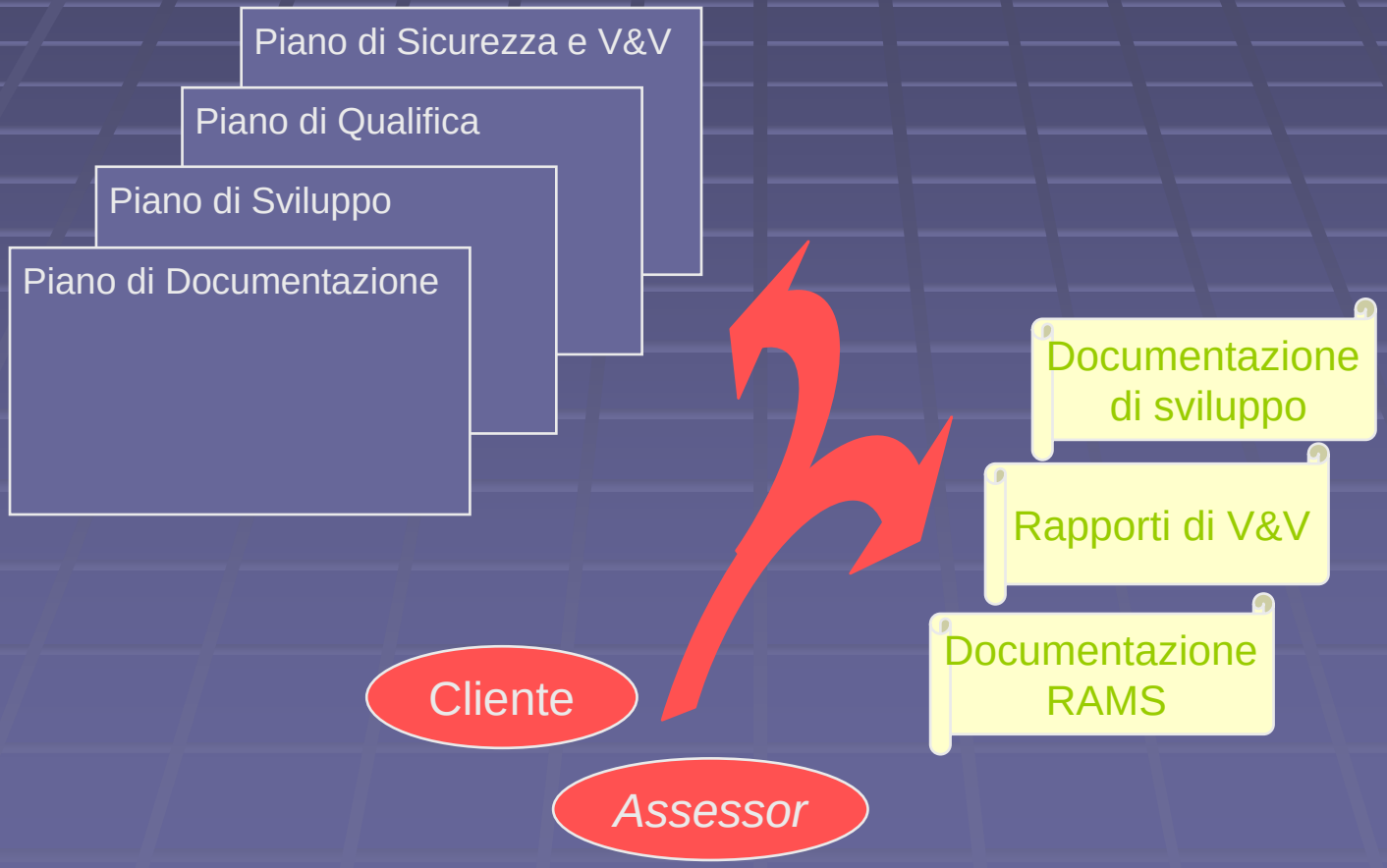


Fasi del ciclo di vita – *overview*

Ciclo di vita

Dimostrabilità

Possibilità di documentare agevolmente il processo in sede di certificazione

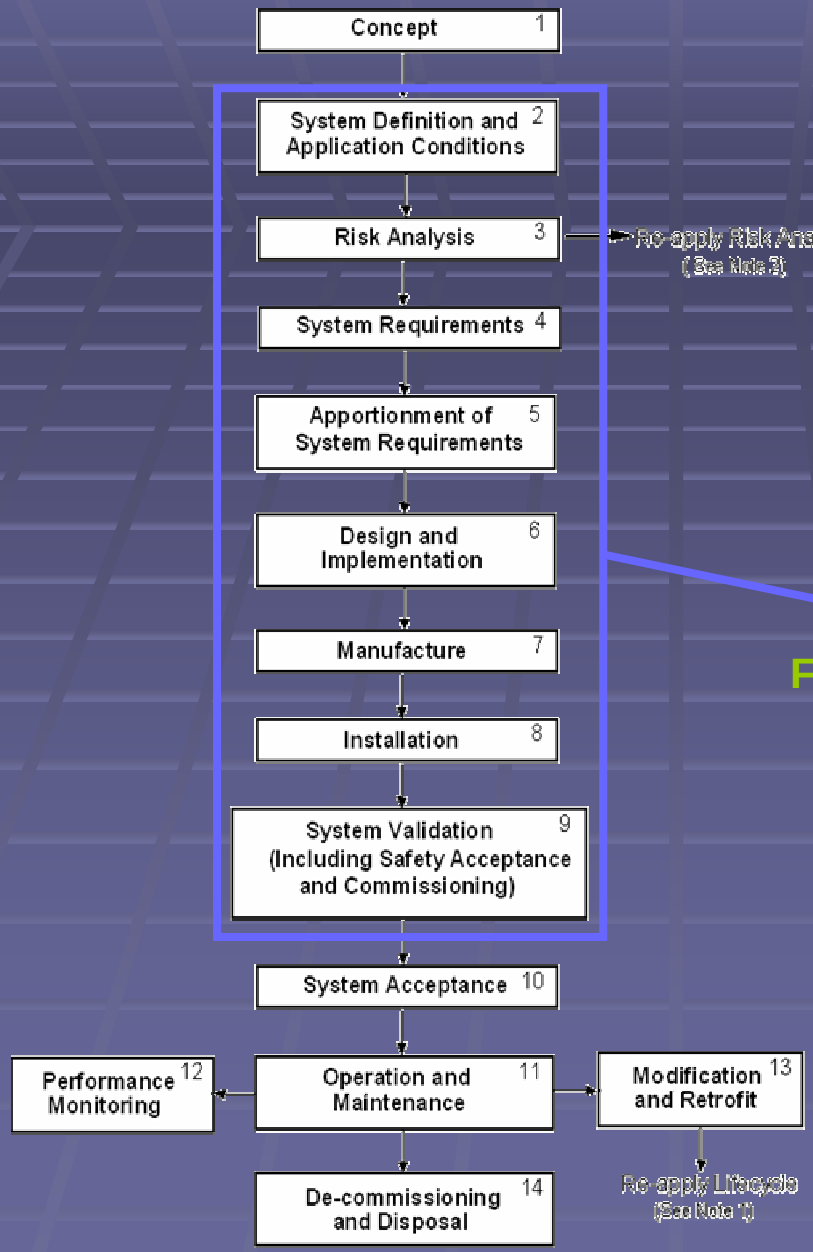


Fasi del ciclo di vita – *overview*

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*

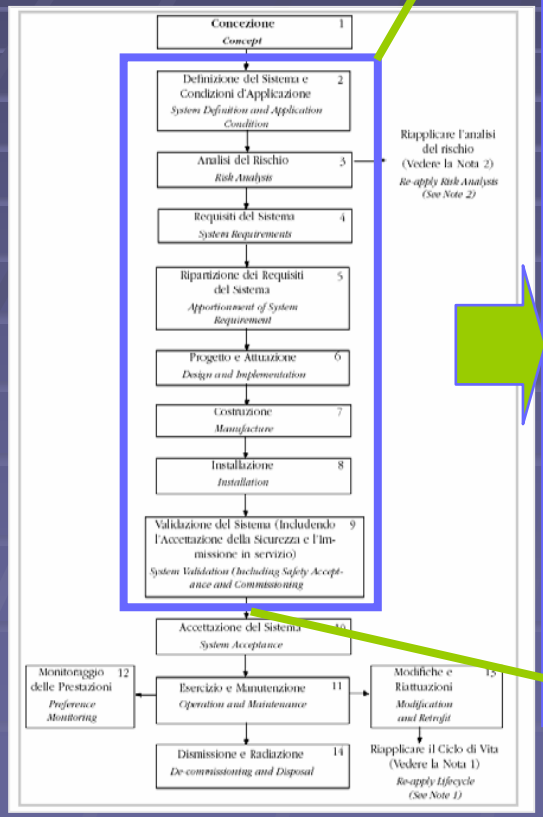


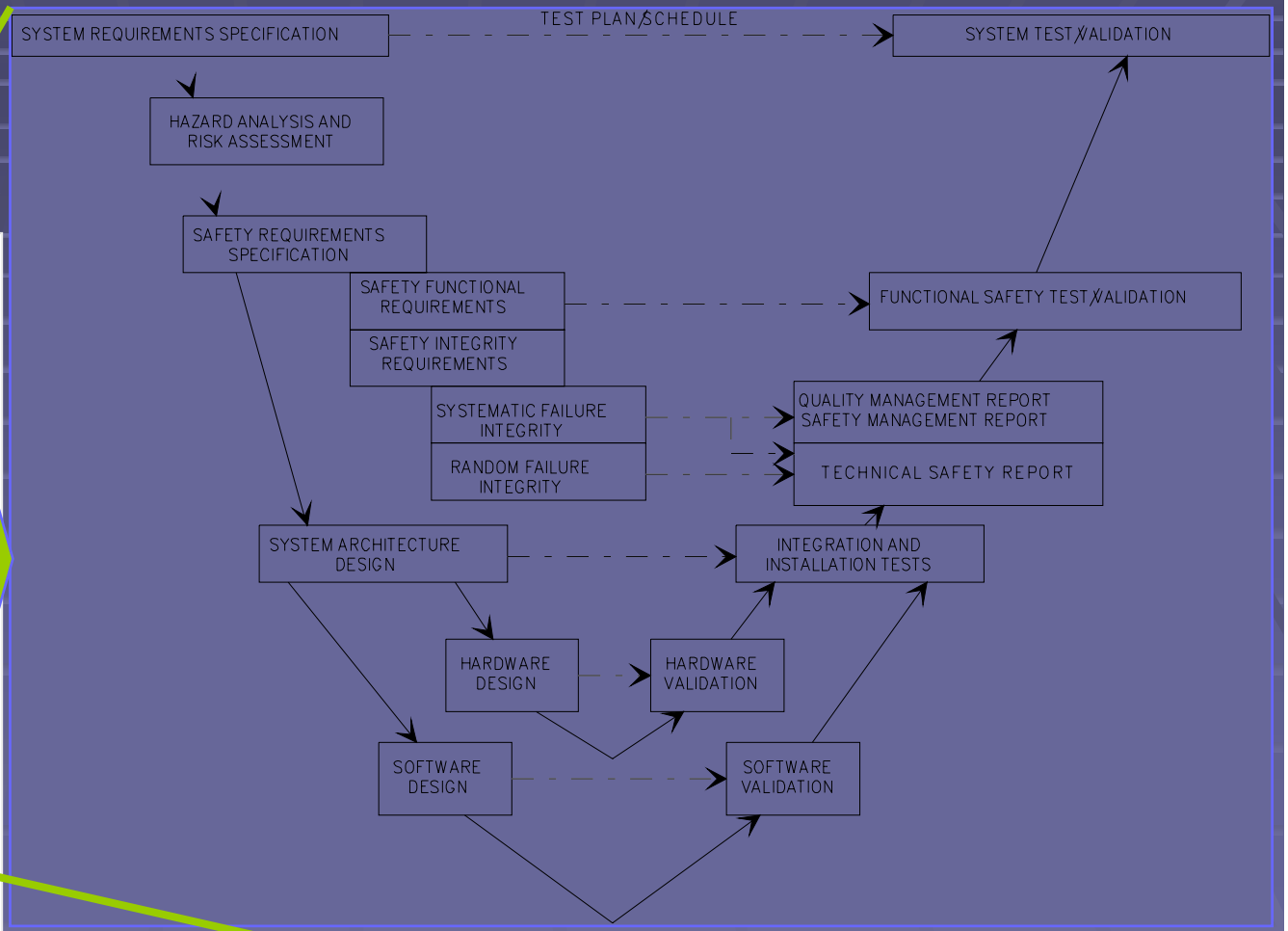
Sequenza logica delle fasi
(CENELEC 50126)

Fasi di Sviluppo e Validazione

Fasi del ciclo di vita – *overview*

Sequenza logica delle fasi
(CENELEC 50126)

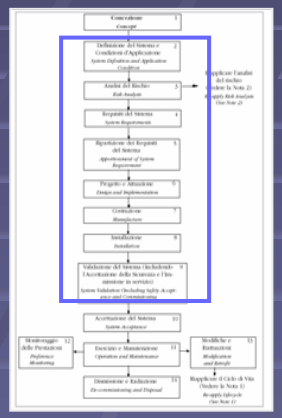




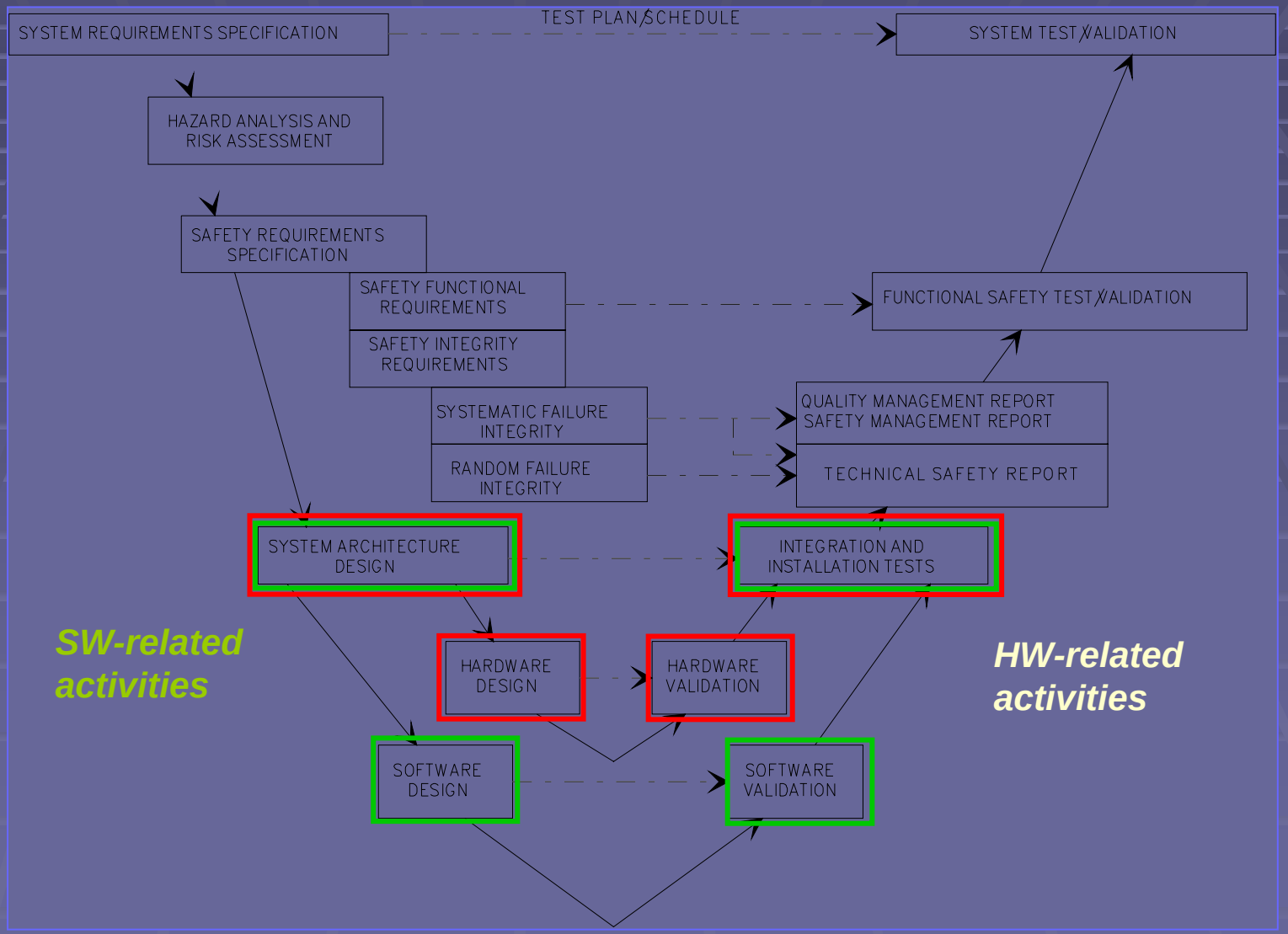
Fasi di Sviluppo e Validazione (dettaglio)

Fasi del ciclo di vita – *overview*

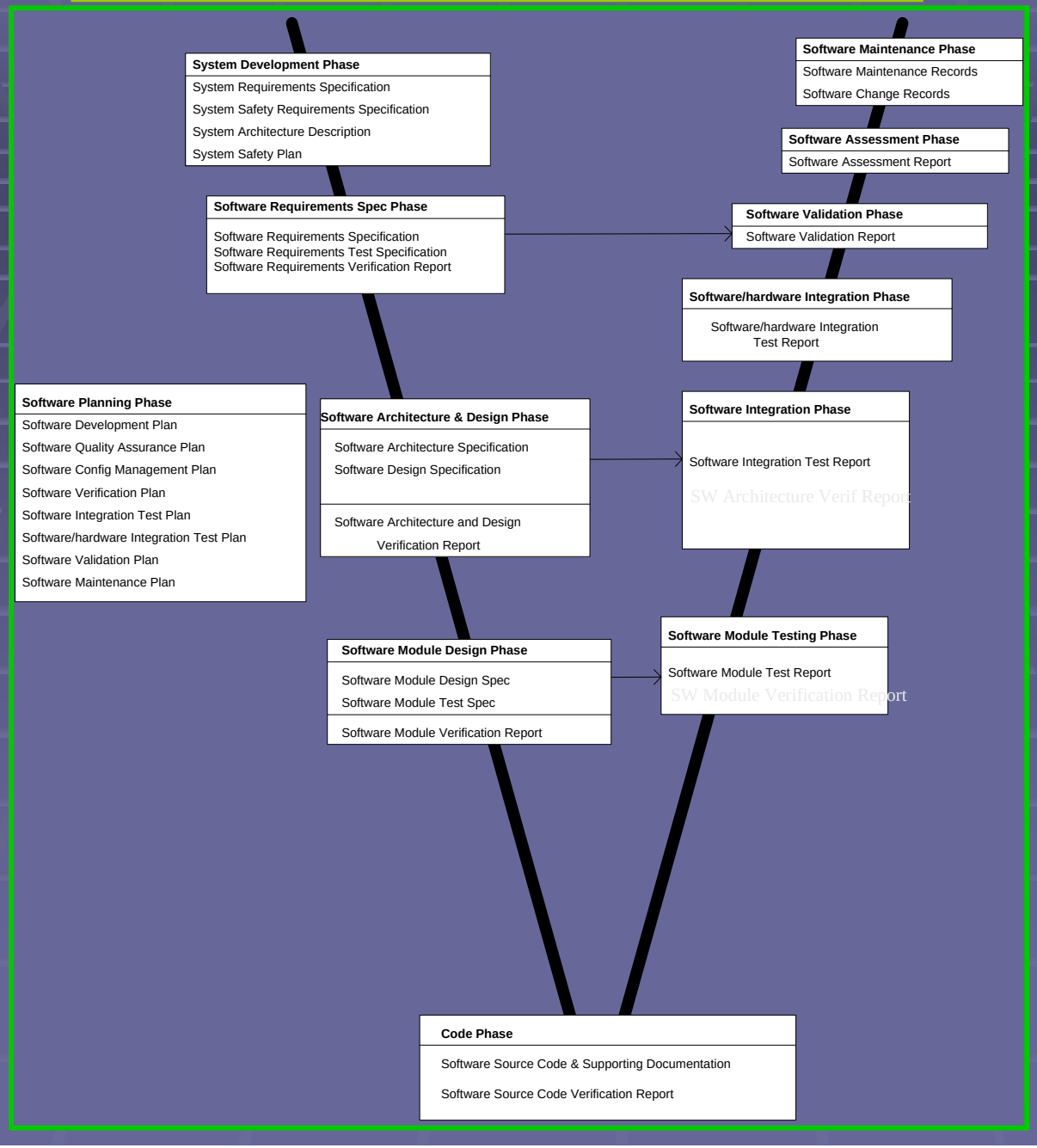
Sequenza logica delle fasi (CENELEC 50126)



Fasi di Sviluppo e Validazione (dettaglio)



Fasi del ciclo di vita – *overview*



SW-related activities
(CENELEC 50128)

Fase 2 – Definizione di Sistema

Studio di fattibilità tecnica

Valutazione commerciale e di programma

Definizione del sistema

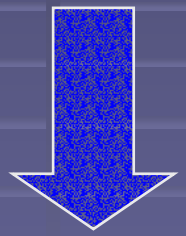
Profilo di missione

Piano di *Safety*

Condizioni applicative

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

Ing. C. Iapicca

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 per i 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

Ing. C. Iapicca

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

Ing. C. Iapicca

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

Ing. C. Iapicca

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 mitigazione

FMEA: *Failure Mode and Effects Analysis*
a volte chiamata anche
FME**C**A: … and Criticality …

PHA - Identificazione degli *hazard*

1. Utilizzo di *checklist* di dominio ferroviario
   - *Preliminary Hazard List* (PHL)
2. Indagini mirate alla funzionalità del sistema in esame
   - *Hazard and Operability studies* (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

- Eseguita effettuando una analisi FMEA del sistema nella quale sono evidenziate
  - *Cause esterne (materiali particolari, condizioni ambientali, fattori umani, ecc.)*
  - *Malfunzionamenti propri del sistema*
  - *Malfunzionamento delle interfacce di connessione*
- I risultati sono riportati in forma tabulare
  - Tabella Id delle Cause

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

Determinazione e riduzione del rischio

- Raccogliendo solo le cause di *hazard* della tabella (ID delle Cause) si compone una nuova tabella (rapporto PHA) ove si
  1. Identifica la classe di rischio (RC) iniziale
  2. Identificano le misure per la riduzione del rischio
  3. Identifica la classe di rischio finale
     - Accettabilità del rischio

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

Analisi delle cause (tabella precedente)

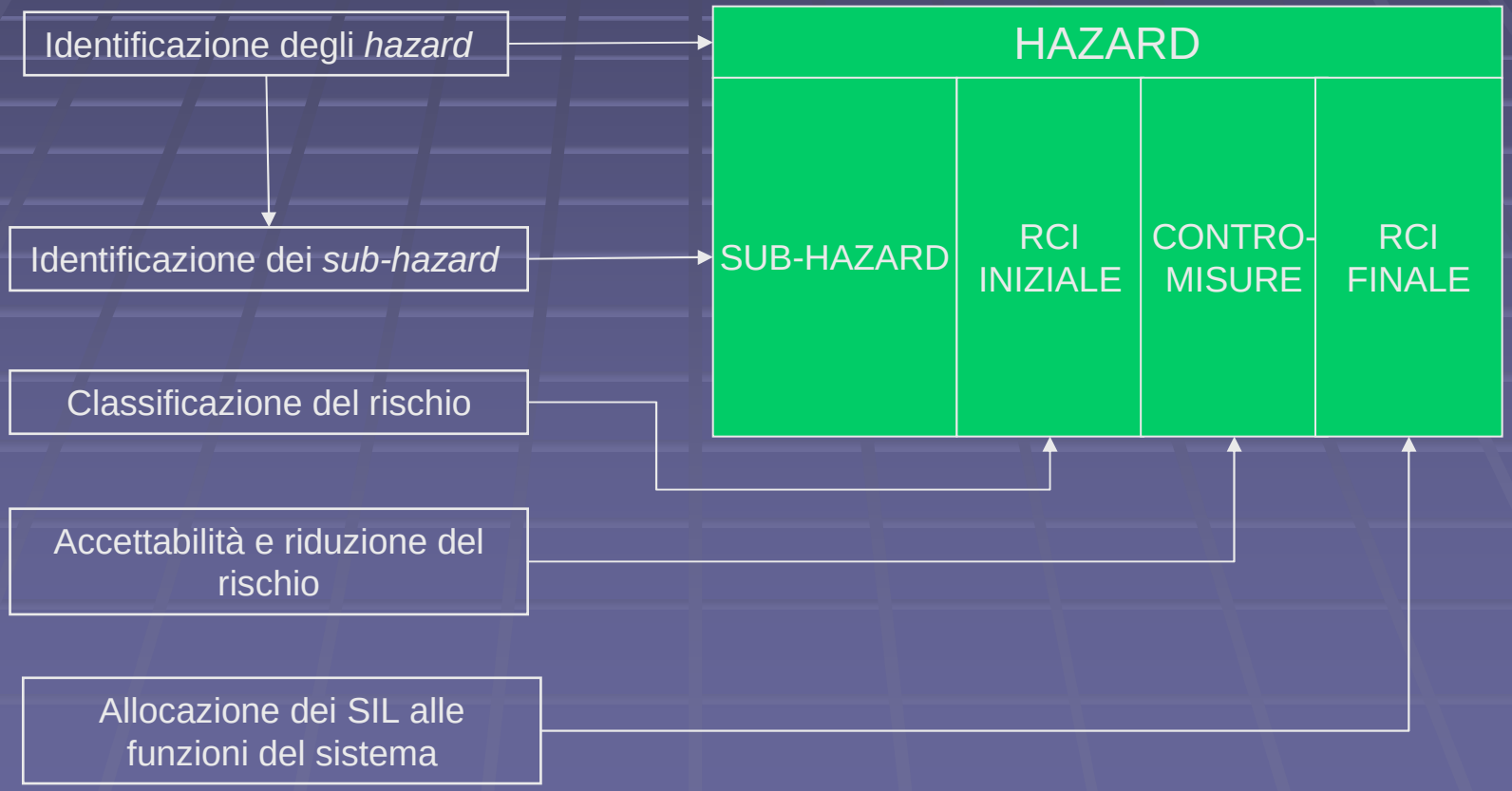
Requisiti di sicurezza

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 tramite mitigazione
  4. L'applicazione delle misure di mitigazione riduce la frequenza di accadimento ma non ne 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 definizione 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 dalla fase

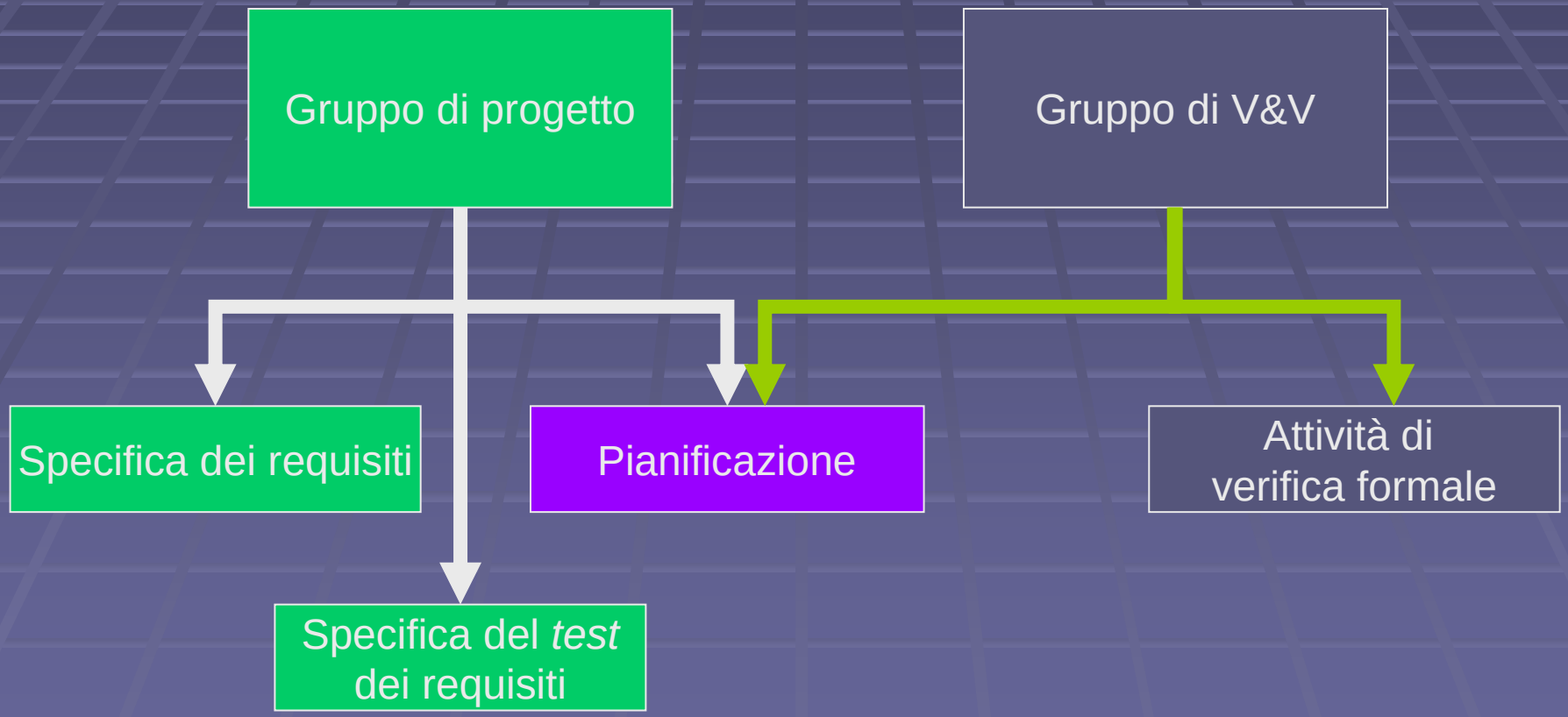
1. *Hazard* legati al sistema e cause che li generano
2. Misure prese per la mitigazione delle cause
3. Registro delle situazioni pericolose

Verifica

- Le attività del processo 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*

Fase 4 – Requisiti di Sistema

Attori



Specifica dei requisiti di sistema

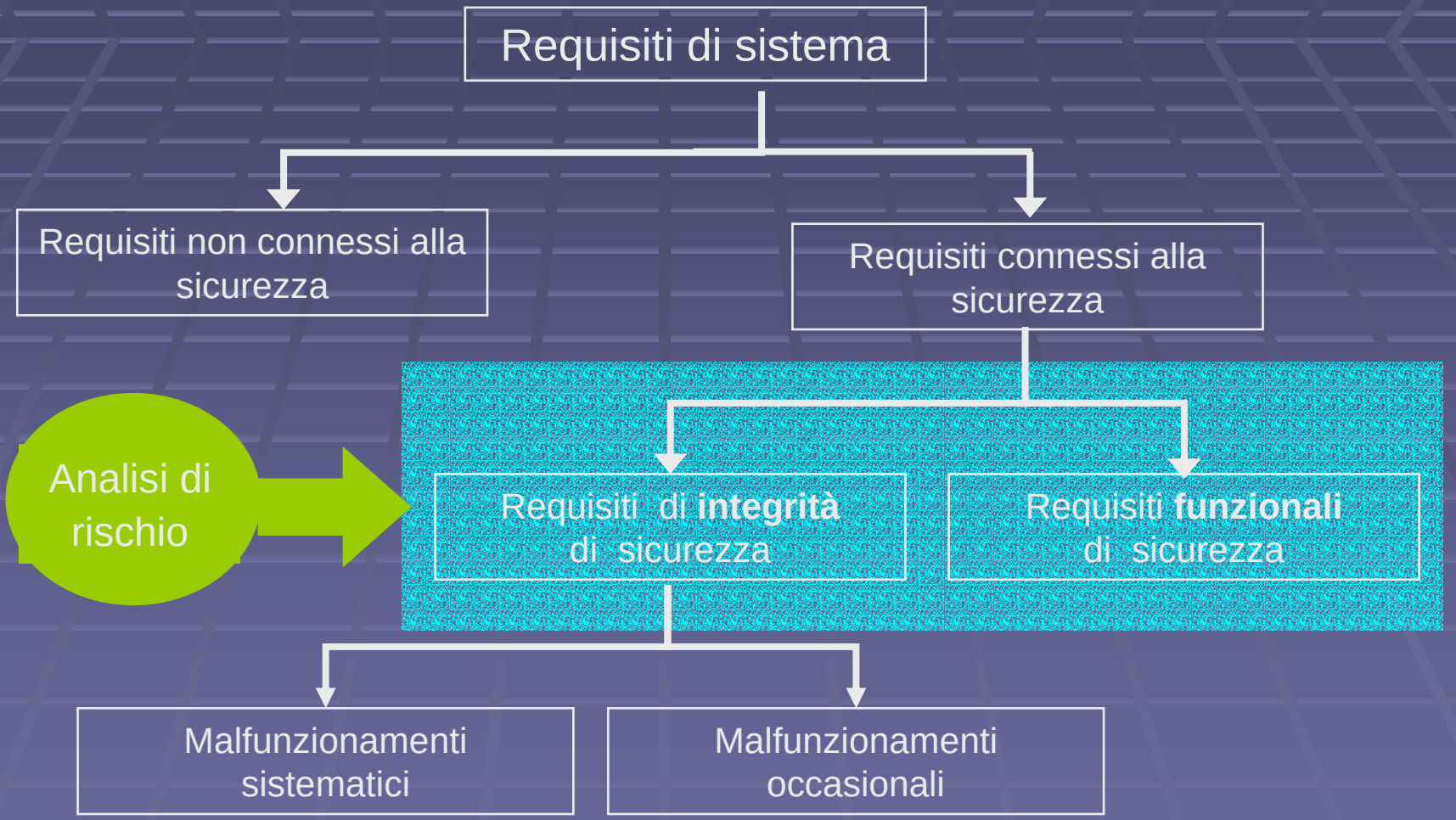
- Criteri generali
  1. Devono essere globali
     - Devono coprire l'intero sistema
  2. Devono formare una base per il progetto e per la sua ottimizzazione
  3. Devono consentire un approccio logico ed economico ai cambiamenti
  4. Devono essere testabili
     - Devono essere assoggettabili a procedure di *test*
  5. Devono essere tracciabili
     - Sulle richieste del cliente e sul capitolato
  6. Possono essere usati come chiara base contrattuale

Un requisito dice sempre cosa e mai come

Specifica dei requisiti di sistema

- Sorgenti di requisiti
  - Cliente
  - Normative vigenti
  - PHA
    - Uscita di fase 3
  - Fornitore
    - Cultura aziendale, riuso
- Categorie di requisiti
  - Funzionali
  - Di sicurezza (*safety*)
  - RAM (*reliability*, *availability*, *maintainability*)
  - Ambientali

Requisiti funzionali e di sicurezza



Requisiti RAM

- Affidabilità
  - Parametri *target* caratteristici
    - Del dominio, dell'ambiente, del materiale
- Manutenibilità
  - Parametri *target* caratteristici
  - Tipologia di manutenzione necessaria
    - Correttiva, adattiva (tipicamente non evolutiva)
- Disponibilità
  - Parametri *target* caratteristici
  - Necessità di scorte di magazzino
    - Anche per componenti *software* (ma nel suo modo proprio)

Metodi di specifica e SIL

Dai SIL derivano differenti metodi di specifica dei requisiti

Tecnica/Misura	SIL 1	SIL 2	SIL 3	SIL 4
Separazione fra sistemi correlati e non correlati alla sicurezza	**R**: Interfacce ben definite fra sistemi connessi e non alla sicurezza		**HR**: Interfacce ben definite fra sistemi connessi e non alla sicurezza e analisi interfacce	
Descrizione grafica esempio diagrammi a blocchi	**HR**		**HR**	
Specifiche strutturate	**HR**: Separazione gerarchica manuale, descrizione interfacce		**HR**: separazione gerarchica con uso di metodi formalizzati e controlli automatici di congruenza	
Metodi formali o semi formali			**R**: automatizzati (*computer-aided*)	
Strumenti di specifica assisti dal *computer*	--	**R**: qualunque strumento	**HR**: procedure orientate sui modelli con suddivisione gerarchica e controlli automatici di congruenza	
Checklist	**R**: *Checklist* elaborate per tutte le fasi del ciclo di vita		**R**: *Checklist* elaborate per tutte le fasi del ciclo di vita connesse alla sicurezza	
Hazard Log	**HR**: L'*Hazard Log* deve sempre essere tenuto aggiornato durante tutte le fasi del ciclo di vita del sistema			
Verifica delle specifiche	**R**		**HR**	

Specifica dei *test* dei requisiti di sistema

- Modalità di *test*
  - Ispezione visiva del sistema
  - Ispezione documentale
  - *Test* funzionale e di sicurezza (*safety*)
- Definizione dei criteri per la gestione di anomalie e modifiche
  - Istituzione di un registro delle anomalie
  - Metodi per la modifica del sistema e *test* di regressione
    - *Re-testing*

Specifica dei *test* dei requisiti di sistema

- Modalità: ispezione documentale
  - Azioni
    - Ricerca di parametri in documenti di analisi
    - Ricerca di risultati in documenti di analisi e/o di rapporti
  - Rispetto a requisiti soggetti a verifica tramite prova
    - RAM
    - Procedure di installazione
    - Procedure di collaudo
    - Conformità a requisiti

Ing. C. Iapicca

Specifica dei *test* dei requisiti di sistema

- Modalità: *test* funzionale e di sicurezza
  - Tipologie di *test*
    - *Test* intrusivi sul sistema
    - *Test black-box* funzionale
  - Requisiti soggetti a verifica tramite test F&S
    - Requisiti funzionali
    - Requisiti di sicurezza (*safety*)
    - Requisiti prestazionali

Specifica dei *test* dei requisiti di sistema

- Azioni per *test* funzionale e di sicurezza
  1. Definizione della strumentazione necessaria
  2. Definizione degli ambienti e/o scenari di test
  3. Definizione delle impostazioni iniziali
  4. Definizione delle procedure di esecuzione
  5. Definizione dei risultati attesi

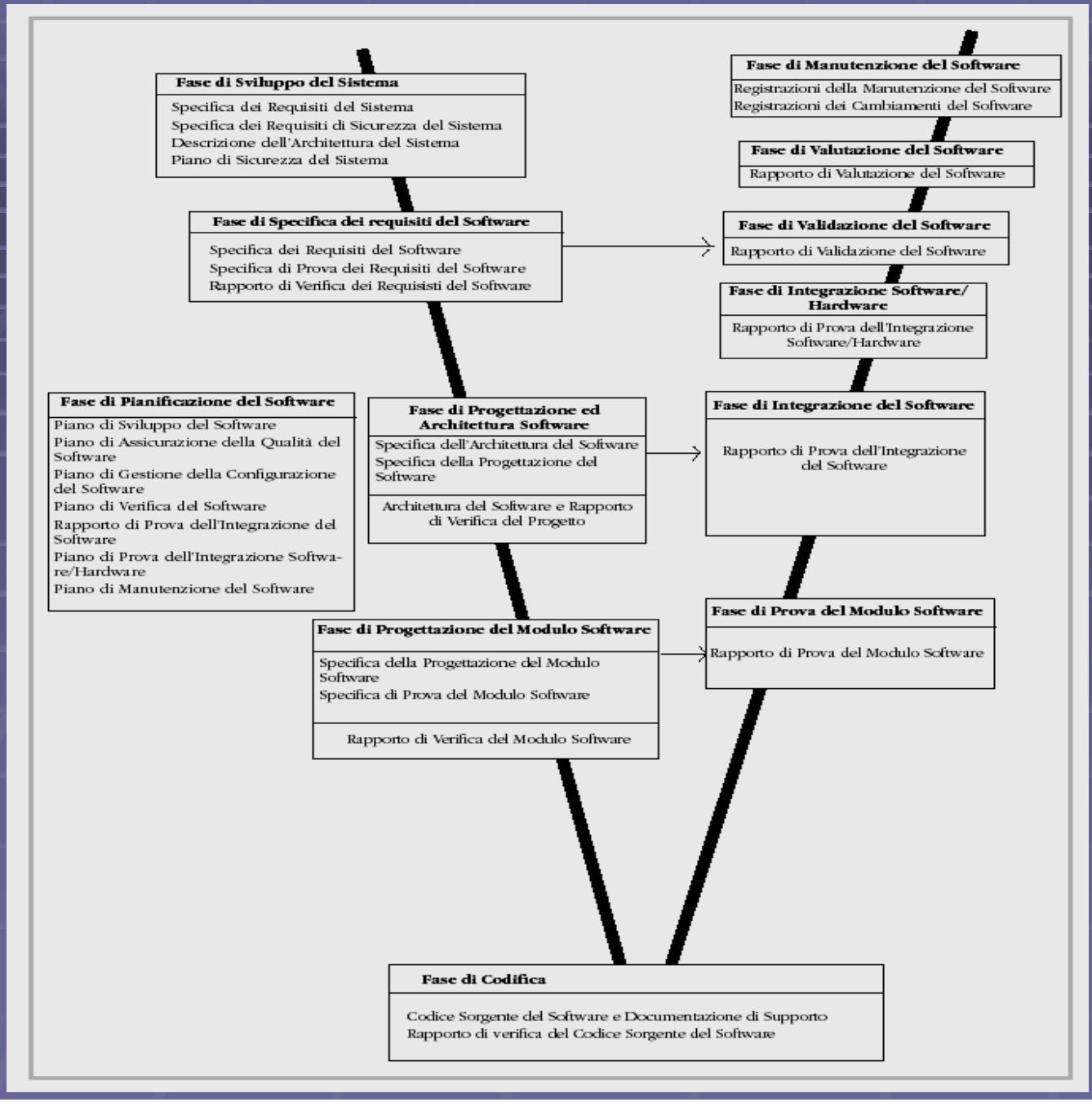
Pianificazione

- La Pianificazione deve
  - Coprire la fase di *Design* (progettazione)
  - Coprire la fase di Verifica e Validazione
  - Coprire gli aspetti RAM
  - Essere concordata con l'autorità regolatrice del dominio

Pianificazione di aspetti RAM

- Occorre descrivere
  - Politiche e strategie per il raggiungimento dei obiettivi RAM
  - Il sistema adottato per l'analisi dei rapporti di guasto e le relative azioni correttive (FRACA[s])
    - *Failure reporting analysis and corrective action(s)*
  - Le relazioni con altri programmi e piani collegati
  - Ruoli, responsabilità e competenza del personale coinvolto
  - Modalità di gestione degli aspetti RAM da parte dei sottofornitori

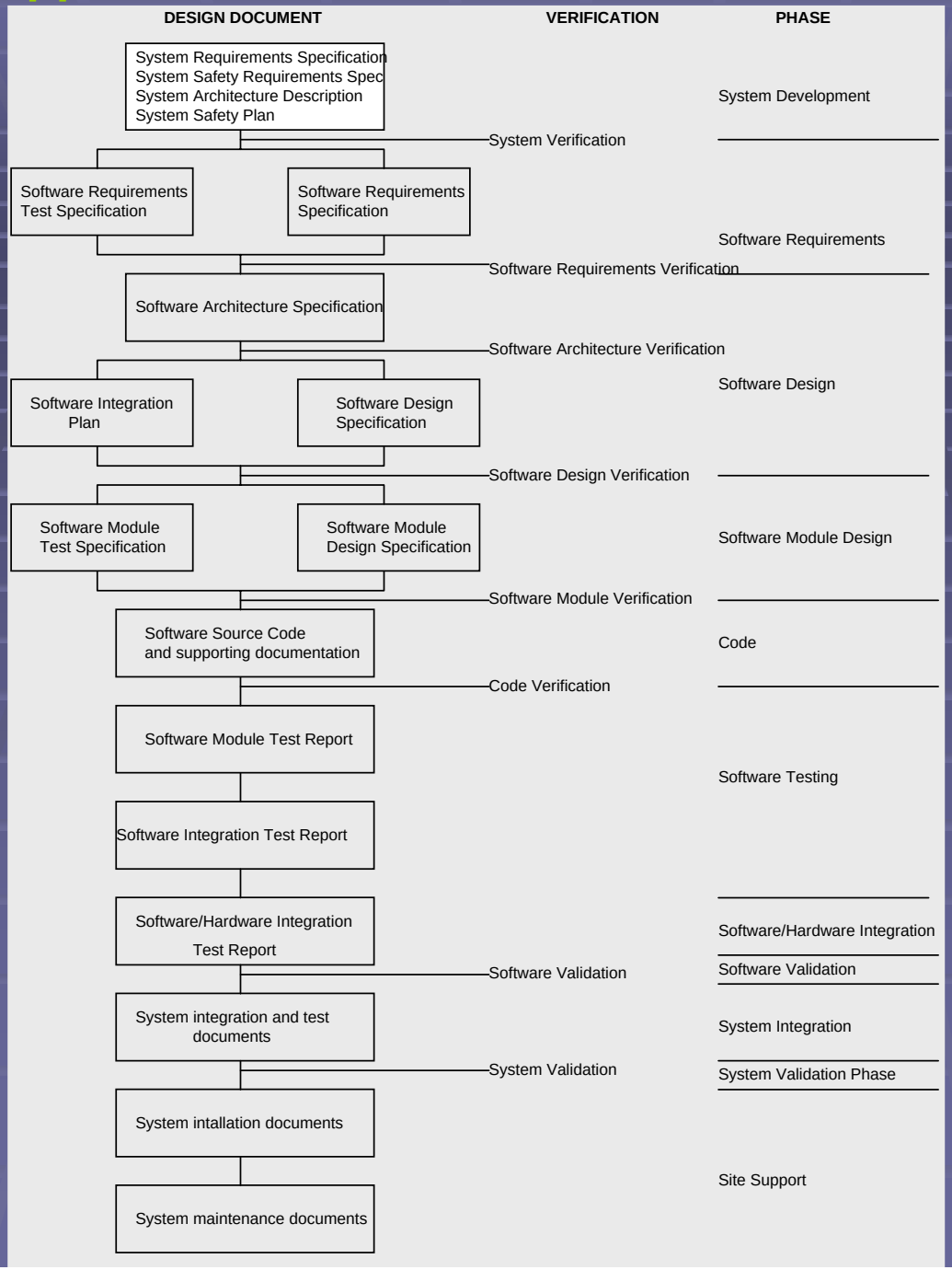
Fase 6: Sviluppo – Ciclo di vita *Software*



Attività / fasi di sviluppo SW secondo EN50128

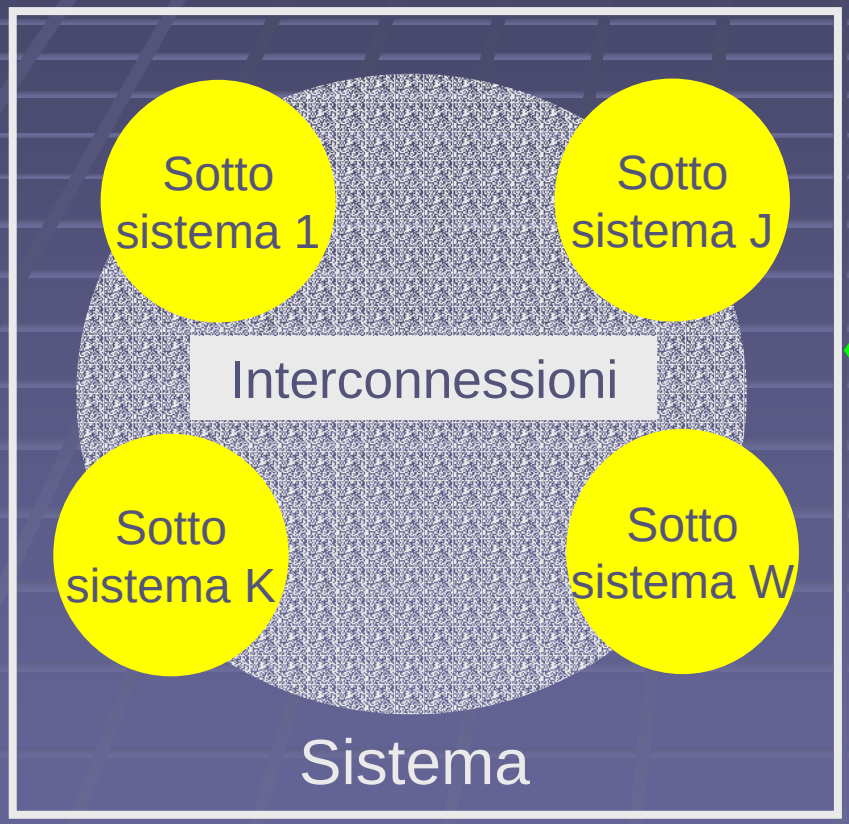
Fase 6: Sviluppo – Ciclo di vita *Software*

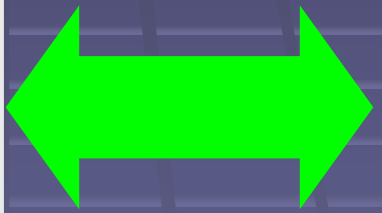
Ing. C. Iapicca



Documenti / fasi di sviluppo SW secondo EN50128

Validazione di sistema





Requisiti

La validazione di sistema implica *test* aggiuntivi rispetto a quelli già eseguiti su ogni sottosistema!

Validazione di sistema

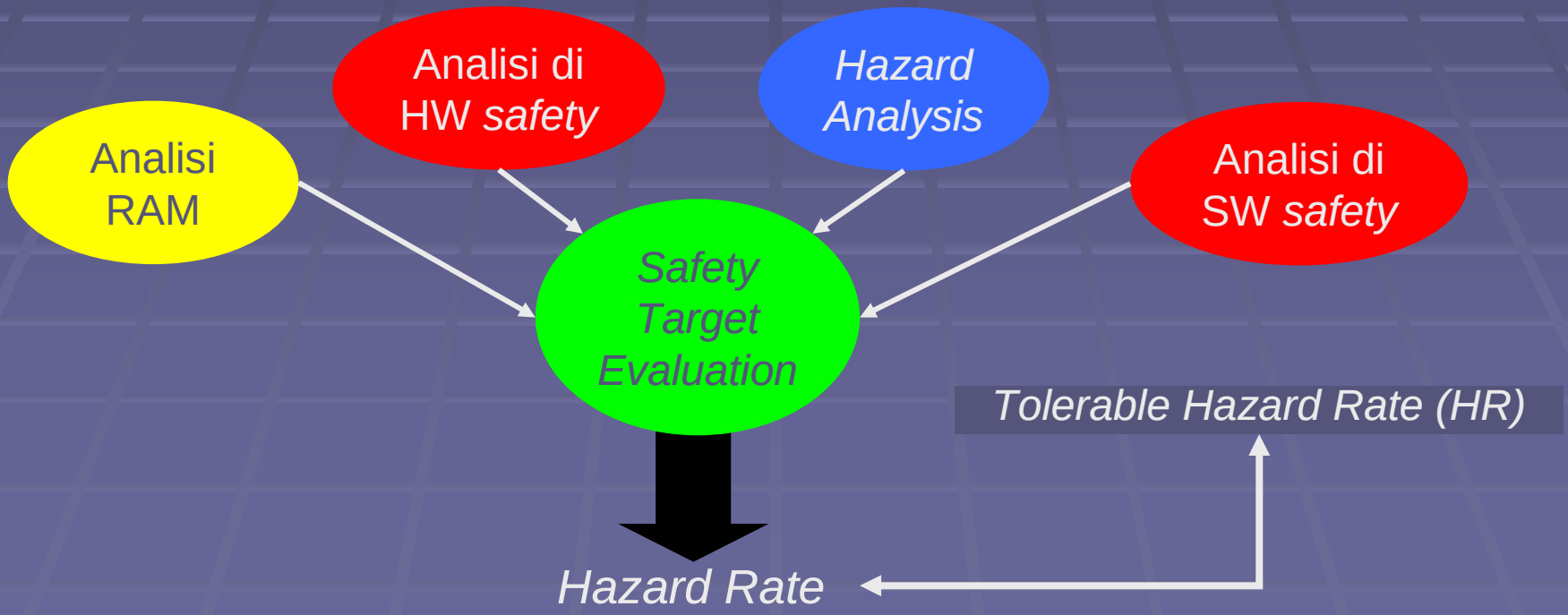
- Sancisce la chiusura positiva di tutte le attività di verifica
  - Contenuti
    - Descrizione del processo applicato e degli strumenti utilizzati
    - Risultati per tutti i criteri di accettazione
    - Limitazioni o restrizioni applicabili al sistema
  - Elementi di uscita
    - Rapporto di validazione del sistema
    - Piano di immissione in servizio
    - *Safety Case*

Test di Validazione

- *Test* aggiuntivi scritti dal Validatore
  - *Testing* del sistema da un punto di vista indipendente
  - Confluisce nel Rapporto di Validazione
- Tipologie di *test* utilizzabili
  - Dedicati ai requisiti funzionali
  - Dedicati ai requisiti di sicurezza
  - Prove di guasto singolo e multiplo
  - Sul comportamento temporale delle funzioni “time-critical”
  - Prove di stress funzionale
  - Prove di simulazione dell’ambiente operativo

Safety Target Evaluation

- Dimostrazione quantitativa del **rischio residuo** associato al sistema
  - Necessario alla redazione del Safety Case



Piano di immissione in servizio

- Deve prevedere
  - Attività per l'immissione in servizio
  - Modalità di gestione dei rapporti di segnalazione dei guasti
  - Descrizione di eventuali limitazioni al servizio del sistema
- Il piano **guida** la preparazione della fase di installazione
  - Piano di installazione
  - Procedure di installazione
    - Specifica dei collaudi
  - Rapporto di installazione
  - Aggiornamento del piano di *safety*

Validazione del sistema

- Condotta con il cliente dopo il completamento della fase di installazione
- Viene effettuata “sul campo”
- Una volta completata con successo (**accettazione del sistema**) dà il via **all’immissione in servizio**

Monitoraggio delle prestazioni

- Comporta raccolta, classificazione, analisi dei dati di osservazione sul campo
  - Enfasi sulle deviazioni comportamentali e prestazionali
  - Alimenta il FRACAS
- Consente aggiornamento delle analisi e del progetto