L’impatto del Safety Integrity Level (SIL) nei sistemi di supervisione e controllo per le infrastrutture critiche

IEC 61508 : 2010

Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC/EN 61508 & SIL

I sistemi relativi alla sicurezza fisica in conformità con il IEC 61805

Lo standard internazionale IEC/EN 61508 è ampiamente accettato come base per la realizzazione delle specifiche, la progettazione e in generale l'operatività di un Sistema Strumentale Sicuro - Safety Instrumented System (SIS).

Come standard di base IEC/EN 61508 utilizza una formulazione basata sulla valutazione del rischio (risk assessment):

Una volta realizzata tale valutazione del rischio e attraverso una procedura per la sua riduzione/mitigazione si determina il necessario SIL Safety Integrity Level (SIL) per quei componenti e sistemi con funzioni che impattano con la sicurezza fisica delle persone e dell'ambiente.

Come chiaramente indicato la valutazione viene effettuata sulla funzionalità di un sistema e quindi non è unicamente orientata alla sola probabilità di rottura di un dispositivo (es. un dispositivo elettronico può essere perfettamente attivo ma rispondere "funzionalmente" in modo errato ad una sollecitazione esterna).

La valutazione SIL dei componenti e dei sistemi si intende quindi orientata a ridurre i rischio associato ad un sistema o ad un dispositivo sino ad un livello di "rischio tollerabile".

Elementi di Analisi del Pericolo e del Rischio secondo IEC/EN 61508

Category	Definition	Range (failures per year)
Frequent	Many times in system lifetime	> 10−3
Probable	Several times in system lifetime	10−3 to 10−4
Occasional	Once in system lifetime	10−4 to 10−5
Remote	Unlikely in system lifetime	10−5 to 10−6
Improbable	Very unlikely to occur	10−6 to 10−7
Incredible	Cannot believe that it could occur	< 10−7

Category	Definition
Catastrophic	Multiple loss of life
Critical	Loss of a single life
Marginal	Major injuries to one or more persons
Negligible	Negligible

	Consequence			
Likelihood	**Catastrophic**	**Critical**	**Marginal**	**Negligible**
Frequent	1	1	1	2
Probable	1	1	2	3
Occasional	1	2	3	3
Remote	2	3	3	4
Improbable	3	3	4	4
Incredible	4	4	4	4

- **Classe 1**: Inaccettabile in ogni circostanza;
- **Classe 2:** Indesiderabile: tollerabile solo se la riduzione del rischio è impraticabile o se i costi sono molto sproporzionati in relazione ai possibili miglioramenti ottenibili;
- **Classe 3**: Tollerabile se il costo della riduzione del rischio può superare i possibili miglioramenti;
- **Classe 4**: Accettabile così com'è, anche se deve essere monitorato.

Cos'è SIL?

Safety Integrity Level

E' la probabilità (likelihood) che un sistema, che impatta sulla sicurezza fisica delle persone e sull'ambiente, svolga la funzione di sicurezza richiesta in tutte le condizioni indicate entro un determinato periodo di tempo.

Esistono quattro livelli di SIL da 1 a 4, dal meno gravoso al più gravoso.

La classificazione dello specifico livello può essere effettuata, per le operazioni e i processi continui, attraverso la Probabilità di Malfunzionamento per Ora (PFH) e del suo corrispondente Fattore di Riduzione del Rischio (RRF).

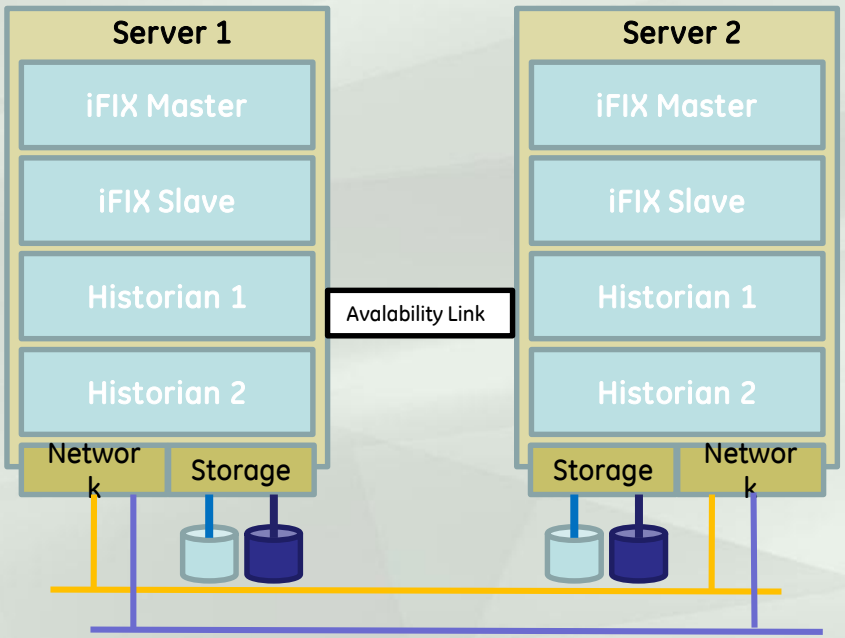
SIL	PFH (Probability of Failure per Hour - Probabilità di Rottura per Ora)	PFH (power)	RRF (Risk Reduction Factor - Fattore di Riduzione del Rischio)
1	0.00001-0.000001	10^{-5} – 10^{-6}	100,000–1,000,000
2	0.000001-0.0000001	10^{-6} – 10^{-7}	1,000,000–10,000,000
3	0.0000001-0.00000001	10^{-7} – 10^{-8}	10,000,000–100,000,000
4	0.00000001-0.000000001	10^{-8} – 10^{-9}	100,000,000–1,000,000,000

Il SIL nei sistemi di supervisione e controllo

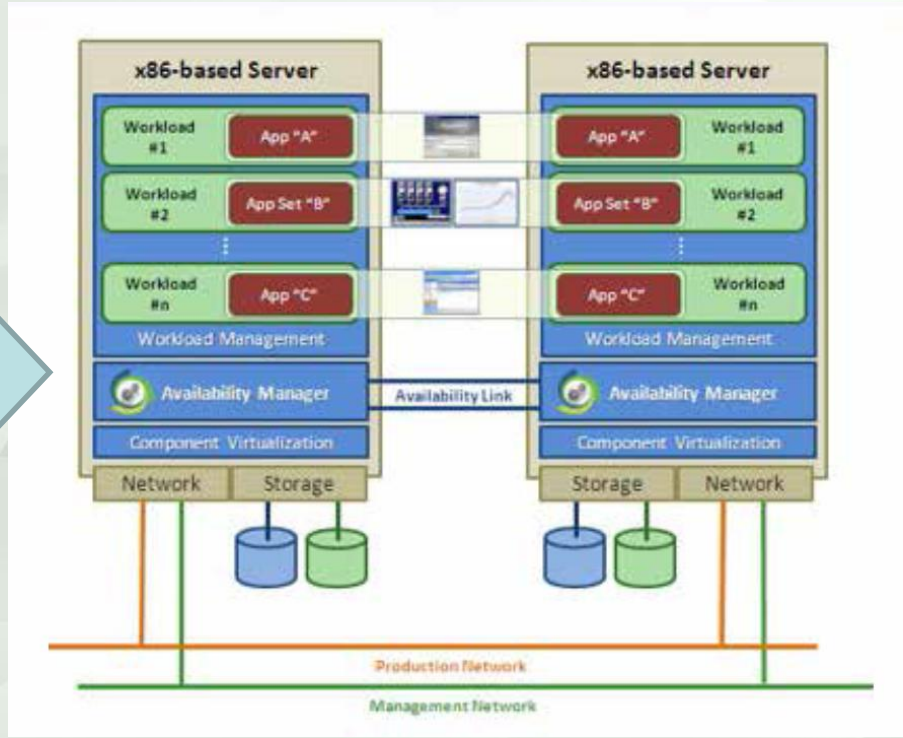
- Non tutti i sistemi di controllo e ancor meno i sistemi si supervisione (HMI e SCADA) hanno, o possono avere, impatto diretto con la sicurezza fisica delle persone o con l'ambiente.
- Ciononostante, nelle infrastrutture critiche (trasporti, energia,utilities), i sistemi di controllo e di supervisione sono determinanti nei processi funzionali complessi e possono quindi rappresentare elementi di rischio. In questo senso una valutazione dell'impatto che questi sistemi possono avere sulla sicurezza può e deve essere effettuata.

Una configurazione software ridondante e resiliente

Ridondanza e Sincronizzazione



Workload Management



iFIX/Historian + Stratus uptime

- GE Digital e Stratus propongono un insieme di soluzioni per l'Alta Disponibilità e la Fault Tollerance orientate a mitigare il rischio nei sistemi in ambito SIL.

Description	Number of Servers	Availability Level	Average Yearly Downtime	PFH	SIL Level *	RRF [1]
Standard Market or Host Server	1	99,9	8 hours, 45 minutes	0,001	.	Base
iFIX / Historian Redundant Server[2]	2	99,95	4 hours, 23 minutes	0,0005	.	2
iFIX / Historian Stratus HA everRun Server[3]	2	99,99	52 minutes, 56 seconds	0,0001	.	10
iFIX / Historian Stratus FT everRun Server[3]	2	99,999	5 minutes, 16 seconds	0,0000095	1	105
iFIX / Historian Stratus FT Server	1[4]					1666

1666 volte + sicuro di un server di mercato

http://www.stratus.com/about/company-information/uptime-meter/

1: RRF - Fattore di riduzione del rischio relativamente ad un server standard di mercato (base)
2: iFIX 5.8 enhanced failover, Historian cluster server
3: Controllare la compatibility list di Stratus everRun
4: Two redundant CPU boards

ServiTecno

www.servitecno.it

Servitecno Srl
Tel.02-48.61.41 – Fax.02-48.61.44.41
ftieghi@servitecno.it
via Francesco Koristka, 10
20154 Milano (MI) – Italy