zetalab

ENGINEERING THE NEW ERA

Analisi dei Rischi Software
Metodologia e normative di riferimento
Cosenza, 7 Aprile 2015

Chi Siamo

Z Lab è stata fondata nel 2006 ed opera con successo nei seguenti settori:

- **Analisi RAMS**
- **Manuali Tecnici**
- **Analisi FEM & CFD**
- **Acustica (**Ambientale, Architettonica, Laboratorio ed Industriale**)**

Sedi Z Lab


zetalab ITALIA
zetalab BRASIL
VERONA (Lab)
FIRENZE
LECCE
COSENZA
ITAJUBÁ

Certificazioni Z Lab

GLOBE
CERTIFICAZIONI
N. 1845
UNI EN ISO 9001:2008

Principali Business Area Z Lab

Elementi dell'Analisi di Rischio

bene (o asset) ciò che bisogna salvaguardare (persone, oggetti, software, informazioni, ecc.)

vulnerabilità caratteristiche dei sistemi e dei processi che, in particolari condizioni, possono comportare la perdita di riservatezza, integrità o disponibilità delle informazioni

minacce possibili eventi non desiderati che portano alla perdita di riservatezza, integrità o disponibilità delle informazioni

Il Rischio

Il rischio è la probabilità che una minaccia nei confronti di un bene si attui sfruttando una vulnerabilità del sistema

Analisi di Rischio del Software

RISCHIO = potenziale difetto il cui verificarsi comporta dei danni

Danno

- Non raggiungimento di uno o più obiettivi (benefici attesi)
- Fallimento totale del progetto

I metodi di analisi del rischio

Quantitativi

- valore dei beni in termini economici
- analisi in base ad algoritmi matematici
- scelte secondo criteri oggettivi

Qualitativi

- valore dei beni in termini relativi (alto, medio, basso)
- analisi in base a tabelle
- scelte secondo criteri qualitativi

Esempio di analisi quantitativa

Bene: autovettura, valore € 20.000
Vulnerabilità: trasportabilità
Minaccia: furto

	Senza antifurto	Con bloccapedali	Con antifurto satellitare
Statistica furti annui per 100.000 vetture	1000	200	2
Probabilità furto (rischio)	0,01	0,002	0,00002
Esposizione economica al rischio	€ 200	€ 40	€ 0,4
Costo annuo della protezione	-	€ 12	€ 300

Limiti dell'Analisi Quantitativa

- Difficoltà nel monetizzare il valore dei beni
- Necessità di statistiche
- Difficilmente applicabile ad eventi con probabilità molto bassa

Esempio di analisi qualitativa

Bene: documenti amministrativi (memorizzati su server NT)
Vulnerabilità: accesso al sistema NT
Minaccia: acquisizione non autorizzata dei diritti di amministratore

Classe di criticità del bene → *media*
Probabilità di subire danni imputabili ad attacco → *bassa*

↓

Livello di rischio → medio

Funzioni di sicurezza per livello di rischio medio

- Consentire accesso come amministratori solo localmente
- Aggiornamento trimestrale dei Service pack
- Traccia degli utenti che hanno modificato il registro

Analisi di Rischio del Software

- Analisi sistematica e completa di tutti i possibili rischi che possono far fallire od intralciare la realizzazione del sistema in una qualsiasi fase del processo di sviluppo.

Ogni rischio presenta due caratteristiche:

- **Probabilità che avvenga**
  non esistono rischi con una probabilità del 100% (sarebbero vincoli al progetto)
- **Costo**
  se il rischio si realizza, ne seguono effetti indesiderati e/o perdite

Analisi di Rischio del Software

- **Rischi relativi ai requisiti**
  I requisiti sono perfettamente noti?
  Il rischio maggiore è quello di costruire un sistema che non soddisfa le esigenze del cliente.

- **Rischi relativi alle risorse umane**
  è possibile contare sulle persone e sull'esperienza necessarie per lo sviluppo del progetto?

Analisi di Rischio del Software

- **Rischi tecnologici**
  si sta scegliendo la tecnologia corretta?
  si è in grado di aggregare correttamente i vari componenti del progetto (ad es., GUI, DB, …)?
  quali saranno i possibili futuri sviluppi della tecnologia?

- **Rischi politici**
  ci sono delle forze politiche (anche in senso lato) in grado di intralciare lo sviluppo del progetto?

Analisi di Rischio del Software

- **Strategia reattiva o “alla Indiana Jones”**
  “Niente paura, troverò una soluzione”

- **Strategia preventiva**
  Si mette in moto molto prima che inizi il lavoro tecnico
  Si individuano i rischi potenziali, se ne valutano le probabilità e gli effetti e si stabilisce un ordine di importanza
  Si predispone un piano che permetta di reagire in modo controllato ed efficace
  Più grande è un rischio, maggiore sarà l’attenzione che bisognerà dedicargli

La Gestione del Rischio

Per ogni rischio occorre:

- valutare se sia opportuno ridurre il rischio ed in caso affermativo valutare in che misura scegliere le modalità con cui ridurre il rischio
- predisporre le misure con cui fronteggiare situazioni in cui il rischio si concretizza in un attacco
- predisporre le procedure per il recupero dei beni in situazioni in cui il rischio si concretizza in un evento negativo

L’analisi del rischio di un sistema complesso

- Il numero dei beni è dell’ordine di decine di migliaia (elaboratori, programmi e dati)
- Il numero dei rischi è in teoria dello stesso ordine di grandezza, con opportune semplificazioni, il numero può diventare dell’ordine di centinaia
- Le possibili soluzioni per ridurre i rischi sono decine (protezioni hardware, soluzioni organizzative, contromisure software che a loro volta possono avvalersi delle funzioni native dei sistemi ecc.)
- Il numero dei possibili eventi dannosi (o attacchi) è di difficile determinazione, quelli attualmente più diffusi sono migliaia

La constatazione dei rischi (risk analysis e gap analysis)

Processi di risk analysis

- Adatti a sistemi nuovi ed esistenti
- I rischi sono valutati esaminando beni, vulnerabilità e minacce
- Sono svolti con il supporto di tool specifici
- Popolano una base informativa utile per la fase di gestione

Processi di gap analysis

- Idonei per sistemi esistenti
- I rischi sono valutati sulla base di
  - analogie
  - buona prassi
  - esperienza
- Utilizzano principalmente check-list
- Producono rapporti sul livello di sicurezza e sulle criticità

Vocabolario della Gestione del Rischio

Gestione dei rischi (*risk management*)

Valutazione dei rischi (*risk assessment*)

Analisi dei rischi (*risk analysis*)

Stima di impatto (*risk evaluation*)

Trattamento dei rischi (*risk treatment*)

Accoglimento dei rischi (*risk acceptance*)

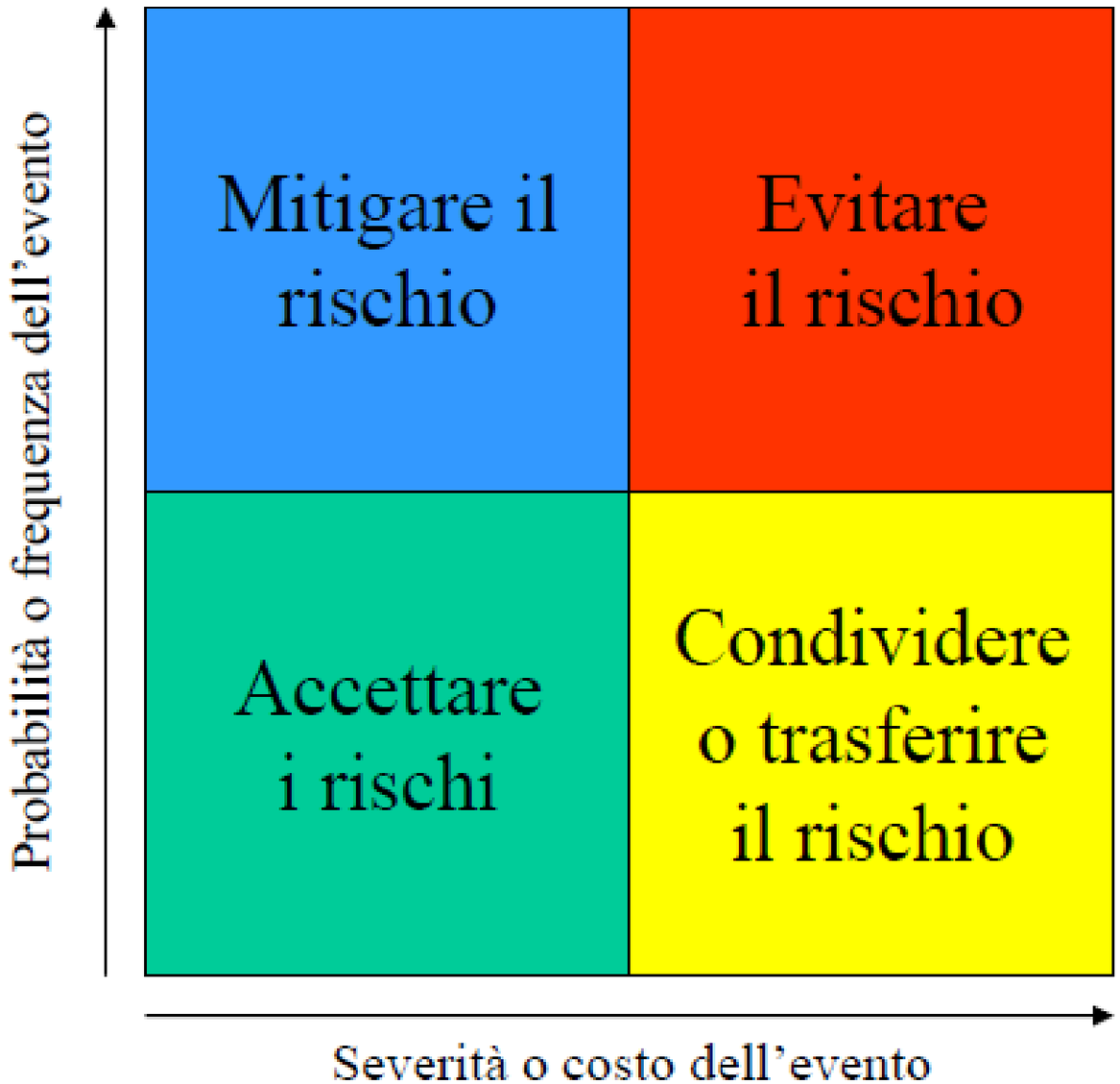
Comunicazione relativa ai rischi (*risk communication*)

Il trattamento dei rischi

Per ogni rischio individuato bisogna decidere se:

- rifiutarlo (*risk avoidance*) evitando il coinvolgimento nella situazione a rischio (ad esempio rinunciando ad un progetto)
- mitigarlo (*risk optimization*) con opportune contromisure
- trasferirlo (*risk transfer*) completamente od in parte a terzi (ad esempio con contratti assicurativi),
- accettarlo (*risk retention*)

La logica di trattamento dei rischi



La pianificazione della sicurezza

- L'attività di analisi del rischio produce generalmente risultati
  - condivisi
  - indicativi (il livello di dettaglio è funzione del metodo seguito)
  - dipendenti dal contesto
- Necessita di revisioni cicliche

- E' opportuno che abbia un costo ed una durata commisurati a costo e durata dell'intero processo

Il fattore Umano

- Importanza del fattore umano:
  - esperienza di chi conduce l'attività, determinante per il buon esito dello stesso,
  - atteggiamento collaborativo di chi deve cooperare all'interno della amministrazione (utenti e personale IT).
- Occorre conoscere a fondo il settore, i processi di business e il portafoglio delle applicazioni tipiche delle organizzazioni che vi operano.

Il fattore Umano

- Di particolare importanza è l'esperienza specifica riferita al preciso settore economico al quale appartiene l'organizzazione in esame. E' infatti completamente diverso effettuare una valutazione o verifica del sistema informativo in una azienda industriale, in una banca o in un istituto previdenziale

Le metodologie

- Mitigano la soggettività dell'intervento umano
- Facilitano il trasferimento delle competenze
- Consentono di vendere *know how* indipendente dalle competenze individuali
- Facilitano la standardizzazione dei processi

Metodologie e strumenti

- Tutte le metodologie sono oggi supportate da strumenti informatici
- Lo strumento può:
  - Rendere automatiche alcune fasi del processo (ad es. acquisizione dati)
  - Velocizzare le fasi che richiedono la gestione di notevoli quantità di informazioni
  - Aiutare a prendere decisioni (sistema esperto o DB della conoscenza)

Metodologie dell'Analisi di Rischio

- Pianificazione
  - Analisi
  - progettazione
  - realizzazione

- Verifica (assessment)
- Miglior. continuo

Valutazione dei rischi
(risk assessment
risk analysis
risk evaluation
risk treatment)

Verifica della sicurezza
(security auditing)

Gestione del rischio

Le fasi dell'Analisi di Rischio

- Rilevazione dello scenario (delimitazione del campo d'indagine, censimento dei beni)
- Modellizzazione (accorpamento, normalizzazione, condivisione del modello)
- Classificazione dei beni (categorizzazione, individuazione del valore economico o qualitativo, raggruppamento in classi)

Le fasi dell'Analisi di Rischio

- Valutazione di vulnerabilità e minacce (identificazione del livello di esposizione a minacce o attacchi)
- Calcolo del rischio (valutazione del livello di rischio intrinseco)
- Trattamento del rischio (scelta del trattamento ed individuazione delle contromisure)
- Reportistica

Modelizzazione

- Consente di rappresentare in forma schematica le informazioni raccolte nella fase di rilevazione dello scenario
- Il modello relaziona gli elenenti dell'indagine: dati, beni fisici, software, utenti, logistica, ecc.
- Il modello deve essere condiviso dai responsabili delle entità rappresentate

Classificazione dei Beni

- L'efficacia del metodo dipende dalla cura con cui viene svolta questa fase
- La classificazione aiuta i gestori della sicurezza a ponderare le scelte che dovranno essere prese durante il trattamento del rischio
- La semplicità della classificazione è fondamentale per l'utilizzabilità dei risultati
- La classificazione può avvenire per: criticità del dato, valore economico, impatti, ecc.

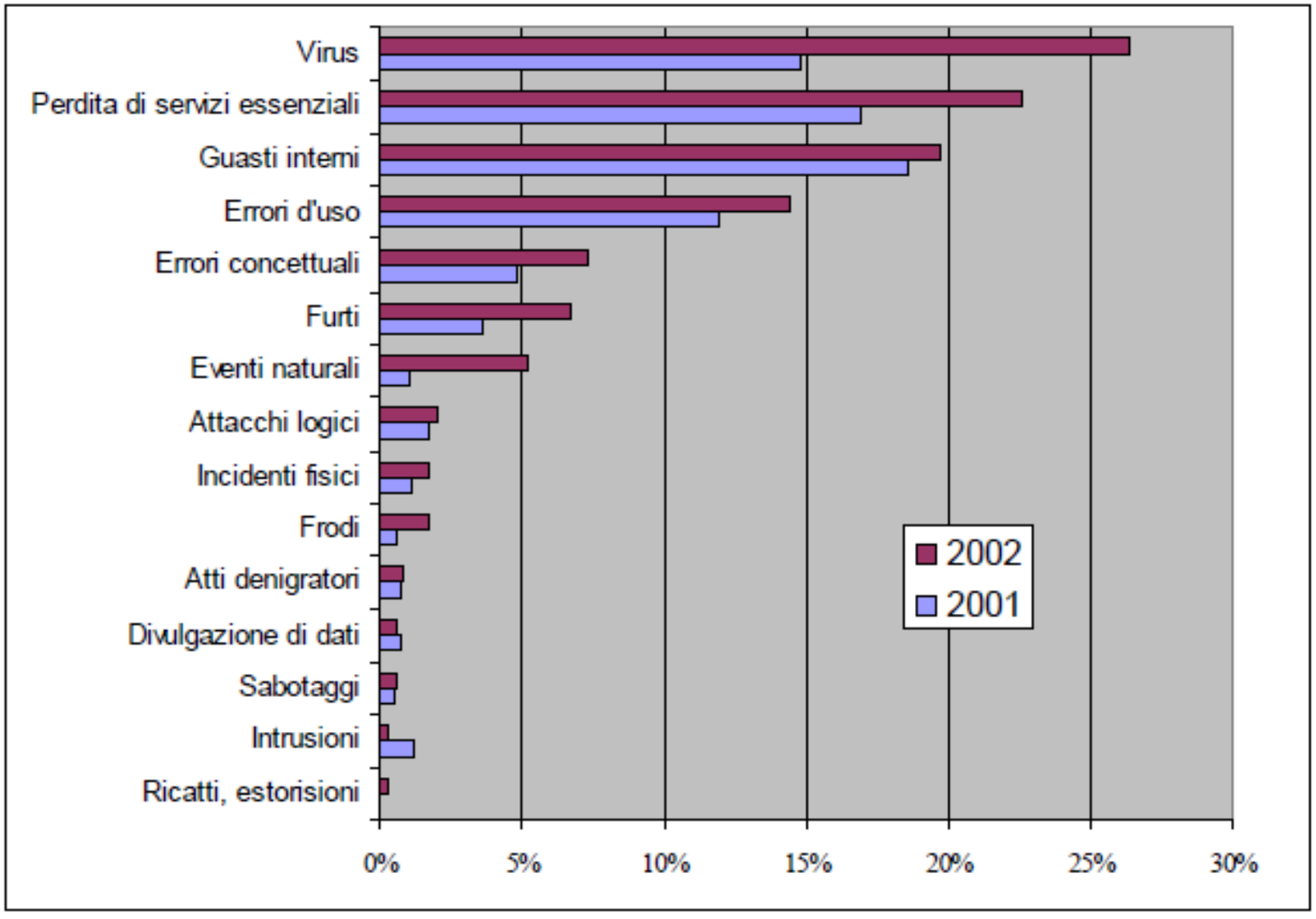
Valutazione di Vulnerabilità e Minacce

- Riporta le vulnerabilità delle entità censite o di loro aggregazioni
- Stima, per ogni entità o aggregazione di entità, la probabilità di subire un attacco o che si manifestino specifiche minacce
- La stima delle vulnerabilità può essere fatta in base a conoscenze pregresse, quella delle minacce con il ricorso a questionari

Calcolo del Rischio

- Consiste nel valutare il rischio che insiste sui beni in base agli elementi che sono stati individuati nelle precedenti attività
- Può essere fatto con l'ausilio di formule (metodi quntitativi) o di tabelle (metodi qualitativi)

Gli osservatori sulla criminalità informatica



Fonte Clusif – étude et statistiques sur la sinistralité informatique en France 2002

Minacce: comportamenti degli operatori

- sottrazione di credenziali di autenticazione
- carenza di consapevolezza, disattenzione o incuria
- comportamenti sleali o fraudolenti
- errore materiale

Minacce: eventi relativi agli strumenti

- azione di virus informatici o di programmi suscettibili di recare danno
- spamming o tecniche di sabotaggio
- malfunzionamento, indisponibilità o degrado degli strumenti
- accessi esterni non autorizzati
- intercettazione di informazioni in rete

Minacce: eventi relativi al contesto fisico/ambientale

- ingressi non autorizzati a locali/aree ad accesso ristretto
- sottrazione di strumenti contenenti dati
- eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi, accidentali o dovuti ad incuria
- guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.)
- errori umani nella gestione della sicurezza fisica

Categorie di Rischio di un Progetto di Sviluppo Software

- Componenti sviluppate da terze parti
- Componenti esterne
- Personale non qualificato per l’attività in oggetto
- Borchie dorate (Gold planting)
- Definizione errata delle funzionalità del sw
- Interfacce utente sbagliate
- Limiti tecnologici
- Instabilità dei requisiti
- Piani non realistici

Categoria di Rischio: Componenti sviluppate da terze parti

Fonti di Rischio:

- assicurazioni ottimistiche del committente circa rapidi riesami ed approvazioni dei piani e delle specifiche dei produttori;
- attività di terzi posizionate su percorsi critici dei piani, riesami legali, approvazioni procedurali e consensi per la sicurezza;
- personalizzazioni di prodotti da parte dei venditori;
- rapporto tra le prestazioni stimate dai sub-fornitori e quelle effettivamente messe in atto.

Tecniche di Controllo:

- eventuali esami per l'assegnazione di premi o l'applicazione di penali;
- contratti con aliquote di premi/penali;
- lista dei controlli da effettuarsi sul processo di sviluppo del sub-fornitore;
- previsione competitiva o prototipizzazione;
- controllo del gruppo di sviluppo del sub-fornitore.

Categoria di Rischio: Componenti esterne

Fonti di Rischio:

- componenti fornite dal committente che potrebbero presentarsi carenti ed inadeguate alla nuova applicazione;
- strumenti di supporto ed ambienti di sviluppo che potrebbero essere incompatibili o con prestazioni scarse;
- componenti commerciali che possono apparire grandi dalle pubblicazioni commerciali, ma possono risultare, nei fatti, immature e/o supportate inadeguatamente.

Tecniche di Controllo:

- raffronti tra pacchetti concorrenti;
- ispezioni;
- liste dei controlli da effettuare sui prodotti;
- analisi di compatibilità;
- analisi di conformità.

Categoria di Rischio: Personale non qualificato per l'attività in oggetto

Fonti di Rischio:

- bisogno di capacità critiche specifiche per il progetto;
- assunzioni non realistiche circa la disponibilità di persone chiave;
- alcune particolari incompatibilità fra il personale candidato al progetto.

Tecniche di Controllo:

- professionisti ad alta specializzazione;
- mappe delle assegnazioni di responsabilità;
- costruzione dello spirito di gruppo;
- consenso del personale chiave;
- addestramento;
- preschedulazione delle persone chiave.

Categoria di Rischio: Borchie dorate (Gold planting)

Fonti di Rischio:

Molti progetti assumono un rischio non necessario nel momento in cui vengono sviluppate funzionalità molto sofisticate ma, al tempo stesso, marginalmente utili ai prodotti software. Una delle cause più frequenti che porta al verificarsi delle borchie d'oro potrebbe essere la ricerca continua, da parte del fornitore, dell'affermazione del prodotto sul mercato, il che porta, molto spesso, alla realizzazione di progetti ingiustificatamente ambiziosi.

Tecniche di Controllo:

- uno sfoltimento dei requisiti;
- la prototipizzazione;
- l'analisi costo-beneficio;
- la previsione del costo.

Categoria di Rischio: Definizione errata delle funzionalità del sw

Fonti di Rischio:

Nella produzione di pacchetti software, frequentemente, si passa alla fase di progettazione e sviluppo degli stessi con l'assunzione che siano stati pienamente compresi i requisiti richiesti dell'utente.

Per questo motivo sono stati scartati, in toto o parzialmente, molti prodotti perché appunto basati su requisiti utente erroneamente definiti o compresi in maniera errata.

Tecniche di Controllo:

- analisi dell'organizzazione;
- formulazione dei concetti operativi;
- opinioni dell'utente;
- prototipizzazione;
- versioni preliminari dei manuali utente.

Categoria di Rischio: Interfacce utente sbagliate

Fonti di Rischio:

Molti prodotti software, invece, possono risultare adeguati alle funzioni richieste, ma hanno una interfaccia utente non del tutto soddisfacente a tali richieste.
Questo rischio è diventato sempre più importante man mano che i prodotti software hanno enfatizzato la interazione con l'utente.

Tecniche di Controllo:

- la prototipizzazione;
- l'analisi delle procedure di lavoro;
- la caratterizzazione dell'utente (funzionalità, stile, carico di lavoro).

Categoria di Rischio: Limiti tecnologici

Fonti di Rischio:

Molti progetti sono a rischio perché utilizzano tecnologie non consolidate ed affidabili. Le più comuni sorgenti di questo tipo di rischio sono:

- incapacità dei sistemi operativi a gestire processi distribuiti ed a gestire dati distribuiti;
- pacchetti di Intelligenza Artificiale o Sistemi aperti. Allo stato attuale sono ancora inefficienti per essere utilizzati in funzioni di uso comune;
- bilanciamento tra la macchina e l'utilizzatore per specifiche applicazioni come il controllo dei processi;
- accuratezza e prestazioni degli algoritmi, soprattutto se complessi o applicati a grandi masse di dati;
- protezione della sicurezza dell'informazione. Molte volte la tecnologia disponibile non è efficace a creare barriere all'accesso non autorizzato degli hackers o degli invasori;
- alta accuratezza e tolleranza ai malfunzionamenti. La tecnologia attuale ha molte limitazioni rispetto alla accuratezza ed alla tolleranza.

Categoria di Rischio: Limiti tecnologici

Tecniche di Controllo:

- analisi tecniche;
- analisi costo-beneficio;
- prototipizzazione;
- liste di prova.

Categoria di Rischio: Instabilità dei requisiti

Fonti di Rischio:

Alcune richieste di cambiamento sono essenziali, ma molte sono solo manifestazioni collaterali scaturite dal fenomeno delle borchie dorate descritto in precedenza.
La maggior parte dei progetti sottostimano l'effetto di ripercussione che i cambiamenti dei requisiti hanno sul progetto, sul codice, sulle prove, sulla documentazione, sulla pianificazione ed il controllo del processo, sulla gestione della configurazione, sull'assegnazione del personale, sulla gestione della comunicazione tra gli addetti ai lavori, sul budget, sui tempi e sulla produttività.

Tecniche di Controllo:

- una soglia per determinare grandi cambiamenti;
- una information hiding (informazioni intrinseche), ovvero rendere altamente indipendenti le diverse parti di una applicazione in modo tale da ridurre le modifiche da apportare;
- uno sviluppo incrementale (cambiamenti differiti a successivi incrementi).

Categoria di Rischio: Piani non realistici

Fonti di Rischio:

I piani non realistici si verificano così spesso che potrebbero essere considerati un generico rischio di progettazione software.
La maggior parte delle cause che generano tale rischio sono specifiche per ogni progetto, pertanto è opportuno che si riservi particolare attenzione ad esse.

Tecniche di Controllo:

- costo multi-sorgente dettagliato;
- previsione del costo;
- sviluppo incrementale;
- riuso delle componenti software;
- semplificazione dei requisiti più complessi

Software RAMS

Ad oggi i sistemi informatici sono utilizzati in molteplici scenari critici sia dal punto di vista economico (business critical) sia in termini di affidabilità e di sicurezza (mission critical):

- Controllo remoto di veicoli senza conducente;
- Controllo del traffico ferroviario;
- Missioni aerospaziali;
- Sistemi ed apparecchiature medicali;
- Controllo ambienti ostili all'uomo (centrali nucleari);

Un sistema è una qualsiasi entità in grado di interagire con altre entità, utenti umani o altri sistemi. Esso è progettato per offrire un certo numero di servizi attraverso la propria interfaccia che, pertanto, delimita i confini del sistema stesso.

Un servizio, è un comportamento del sistema che l'utente può percepire; esso è definito corretto se è conforme alle proprie specifiche mentre in caso contrario si parlerà di fallimento.

L'interfaccia è il confine tra il sistema e l'utente. L'interfaccia su cui viene fornito il servizio è detta service interfacce. Nella figura seguente è rappresentata l'interazione tra sistema e utente.

Il crescente impiego dei sistemi informatici negli scenari fortemente critici, ha evidenziato la necessità di valutare molto attentamente le conseguenze che un loro malfunzionamento può avere sulle persone o sull'ambiente operativo.

Software Safety Engineering

La Software Safety Engineering nasce ufficialmente negli anni ’80 quando la NASA, il Dipartimento della Difesa degli Stati Uniti e le istituzioni equivalenti in molti altri paesi del mondo cominciano a fare pesante uso, nei propri sistemi, di computer e software che realizzano funzionalità di sempre maggiore criticità.

Storicamente, gli ingegneri del software avevano una visione limitata al particolare sotto-problema che gli competeva, e per questo motivo nei primi standard che si occuparono di safety (MIL-STD-882 e derivati) la responsabilità e le attività in merito a questo aspetto vennero assegnate alla fase di ingegnerizzazione di tutto il sistema. Solo in seguito (con il MIL-STD-498) agli ingegneri del software venne assegnato un ruolo definito e delle responsabilità ufficiali riguardo alla Software System Safety. Questo avvenne quando la complessità del software giunse a un punto tale da richiedere la loro competenza specifica per la valutazione e la gestione dei rischi associati al suo impiego.

La pianificazione delle attività è forse la fase più importante per il successo di tutto il programma di safety, di cui è inevitabilmente la prima fase. È importante capire quali siano i requisiti di safety alla base di tutto il progetto. La loro assenza o cattiva formulazione può comportare, quando il problema emerge, ritardi, aumenti di costo e risultati non ottimali.

La valutazione del rischio massimo tollerabile è un’altro dei fattori chiave per la pianificazione del processo. È necessario, partendo dall’analisi dei rischi del sistema, stabilire il livello di qualità del sistema in fatto di safety. Tuttavia è necessario capire dove mettere i confini dei vari livelli di rischio, ad esempio: minimo, serio, inaccettabile. Quest’ultima valutazione viene in genere fatta dal cliente e dai vari anelli intermedi che ci sono fino allo sviluppatore.

Standard Industriali per le SRAMS

Esistono molte direttive, regolamenti, standard e linee guida che stabiliscono i requisiti di safety per l'acquisizione, lo sviluppo e il mantenimento di sistemi elettronici che impiegano software. Ogni macro-settore industriale, come quello militare, aerospaziale o aeronautico, presenta una serie di questi criteri che catturano una visione specifica del problema. Ciascuna famiglia di queste normative è stata storicamente concepita da entità governative o agenzie diverse. Molti paesi hanno inoltre sviluppato una serie di regolamenti ad hoc che, ispirandosi a, o adottando altri standard dello stesso contesto, impostano delle norme legislative relative a quel particolare settore.

Esistono delle caratteristiche e dei criteri comuni a molti standard, che quindi costituiscono una forte base teorica e pratica per uno studio trasversale sulla Software Safety in generale.

IEEE - Serie IEEE

La IEEE ha pubblicato gli standard (IEEE-1228, 1994) per la pianificazione della safety nel software per fissare i requisiti minimi di safety che devono essere contenuti nel piano di sicurezza software. Questi standard contengono quattro parti che parlano di come applicare il processo facendo anche riferimento ad altri standard, definendo il contenuto obbligatorio del piano di safety che si riferisce al software. L'applicazione di questo standard è da intendere come interamente volontaria e il tutto è diretto a chi in qualche modo è incaricato di definire, pianificare, implementare o supportare il piano di safety

Standard Industriali per le SRAMS

EIA

L'EIA (Electronic Industries Association) ha pubblicato il "Safety Engineering Bulletin 6B, System Safety Engineering in Software Development", nel 1990. Lo standard e la commissione che lo hanno generato si focalizzano sulle procedure, le metodologie, e lo sviluppo di criteri per la gestione della safety nei sistemi, sottosistemi ed equipaggiamenti.

Lo scopo del documento è dare delle linee guida su come condurre l'analisi della safety sui sistemi controllati o monitorati da computer. Specifica le problematiche e le soluzioni associati a quest'attività, i processi da seguire, quali attività vanno fatte, e i metodi da impiegare (EIA, 1990).

MIL-STD-882B

Lo scopo di questo standard è stabilire uno SSP (System Safety Program) che riguardi gli aspetti di safety, compatibili con i requisiti delle specifiche missioni, dei sistemi, sottosistemi, apparecchiature, servizi e delle loro interfacce.(MIL-STD-882B, 1987)

Gli autori riconoscono e valutano i rischi presenti nei sistemi safety-critical.

Tale standard è stato utilizzato in molti programmi governativi statunitensi creati durante gli anni '80, fornendo linee guida e compiti specifici al team di sviluppo per ciò che riguarda il software, l'hardware, il sistema in generale e l'interfaccia uomo-macchina.

Standard Industriali per le SRAMS

MIL-STD-882D

I sistemi e i progetti realizzati all'interno del Dipartimento della Difesa degli Stati Uniti sviluppati attualmente sono soggetti a requisiti dettati da questo standard.

È richiesto agli sviluppatori del sistema di documentare le loro attività per soddisfare i requisiti imposti; di identificare i rischi all'interno del sistema attraverso un'analisi sistematica; di valutare la gravità dei rischi; identificare tecniche di contenimento dei rischi; ridurre la probabilità di rischi minori a livelli accettabili; verificare e validare la riduzione dei rischi minore; riportare i rischi residui al Project Manager (MIL-STD-882D, 1999).

RTCA-DO 178B

La FAA (Federal Aviation Administration) richiede questo standard per la certificazione del software da impiegare in un qualsiasi (sotto)sistema di un velivolo commerciale o di altra strumentazione aeroportuale.

La RTCA (RadioTechnical Commission for Aeronautics) punto di riferimento tecnico per l'industria aeronautica civile in tutto il mondo ha sviluppato questo standard per stabilire dei criteri per sviluppatori, installatori e utenti di software in dispositivi a microprocessore per l'avionica.

Il DO-178B è una linea guida per determinare, in modo consistente e con un ragionevole livello di certezza, che gli aspetti software di un velivolo o di un suo componente rispettano i requisiti FAA di aero-navigabilità.(DO-178B, 1992)

Standard Industriali per le SRAMS

NASA – Serie NSS

La NASA ha da sempre sviluppato sistemi safety-critical, tanto aerospaziali quanto aeronautici, per supportare la pianificazione delle attività che si riferiscono alla safety nei suoi vari dipartimenti, ha pubblicato questo standard con lo scopo di fissare dei requisiti per un approccio sistematico alla safety del software come parte integrale dell'SSP.

Lo standard descrive le attività necessarie per assicurarsi che la safety sia considerata nel software acquistato o sviluppato dalla NASA, e che sia supportata durante l'intero ciclo di vita del software. Il documento è stato creato secondo i principi di altri standard, quali il DOD-STD-2167A e il MIL-STD-882C.

Gli obiettivi definiti dallo standard (NSS-1740.13, 1994) sono:

Garantire che il sistema non si trovi direttamente o indirettamente in uno stato "pericoloso", che il sistema non possa non accorgersi di trovarsi in uno stato pericoloso e che prenda le opportune contromisure e infine che il sistema non fallisca nell'attenuare il danno in caso d'incidente.

EN 50128 – Applicazione Software Ferroviario

Questa norma si applica ai sistemi/prodotti elettronici programmabili per il segnalamento, e, in genere, a tutti i sistemi ferroviari di comando e protezione.

Essa riguarda requisiti di qualità, verifica e validazione che si richiedono per la garanzia di integrità della sicurezza delle funzioni realizzate per i sistemi di sicurezza in cui sono integrati.

Il SW deriva I propri requisiti SIL dal livello SIL definito per ciascuna funzione di sistema, a cui il SW fornisce parte dei servizi richiesti, dalla EN50129. Il SIL del SW di una funzione deve essere maggiore o uguale a quello richiesto per la funzione stessa.

La EN50128 definisce 5 livelli SIL (incluso il SIL0) mentre la EN50128 solo 4 (non incluso il SIL0). Le nuove norme in preparazione risolvono questa differenza, distinguendo fra SIL0 e «non-safety related».

Questa norma identifica tecniche e misure qualitative per I 5 livelli SIL, elencate nell'Allegato A che è da considerare obbligatorio.

EN 50128 – Applicazione Software Ferroviario

Questa norma si applica ai sistemi/prodotti elettronici programmabili per il segnalamento, e, in genere, a tutti i sistemi ferroviari di comando e protezione.

Essa riguarda requisiti di qualità, verifica e validazione che si richiedono per la garanzia di integrità della sicurezza delle funzioni realizzate per i sistemi di sicurezza in cui sono integrati.

Il SW deriva I propri requisiti SIL dal livello SIL definito per ciascuna funzione di sistema, a cui il SW fornisce parte dei servizi richiesti, dalla EN50129. Il SIL del SW di una funzione deve essere maggiore o uguale a quello richiesto per la funzione stessa.

La EN50128 definisce 5 livelli SIL (incluso il SIL0) mentre la EN50128 solo 4 (non incluso il SIL0). Le nuove norme in preparazione risolvono questa differenza, distinguendo fra SIL0 e «non-safety related».

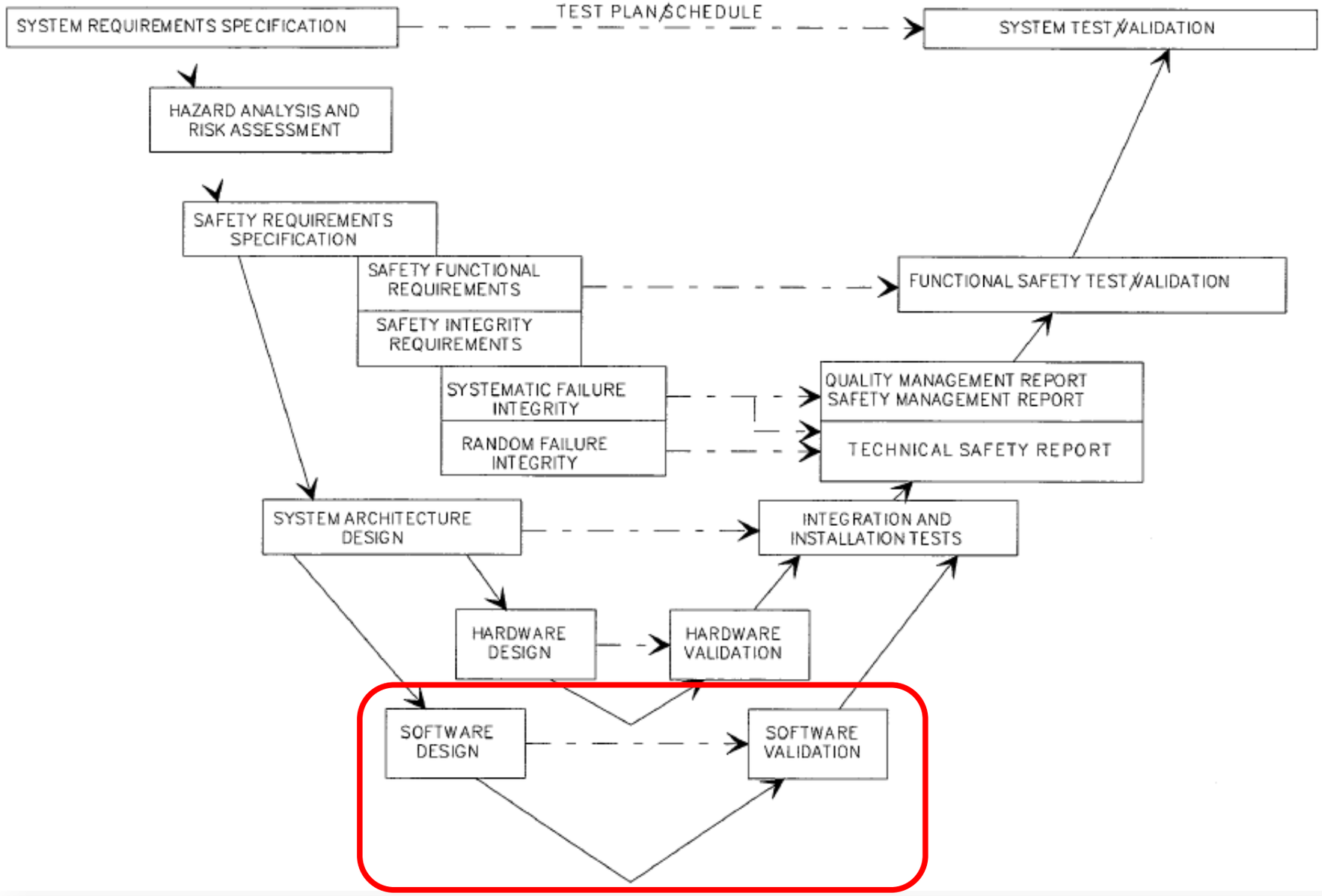
Questa norma identifica tecniche e misure qualitative per I 5 livelli SIL, elencate nell'Allegato A che è da considerare obbligatorio.

EN 50128 – Applicazione Software Ferroviario

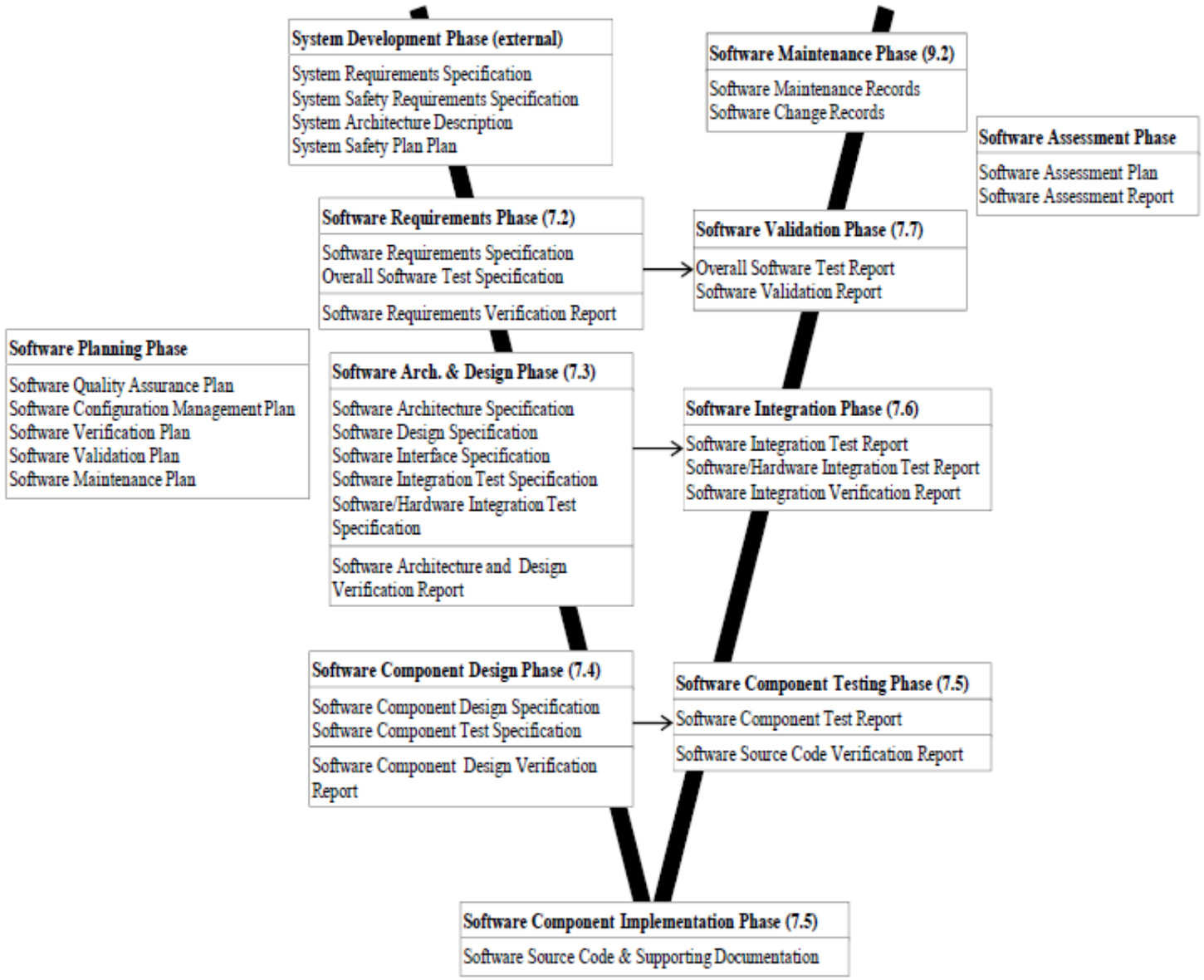
La norma si applica a:

- *Nuovi sistemi di comando e protezione;*
- *Modifiche sostanziali di sistemi di sicurezza esistenti;*
- *Componenti SW, commerciali o no, integrati in sistemi safety-related (es. SW di comunicazione fra unità o RTOS);*
- *Software generico per uso in applicazioni di sicurezza (es. Piattaforme di elaborazione generiche di sicurezza);*
- *Tool di supporto allo sviluppo di applicazioni SW ed alla configurazione su apparati target.*

EN 50128 – Ciclo di vita di un progetto



EN 50128 – Ciclo di vita e di documentazione del SW



EN 50128 – Fasi di Garanzia del SW

- Software testing
- Software verification
- Software validation
- Software assessment
- Software quality assurance
- Modification and change control
- Support tools and languages

EN 50128 – Test del Software

Obiettivi

Il test del SW é eseguito dal Tester e/o dall'Integratore. Deve accertare il corretto funzionamento, rispetto ai requisiti di progetto, e le prestazioni del SW nei suoi componenti e nel suo insieme. I rapporti delle prove si limitano a riportare i passi di prova eseguiti ed i risultati positivi o negativi ottenuti. Non esprime giudizi sugli stessi che sono lasciati al verificatore o al validatore.

Documenti di Input

Documenti di Sistema, di HW e SW come specificato nel Piano di V&V del SW.

Documenti di Output

1. Specifica di prova del SW totale e relativo Rapporto prove
2. Specifica di prova di integrazione HW/SW e relativo Rapporto prove
3. Specifica di prova di integrazione del SW e relativo Rapporto prove
4. Specifica di prova dei singoli Moduli SW e relativo Rapporto prove

EN 50128 – Verifiche del Software

Obiettivi

Giudicare, sulla base di esami e prove oggettive, che il processo di progettazione ed i risultati ottenuti in una data fase del ciclo di sviluppo soddisfa i requisiti e le attese previste con riguardo a completezza, correttezza e congruenza.

Documenti di Input

Piani di sviluppo e Piano di gestione della Qualità del SW e Output delle fasi precedenti

Documenti di Output

1) Piano di verifica del SW (contenente criteri, tecniche e tool da usare nel processo di verifica in considerazione delle Tabelle A.5, A.6, A.7 e A.8)

2) Rapporti di verifica del SW

3) Rapporto di verifica della Qualità del SW

EN 50128 – Validazione del Software

Obiettivi

Dimostrare, attraverso esame e test, che tutti i requisiti del SW, inclusi i requisiti SIL (di processo), siano stati specificati, realizzati e verificati con esito positivo e valutare la criticità o meno, nei confronti del sistema totale, di tutte le anomalie e non-conformità trovate sia in fase di prova che di verifica e dalle attività stesse della validazione.

Documenti di Input

Tutti i documenti di sistema, i piani di sviluppo e di gestione Q&S, le specifiche dei requisiti, i documenti di progetto, i rapporti di prova e di verifica.

Documenti Output

1. Piano di validazione del SW - con definizione delle misure e tecniche di test (fra quelle di sopra) e di esame documentale previste per il livello SIL d'interesse, con particolare riguardo delle prove di sistema, alle prove del SW totale, dell'integrazione HW/SW e dei moduli nonché dei relativi ambienti di prova)
2. Rapporto di Validazione del SW
3. Rapporto di verifica della validazione del SW (Piano e Rapporto di Validazione) in termini di chiarezza, tracciabilità, completezza e coerenza.

EN 50128 – Garanzia della Qualità del Software

Obiettivi

Identificare, monitorare e controllare tutte le attività, sia tecniche che gestionali, necessarie per garantire uno sviluppo del SW in regime di controllo della qualità.

Documenti di Input

Tutti i documenti del PDD

Documenti di Output

1) Piano di Qualità del SW
2) Piano di gestione delle Configurazioni del SW (se non incluso a livello di sistema)
3) Rapporti di audit di qualità
4) Rapporto sulla verifica della garanzia della qualità del SW

EN 50128 – Assessment del Software

Obiettivi

Valutare se il processo di sviluppo e di V&V del SW (in tutto il ciclo di vita) ha definito requisiti adeguati al livello SIL richiesto, li ha rispettati e ne sono state fornite evidenze adeguate, nonché esprimere un giudizio finale di adeguatezza sui risultati globali ottenuti e valutare la fattibilità delle eventuali mitigazioni proposte per risolvere possibili difformità.

L'assessor deve avere accesso a tutta la documentazione di specifica, di progetto, di V&V, di gestione della configurazione, la gestione di Q&S (incluso organizzazione, competenze e training (v. Allegato B).

Per SW SIL 0, si valutano I requisiti generici di qualità che si possono tralasciare se l'azienda è certificata secondo la EN ISO 9001/9003 per attività legate al SW.

Documenti d'ingresso

1. Specifica dei requisiti di sistema
2. Specifica dei requisiti del SW
3. Rapporto di Validazione
4. Rapporti di verifica
5. Rapporti di test.

Documenti di ouptut

1. Piano di assessment del SW
2. Rapporto di assessment del SW
3. Rapporto di verifica dell'assessment del SW

EN 50128 – Controllo e gestione delle Modifiche

Obiettivo

Garantire che il SW realizzi le nuove funzioni richieste, dopo la realizzazione di una data modifica, nella non intrusività sulle funzioni non affette dalle modifiche, nel rispetto delle prestazioni previste e che preservi o migliori le caratteristiche SIL e di disponibilità pre-esistenti.

Documenti di Input

1. Piano di qualità del SW
2. Piano di gestione della configurazione del SW
3. Documentazione di progetto del SW
4. Richiesta di modifica
5. Analisi di impatto della modifica ed autorizzazioni

Documenti di Output

1. Tutti i documenti modificati
2. Registrazioni delle modifiche al SW
3. Tutti i dati caratteristici della nuova configurazione

EN 50128 – Tool di supporto allo sviluppo e alla verifica del SW

Obiettivi

Fornire l'evidenza che possibili guasti dei tool non inficiano negativamente il sistema di tool in modo non rilevabile da misure tecniche o organizzative messe in atto a garanzia del loro uso sicuro. Metodologie suggerite:

1. Valutazione esplicita dei rischi e misure mitigative corrispondenti (se il progetto del tool è disponibile)
2. Adeguata combinazione di storie di uso positivo in ambienti e in applicazioni simili ("proven in use")
3. Verifiche degli output mediante comparazione con output prodotti da altri tool equivalenti ma dibversi o mediante esame degli output creati dal tool a partire da SW appositamente creati per il test dello stesso tool.

Documenti di Input

Specifiche o manuali d'uso dei Tools.

Documenti di Output

Rapporto di validazione dei Tool tipo T3

Thank you for your attention!

zetalab

ENGINEERING THE NEW ERA