Sistema Socio Sanitario
Regione Lombardia
ATS Milano
Città Metropolitana

AGENZIA DI TUTELA DELLA SALUTE DELLA CITTÀ METROPOLITANA DI MILANO
Dipartimento di Igiene e Prevenzione Sanitaria
UOC Impiantistica – UOS Sicurezza Elettrica
Sede di via Statuto, 5 - MILANO 20121 - Tel. 02/8578.9344 fax 02/8578.9359
e-mail: sicurezzaelettrica@ats-milano.it
PEC: dipartimentoprevenzione@pec.ats-milano.it
Sede Legale: Milano, 20122, Corso Italia 19 - Codice fiscale e P.IVA09320520969

COORDINAMENTO TECNICO INTERREGIONALE SALUTE E SICUREZZA LUOGHI DI LAVORO
Gruppo Tematico Macchine e Impianti

Linee di indirizzo per la costruzione di impianti ad atmosfera controllata per la conservazione della frutta Focus sulla conservazione delle mele
(Agosto 2016)

ALCUNE MISURE DI PREVENZIONE INTERESSANO LA SICUREZZA FUNZIONALE

QUADERNO TECNICO

RISCHIO DI ASFISSIA
AMBIENTI SOTTO OSSIGENATI PER LA CONSERVAZIONE DELLE MELE
AFFIDABILITÀ DEL SISTEMA DI MONITORAGGIO E CONTROLLO

Autore:
Tecnico della Prevenzione
dott. Mauro Baldissin

Responsabile scientifico:
Dirigente Ingegnere
dott. ing. Massimo Rho

INDICE

1. PREMESSA

Le "*Linee di indirizzo per la costruzione di impianti ad atmosfera controllata per la conservazione della frutta. Focus sulla conservazione delle mele*" (nel seguito: "documento"), elaborate dal Gruppo Tematico Macchine e Impianti del Coordinamento Tecnico Interregionale Salute e Sicurezza Luoghi di Lavoro, considerano la tecnologia per la conservazione delle mele denominata *atmosfera controllata* (AC), prendono in esame le principali criticità sotto l'aspetto della sicurezza e forniscono le relative possibili misure di prevenzione.
Il documento, al quale si rinvia per la trattazione completa, focalizza l'attenzione sul pericolo costituito dall'atmosfera sotto ossigenata, presente nel volume delle celle per la conservazione della frutta durante il funzionamento in AC. Tale pericolo, potenzialmente, esiste nelle stesse celle anche in condizioni di libero accesso (dopo bonifica) e nei locali tecnici pertinenti a causa dei possibili guasti sull'impianto di erogazione azoto o di anomalie del processo.
Tra le misure di prevenzione suggerite, alcune prevedono l'utilizzo di sistemi di monitoraggio dell'atmosfera in grado di controllare segnalazioni, allarmi e componenti dell'impianto, per i quali il documento precisa: *al fine di garantire un'adeguata affidabilità delle funzioni di sicurezza del sistema di monitoraggio e controllo, necessario per assicurare la vivibilità dell'ambiente in presenza di persone, le stesse devono essere realizzate secondo la regola dell'arte, con eventuale riferimento alle norme tecniche della serie CEI EN 61508 "Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza"*.

Il presente elaborato propone una possibile modalità di analisi e valutazione dell'affidabilità delle funzioni di sicurezza di un ipotetico sistema di monitoraggio e controllo.
Le considerazioni svolte sono frutto di esperienze in attività di vigilanza inerente la legislazione in materia di protezione da atmosfere esplosive e di sintesi della letteratura tecnica reperita.
Quanto sviluppato riveste carattere generale e non cogente. Le indicazioni fornite costituiscono una possibile interpretazione delle norme tecniche e prassi applicabili, alle quali occorre comunque riferirsi.
In quanto principale destinatario degli obblighi di legge in materia di salute e sicurezza sul luogo di lavoro, il datore di lavoro deve valutare l'idoneità alla propria specifica attività lavorativa dell'esempio proposto che è didattico e indicativo delle sole situazioni considerate o di situazioni assimilabili.

2. CENNI SULLA TEORIA DELL'AFFIDABILITÀ

Si definisce affidabilità (reliability) di un elemento (componente, dispositivo o apparato), che funziona in condizioni prestabilite per un determinato tempo, la probabilità che in tale intervallo di tempo non sopraggiunga un guasto[1].
Se i guasti sono casuali (esclusi quindi i guasti infantili e quelli dovuti ad errori di progetto o all'usura), l'affidabilità si esprime con la seguente relazione:

$$R(t) = e^{-\lambda t}$$

dove:

e	= 2,718	base dei logaritmi naturali
λ		tasso di guasto (supposto costante)
t		tempo di impego (o di *osservazione*) dell'elemento al quale è riferita l'affidabilità

Il tasso di guasto λ rappresenta il numero di elementi che si guastano nell'unità di tempo, espresso in "numero di guasti per ora o per anno" (t deve essere misurato nella stessa unità di tempo).
La probabilità di guasto nel tempo t vale $1 – R(t)$.
Ovviamente, a parità di tasso di guasto λ, più è elevato il tempo e minore è il valore dell'affidabilità (che tende a zero quando il tempo tende all'infinito).

L'affidabilità dei sistemi di sicurezza basati su una tecnologia elettrica, elettronica ed elettronica programmabile è normata, in ambito internazionale, da varie norme tecniche relative alla sicurezza funzionale (*Safety-related systems*).
La norma CEI EN 61508 "*Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza*" rappresenta un riferimento generale per la materia, è destinata ai fabbricanti di componenti e sistemi di sicurezza ed ha introdotto il concetto fondamentale di livello di integrità della sicurezza (SIL - *Safety Integrity Level*) delle funzioni che devono garantire la sicurezza dell'attrezzatura sotto controllo (EUC – *Equipment Under Control*) e della strumentazione che la realizzano, quale indice della sicurezza funzionale.

[1] Un guasto generico, anche non pericoloso.

Tale norma definisce valori discreti di SIL da 1 a 4, in ordine crescente di integrità, a cui corrispondono gamme di valori di probabilità di fallimento decrescente della funzione di sicurezza considerata, per due condizioni di funzionamento (Tabella 2.1):

- funzionamento a bassa richiesta di intervento della funzione (meno di una volta all'anno), per il quale si specifica la probabilità per ogni singolo evento;
- funzionamento ad alta richiesta di intervento della funzione (o continua), per il quale si specifica la densità di probabilità (probabilità per ora di funzionamento).

Tabella 2.1 - Livelli di Integrità della Sicurezza definiti nella norma CEI EN 61508

Livello di Integrità della Sicurezza (**SIL**)	Probabilità di fallimento media su domanda per anno (o bassa domanda) ($\mathbf{PFD_{avg}}$)	Disponibilità di Sicurezza ($\mathbf{1\text{-}PFD_{avg}}$)	Fattore di Riduzione del Rischio (**RRF**)	Probabilità di fallimento media per ora (modo continuo o alta domanda) ($\mathbf{PFH_{avg}}$)
SIL 4	$\geq 10^{-5}$ a $< 10^{-4}$	99,99 ÷ 99,999%	100.000 ÷ 10.000	$\geq 10^{-9}$ a $< 10^{-8}$
SIL 3	$\geq 10^{-4}$ a $< 10^{-3}$	99,9 ÷ 99,99%	10.000 ÷ 1.000	$\geq 10^{-8}$ a $< 10^{-7}$
SIL 2	$\geq 10^{-3}$ a $< 10^{-2}$	99 ÷ 99,9%	1.000 ÷ 100	$\geq 10^{-7}$ a $< 10^{-6}$
SIL 1	$\geq 10^{-2}$ a $< 10^{-1}$	90 ÷ 99%	100 ÷ 10	$\geq 10^{-6}$ a $< 10^{-5}$

3. ANALISI DEL LIVELLO DI PROTEZIONE (LOPA)

3.1 INTRODUZIONE

L'analisi del livello di protezione (LOPA - *Layers of Protection Analisys*) è un modo strutturato di calcolo degli obiettivi di riduzione del rischio e può essere utilizzata anche per stabilire gli obiettivi SIL.

Il metodo LOPA considera ogni pericolo identificato e documenta le cause innescanti e i livelli di protezione che prevengono o limitano il pericolo. Successivamente, viene determinata l'entità totale di riduzione del rischio e analizzato il bisogno di un'ulteriore riduzione.

Se occorre fornire protezione aggiuntiva sotto forma di un sistema strumentato di sicurezza (SIS - *Safety Instrumented System*), la metodologia consente la determinazione del SIL appropriato e della probabilità media di guasto richiesta (PFD_{avg} – *Average Probability of Failure on Demand* / PFH_{avg} - *Average Probability of Failure per Hour*).

Il processo LOPA viene registrato su fogli di lavoro che permettono di quantificare gli eventi scatenanti e le loro frequenze, oltre che di attestare la riduzione del rischio fornita dai livelli di protezione indipendenti (IPL – *Indipendent Protection Level*).

Le spiegazioni del foglio di lavoro elaborato per il caso in questione, sono descritte nelle sezioni seguenti.

3.2 ANALISI LOPA 3.A – STATO DI FATTO

3.2.1 ID/Rif. pericolo

Fornisce un identificativo per ogni pericolo ai fini della tracciabilità con altri studi e con l'assegnazione della funzione di sicurezza e della verifica del SIL.

3.2.2 Descrizione zona

Fornisce la descrizione della zona in cui è presente il pericolo.

3.2.3 Descrizione evento (pericolo)

Fornisce una descrizione del pericolo identificato. Nell'esempio, i pericoli considerati nell'analisi sono:

- rif. 1.01: accesso di un lavoratore nella cella in regime di AC;
- rif. 1.02: accesso di più lavoratori nella cella bonificata con possibile insufflazione involontaria di azoto.

3.2.4 Conseguenze

Descrive le conseguenze del pericolo. Nell'analisi LOPA dell'esempio, sono state analizzate le conseguenze del pericolo unicamente in termini di sicurezza del personale, escludendo gli eventuali rischi per l'ambiente e quelli di tipo economico (es. danni agli impianti, fermata del processo, ecc.).

3.2.5 Categoria di gravità

Nell'ambito della valutazione dei rischi, la gravità delle conseguenze può essere categorizzata. Nell'esempio, è stato utilizzato il seguente criterio (Tabella 3.1):

Tabella 3.1 – Categoria di gravità

Conseguenze	Categoria di gravità	Frequenza dei rischi obiettivo (/anno)	Descrizione delle conseguenze
Per le persone (sicurezza)	P1	10^{-1}	Trattamento medico o lesioni che limitano la capacità di lavoro
	P2	10^{-2}	Lesioni senza effetto permanente
	P3	10^{-3}	Lesioni con effetto permanente
	P4	10^{-4}	Un incidente mortale e/o diverse disabilità permanenti
	P5	10^{-5}	Diversi incidenti mortali (2 ÷ 10)
	P6	10^{-6}	Diversi incidenti mortali (oltre 10)

3.2.6 Massimo rischio tollerabile

Quale massima frequenza tollerabile delle conseguenze del pericolo, viene utilizzata quella indicata nella colonna "*Frequenza dei rischi obiettivo (/anno)*" della precedente tabella.

3.2.7 Causa scatenante

Elenca le cause identificate del pericolo. Nell'esempio, le cause scatenanti considerate nell'analisi sono:

- rif. 1.01: errore del lavoratore;
- rif. 1.02: guasto, anomalia nel processo.

3.2.8 Frequenza della causa scatenante (/anno)

Quantifica il tasso di accadimento previsto della causa scatenante. Questo tasso può essere stimato in base all'esperienza, a dati storici disponibili oppure può essere acquisito da adeguate fonti sui tassi di guasto.
Quando basate su fattori umani quali l'errore di un operatore, le frequenze della cause scatenanti possono essere difficile da stimare. Una tecnica è quella di basare la stima sulla frequenza delle opportunità che ha un operatore di compiere un errore, per poi moltiplicarla per la probabilità che ha di compiere un errore pericoloso.

Nell'esempio, la frequenza delle cause scatenanti considerata nell'analisi è:

- rif. 1.01: $1{,}2 \cdot 10^{-2}$ (/anno), ricavata come segue:
  è stata considerata una frequenza mensile (n. 12 all'anno) di presenza di un lavoratore nella zona di ingresso alle celle in regime di atmosfera controllata. Presumendo che il lavoratore sia ben formato, che il compito sia di routine e che egli non sia soggetto a stress, è stata assunta una probabilità di accesso all'interno delle celle per errore dello 0,1% (rif. norma CEI EN 61511-3).
  La frequenza della causa scatenante è stata quindi quantificata nel risultato del prodotto: 12 (presenze/anno) x 0,001 (probabilità di errore) = $1{,}2 \cdot 10^{-2}$ (/anno);
- rif. 1.02: $1{,}6 \cdot 10^{-2}$ (/anno), ricavato come segue:
  è stato acquisito il tasso di guasto/perdita in chiusura della valvola automatica di erogazione azoto considerata in servizio gravoso e del relativo solenoide (componenti considerati in serie dal punto di vista dell'affidabilità), dalle seguenti fonti: Exida - Safety Equipment Reliability Handbook, guida CEI 65-186.

3.2.9 Probabilità del verificarsi delle conseguenze

Le conseguenze del pericolo potrebbero non verificarsi sistematicamente ad ogni evento scatenante. Ad esempio, se la rottura di un serbatoio per sovrapressione può avere come conseguenza la morte di uno o più lavoratori a causa della pericolosità della sostanza contenuta, si potrebbe sostenere che la maggior parte delle condizioni di sovrappressione non comporti la perdita di contenimento ma solo una fuga di lieve entità, ad esempio da una flangia.

Nell'esempio, la probabilità del verificarsi delle conseguenze considerate nell'analisi è:

- rif. 1.01: 1, in quanto nelle celle in condizioni di AC la concentrazione di ossigeno è molto bassa (qualche unità percentuale);
- rif. 1.02: 0,5, in quanto la probabilità che i lavoratori si trovino in una zona a bassa concentrazione di ossigeno nella cella bonificata e con rilevatori di ossigeno in funzione è stimata del 50 %.

3.2.10 Livelli di protezione indipendenti (IPL)

Ciascun mezzo di protezione indipendente viene identificato e valutato in relazione alle proprie caratteristiche di mitigazione, ovvero alla probabilità che non riuscirà ad eseguire la funzione specificata su domanda, probabilità PFD, un valore adimensionale compreso tra 0 e 1. Al diminuire del valore della probabilità PFD, aumenta il fattore di riduzione del rischio che viene applicato come fattore modificante della frequenza della causa scatenante calcolata (3.2.8); quindi, dove non viene attestato alcun livello IPL, nel foglio di lavoro LOPA viene inserito "1"; nel caso in cui l'IPL sia totalmente inesistente, nel foglio di lavoro LOPA non viene inserito alcun valore.

3.2.10.1 Sistema BPCS

Il sistema di controllo di processo base (BPCS - *Basic Process Control System*) può essere preso in considerazione se previene il verificarsi di un pericolo derivante da una potenziale causa scatenante. Una probabilità di guasto PFD di 0,1 è generalmente la massima riduzione del rischio attestabile per un sistema non classificato SIL.
Nell'esempio, la PFD del sistema di controllo di processo base considerate nell'analisi è:
- rif. 1.01: 1, in quanto questo non ha influenza sul verificarsi dell'evento;
- rif. 1.02: 0,1.

3.2.10.2 Allarmi indipendenti

È possibile considerare allarmi, indipendenti dal sistema BPCS, che avvisino l'operatore e ne richiedano l'azione. L'allarme può essere considerato solo se realmente indipendente dal sistema BPCS e solo se l'operatore può rispondere all'allarme e intervenire rendendo il processo sicuro.
Nell'esempio, allo stato di fatto, non sono presenti allarmi indipendenti.

3.2.10.3 Mitigazione aggiuntiva: livelli di presidio

I livelli di mitigazione possono includere la presenza ovvero l'intervallo di tempo durante cui un lavoratore è esposto ad un pericolo ed ha accesso limitato alle zone pericolose.
Nell'esempio, si ipotizza attestata una presenza basata su turni di 4 ore e di 8 ore. Il corrispondente valore considerato nell'analisi è:
- rif. 1.01: 0,16, determinato dal rapporto: 4 ore/24 ore;
- rif. 1.02: 0,33, determinato dal rapporto: 8 ore/24 ore.

3.2.10.4 Frequenza delle conseguenze

La frequenza delle conseguenze viene calcolata moltiplicando i valori delle colonne 8, 9 e 10. Il numero calcolato è in unità di eventi all'anno. La frequenza totale delle conseguenze indica il tasso di domanda su qualunque funzione di sicurezza proposta.

3.2.10.5 PFD richiesta

Calcolata confrontando il massimo rischio tollerabile con la frequenza delle conseguenze (rapporto tra il valore della colonna 6 e quello della colonna 11).

3.2.10.6 SIL richiesto

Ottenuto dalla Tabella 2. e corrispondente alla probabilità PFD richiesta.

3.10.2.7 Foglio di lavoro LOPA 3.A – Stato di fatto

1	2	3	4	5	6	7	8	9	10			11	12		13
ID/Rif. pericolo	Descrizione zona	Descrizione evento (pericolo)	Conseguenze	Categoria di gravità	Massimo rischio tollerabile	Causa scatenante	Frequenza della causa scatenante	Probabilità del verificarsi delle conseguenze	Livelli di protezione indipendenti			Frequenza delle conseguenze	Sistema relativo alla sicurezza (SrS)		Commenti
									Sistema BPCS	Allarmi indipendenti	Mitigazione aggiuntiva: livelli di presidio		PFD richiesta	SIL richiesto	
					(/anno)		(/anno)					(/anno)			
[a]	[b]	[c]	[d]	[e]	[f]	[g]	[h]	[i]	[l]	[m]	[n]	[o]	[p]	[q]	[r]
101	Celle di conservazione della frutta in *atmosfera controllata* (AC)	Accesso di un lavoratore nella cella in regime di AC	Possibile incedente mortale per asfissia	P4	1,00E-04	Errore del lavoratore	1,20E-02	1	1		0,16	1,92E-03	5,21E-02	SIL 1	[h] La frequenza di presenza alla zona di ingresso alle celle è considerata mensile (n. 12 all'anno) [i] Dato il bassissimo tenore di ossigeno si considera il 100% di probabilità di morte [l] Il sistema base di controllo del processo non ha influenza sull'evento [n] Si considera l'area occupata 4 ore al giorno
102	Celle di conservazione della frutta in atmosfera normale (ambiente bonificato)	Accesso di più lavoratori nella cella bonificata con possibile insufflazione involontaria di azoto	Possibile incedente mortale per asfissia	P5	1,00E-05	Guasto, anomalia nel processo	1,60E-02	0,5	0,1		0,33	2,64E-04	3,79E-02	SIL 1	[h] Guasto/perdita in chiusura della valvola automatica di erogazione azoto considerata in servizio gravoso [i] La probabilità che i lavoratori si trovino in una zona a bassa concentrazione di ossigeno nella cella bonificata e con rilevatori di O_2 in funzione è stimata del 50% [l] Si considera che il sistema base di controllo del processo possa evitare 9 eventi (erogazione intempestiva di azoto) su 10 [n] Si considera l'area occupata 8 ore al giorno

3.2.11 Risultato dell'analisi dello stato di fatto

I risultati (Tabella 3.2) mostrano che il pericolo dovuto all'atmosfera sotto ossigenata ha conseguenze sulla sicurezza delle persone che possono essere protette con una funzione strumentata di sicurezza SIL1 in entrambi i casi prospettati, con PFD, rispettivamente, ≤ $5{,}21 \cdot 10^{-2}$ e ≤ $3{,}79 \cdot 10^{-2}$.

Tabella 3.2 - Risultato dell'analisi dello stato di fatto

ID/Rif. pericolo	Pericolo (colonna 4 – lettera [d])	PFD richiesta (colonna 12 – lettera [p])	SIL richiesto (colonna 12 – lettera [q])
1.01	Accesso di un lavoratore nella cella in regime di AC	$5{,}21 \cdot 10^{-2}$	SIL 1
1.02	Accesso di più lavoratori nella cella bonificata con possibile insufflazione involontaria di azoto	$3{,}79 \cdot 10^{-2}$	SIL 1

3.3 INSTALLAZIONE DI UN SISTEMA DI MONITORAGGIO E CONTROLLO DELL'ATMOSFERA SOTTO OSSIGENATA

Seguendo le indicazioni suggerite nel documento, si prevede l'installazione, quale funzione strumentata di sicurezza, di un sistema di monitoraggio e controllo dell'atmosfera sotto ossigenata con funzioni di segnalazione visiva dello stato delle celle (presenza di AC, cella con libero accesso) e di allarme nel caso di apertura della porta delle celle in condizioni di AC; inoltre, anche in assenza di condizioni di AC, con funzioni di blocco sulla tubazione di erogazione dell'azoto nel caso di apertura della porta delle celle.

3.3.1 SISTEMA STRUMENTATO DI SICUREZZA

La valutazione affidabilistica viene effettuata secondo il metodo delle norme CEI EN 61508.

L'affidabilità dei sistemi strumentati di sicurezza basati su una tecnologia elettrica, elettronica o elettronica programmabile, sono complessivamente rappresentabili come indicato in Figura 3.1:

Figura 3.1 – Schema a blocchi di un sistema strumentato di sicurezza

Il metodo consente il calcolo della probabilità media di fallimento, nel caso specifico su domanda (PFD_{avg}), e si basa sulle seguenti assunzioni:

a) utilizzo di equazioni semplificate per valutare l'integrità di un sistema strumentato di sicurezza;
b) ratei di guasto degli elementi (sottosistemi) costanti per l'intero ciclo di vita;
c) stesso rateo di guasto per elementi uguali ridondati;
d) rateo di guasto dei sensori inclusivo di ogni elemento, dal modulo di ingresso dello strumento al modulo di ingresso del risolutore logico;
e) rateo di guasto del risolutore logico, inclusivo del modulo di ingresso, della logica, del modulo in uscita, delle sorgenti di potenza e normalmente fornito dal fabbricante;
f) rateo di guasto degli attuatori inclusivo di ogni elemento, dal modulo d'uscita del risolutore logico fino all'elemento finale stesso;
g) intervallo di tempo tra le verifiche e prove (TI – *Time Interval between tests*), molto più breve del tempo medio tra i guasti (MTTF - *Mean Time To Failure*);
h) **in occasione delle verifiche e prove degli elementi del sistema, tutti i guasti sono rilevati e riparati**;
i) sensori e attuatori sono selezionati (possibilmente) a sicurezza positiva (*Fail safe*), ovvero in modo tale da portare l'impianto in uno stato di sicurezza quando disalimentati.

Il metodo prevede una serie di "architetture" (MooN: "*M*" *su* "*N*")[2] del sistema strumentato di sicurezza che pongono i seguenti limiti al livello di integrità della sicurezza hardware (Tabelle 3.3 e 3.4):

Tabella 3.3 – Integrità della sicurezza dell'hardware. Vincoli architetturali per sottosistemi relativi alla sicurezza di Tipo A[3]

Frazione dei guasti sicuri (SFF)[4]	Tolleranza al guasto hardware		
	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60% ÷ < 90%	SIL 2	SIL 3	SIL 4
90% ÷ < 99%	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

Tabella 3.4 – Integrità della sicurezza dell'hardware. Vincoli architetturali per sottosistemi relativi alla sicurezza di Tipo B[5]

Frazione dei guasti sicuri (SFF)	Tolleranza al guasto hardware		
	0	1	2
< 60%	Non ammesso	SIL 1	SIL 2
60% ÷ < 90%	SIL 1	SIL 2	SIL 3
90% ÷ < 99%	SIL 2	SIL 3	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

I tassi di guasto λ necessari per l'analisi sono stati ricercati nelle seguenti fonti:
- Exida - Safety Equipment Reliability Handbook;
- Reliability Information Analysis Center - Nonelectronic Parts Reliability Data;
- Offshore REliability DAta Handbook (OREDA);
- norma CEI EN 61508;
- norma CEI EN 61511;
- guida CEI 65-186.

[2] Sistema strumentato di sicurezza, o parte di esso, composto da "N" canali indipendenti, che sono connessi in modo tale che "M" canali sono sufficienti per eseguire la funzione strumentata di sicurezza.

[3] Sottosistemi semplici con un ben noto modo di guasto e con una provata storia di funzionamento (sensori, attuatori, risolutori logici non programmabili).

[4] $SFF = \frac{\sum\lambda_{DD}+\sum\lambda_{SD}+\sum\lambda_{SU}}{\sum\lambda_{DD}+\sum\lambda_{DU}+\sum\lambda_{SD}+\sum\lambda_{SU}}$ [%]

dove:

λ_{DD} tasso dei guasti pericolosi rilevati
λ_{SD} tasso dei guasti sicuri rilevati
λ_{SU} tasso dei guasti sicuri non rilevati
λ_{DU} tasso dei guasti pericolosi non rilevati

[5] Sottosistemi complessi con modi di guasto potenzialmente sconosciuti (risolutori logici programmabili).

3.3.1.1 IPOTESI 1

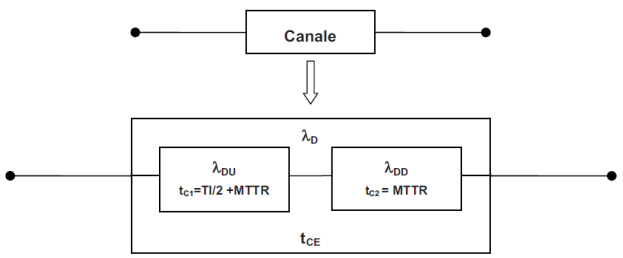
Si ipotizza un sistema di monitoraggio e controllo realizzato con (Figura 3.2):

- Sensore: un rilevatore di ossigeno (O_2)[6], con tolleranza al guasto hardware = 0, senza ridondanza (architettura: 1oo1[7]);
- Risolutore logico: un PLC industriale, con tolleranza al guasto hardware = 0, senza ridondanza (architettura: 1oo1);
- Attuatore A1: un sensore di prossimità installato sulla porta di ingresso alle celle, con tolleranza al guasto hardware = 0, senza ridondanza (architettura: 1oo1);
- Attuatore A2: un sistema di segnalazione visiva dello stato delle celle (luce verde: consenso all'accesso; luce rossa: inibizione all'accesso), con tolleranza al guasto hardware = 0, senza ridondanza (architettura: 1oo1);
- Attuatore A3: un sistema di allarme acustico azionato all'apertura della porta d'ingresso alle celle in condizioni di AC, con tolleranza al guasto hardware = 0, senza ridondanza (architettura: 1oo1);
- Attuatore A4: una valvola automatica di sicurezza sulla tubazione di erogazione dell'azoto azionata all'apertura della porta d'ingresso alle celle, con tolleranza al guasto hardware = 0, senza ridondanza (architettura: 1oo1).

Se non diversamente specificato, il tempo medio di riparazione di ogni sottosistema (MTTR - *Mean Time To Repair*) è assunto pari a 8 ore.

[6] Per ogni zona (spazio tridimensionale) monitorata, le cui dimensioni sono assegnate sulla base delle indicazione del fabbricante, norme tecniche, ecc.

[7] Schema di affidabilità dell'architettura 1oo1:



Dalla figura risulta che il tasso dei guasti pericolosi λ_D è pari a:

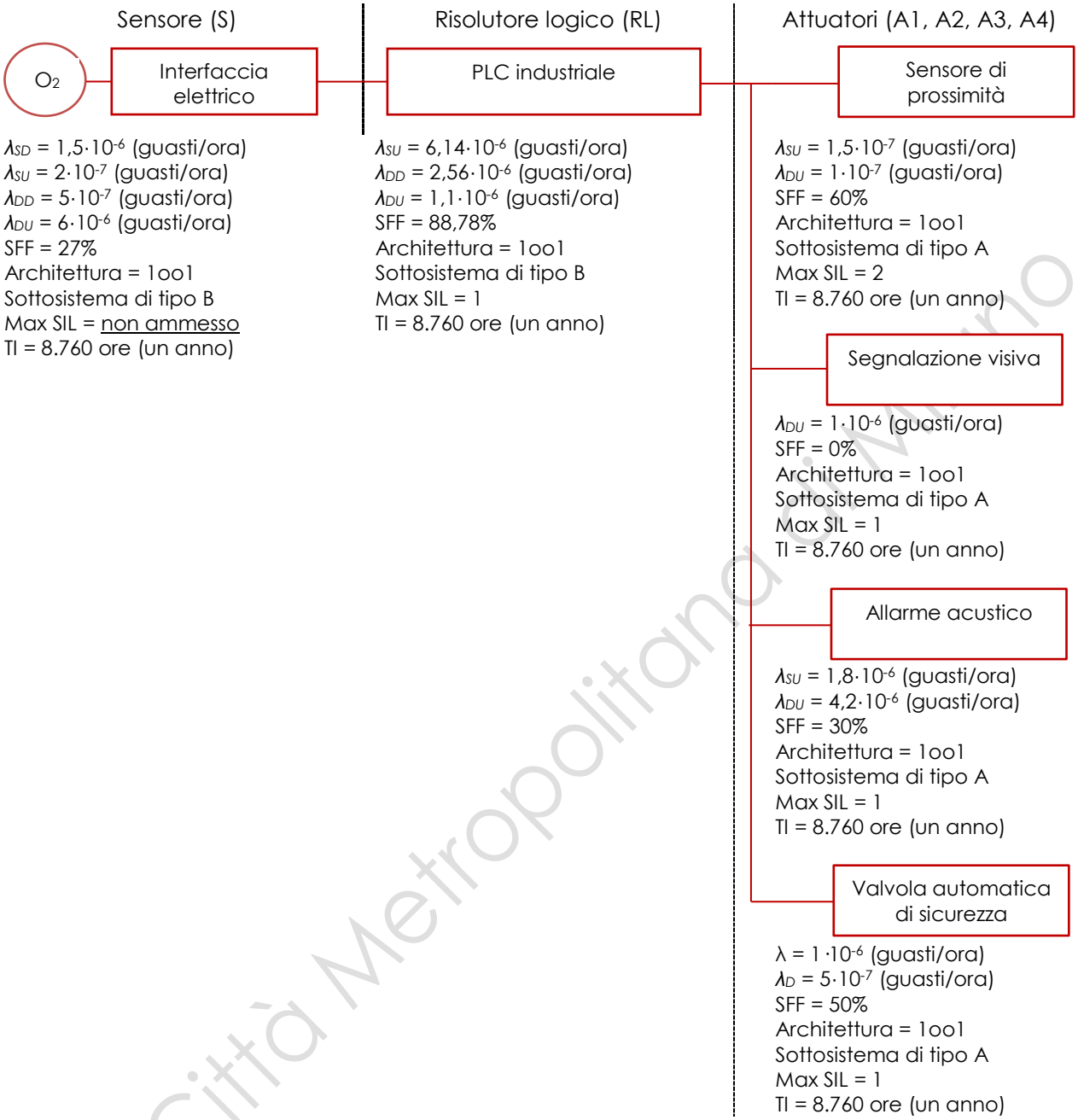
$\lambda_D = \lambda_{DU} + \lambda_{DD} = \lambda/2$

per cui è possibile calcolare il tempo di guasto equivalente del canale t_{CE} tramite la relazione:

$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{TI}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR$

Pertanto il PFD dell'architettura 1oo1 si può così formulare: $PFD_{1oo1} = (\lambda_{DU} + \lambda_{DD}) \cdot t_{CE}$

Figura 3.2 – Schema a blocchi - Ipotesi 1



La valutazione di affidabilità si interrompe vista l'impossibilità di classificare in termini di SIL il rilevatore di ossigeno non ridondante.

3.3.1.2 IPOTESI 2

Viene ripetuta la valutazione affidabilistica con l'aggiunta di un rilevatore di ossigeno (Figura 3.3):

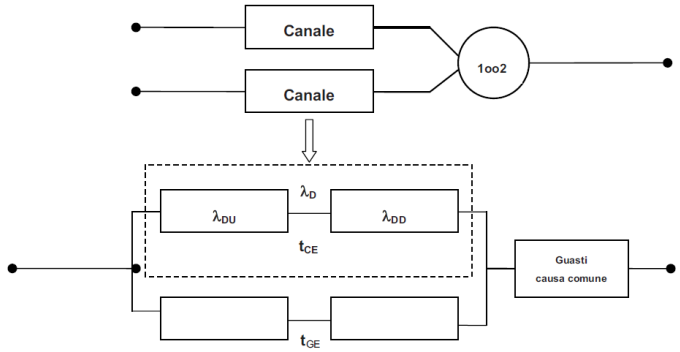
- Sensore: due rilevatore di ossigeno (O_2)[8], ognuno con tolleranza al guasto hardware = 0, con ridondanza (architettura: 1oo2);
- Risolutore logico: un PLC industriale, con tolleranza al guasto hardware = 0, senza ridondanza (architettura: 1oo1);
- Attuatore A1: un sensore di prossimità installato sulla porta di ingresso alle celle, con tolleranza al guasto hardware = 0, senza ridondanza (architettura: 1oo1);
- Attuatore A2: un sistema di segnalazione visiva dello stato delle celle (luce verde: consenso all'accesso; luce rossa: inibizione all'accesso), con tolleranza al guasto hardware = 0, senza ridondanza (architettura: 1oo1);
- Attuatore A3: un sistema di allarme acustico azionato all'apertura della porta d'ingresso alle celle in condizioni di AC, con tolleranza al guasto hardware = 0, senza ridondanza (architettura: 1oo1);
- Attuatore A4: una valvola automatica di sicurezza sulla tubazione di erogazione dell'azoto azionata all'apertura della porta d'ingresso alle celle, con tolleranza al guasto hardware = 0, senza ridondanza (architettura: 1oo1).

Se non diversamente specificato:

- l'MTTR di ogni sottosistema è assunto pari a 8 ore;
- per architetture ridondanti (1oo2[9]), il tasso dei guasti di modo e di causa comune non rilevati dalla diagnostica (Fattore β) è assunto pari al 10%;
- per architetture ridondanti (1oo2), il tasso dei guasti di modo e di causa comune rilevati dalla diagnostica (Fattore β_D) è assunto pari al 5%.

[8] Per ogni zona (spazio tridimensionale) monitorata, le cui dimensioni sono assegnate sulla base delle indicazione del fabbricante, norme tecniche, ecc.

[9] Schema di affidabilità dell'architettura 1oo2:



Dalla figura risulta che il tempo di guasto equivalente del canale t_{CE}, corrisponde a quello dell'architettura 1oo1.

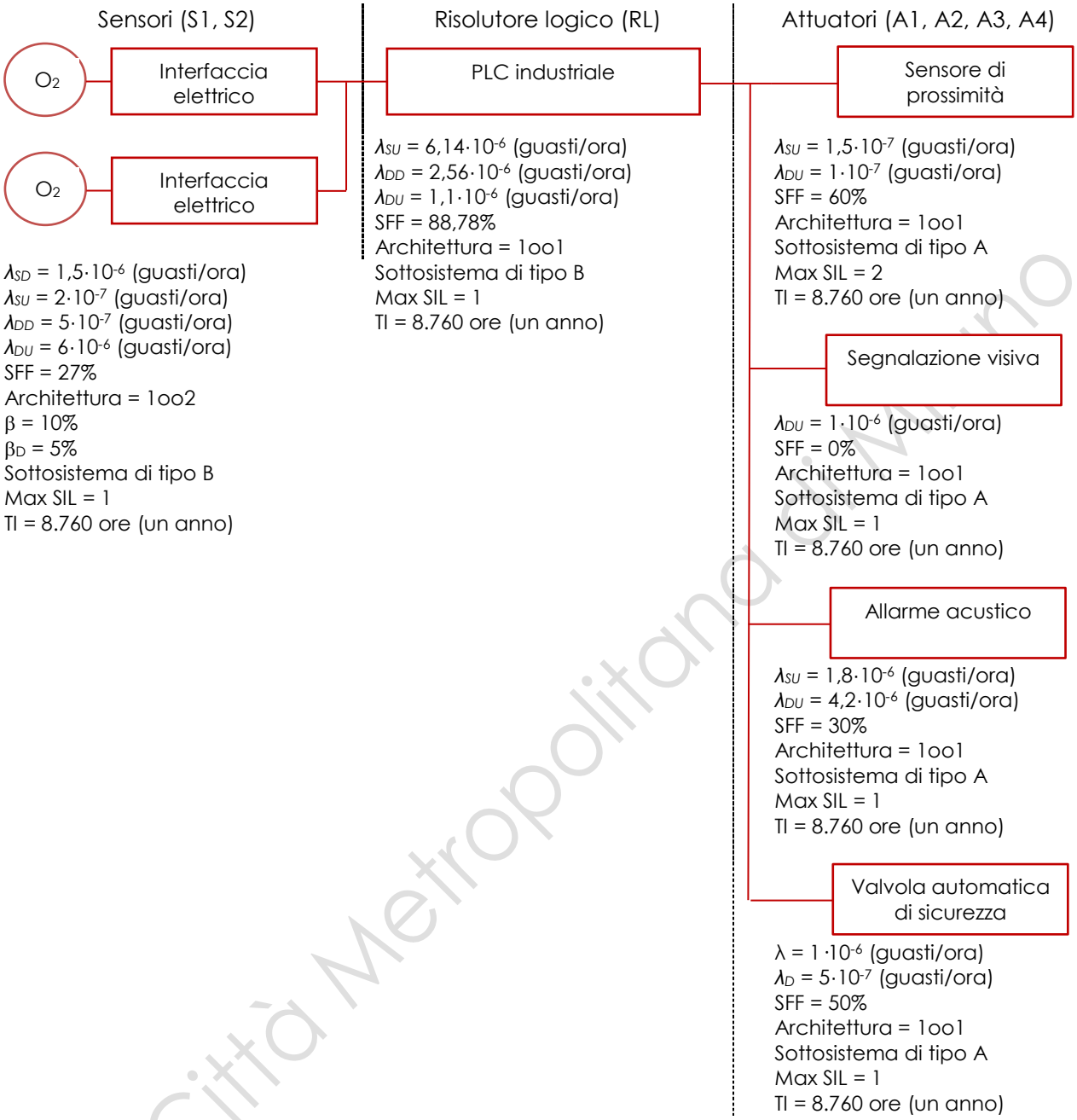
Il tempo di guasto equivalente del sistema è calcolabile tramite la relazione:

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{TI}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR$$

Pertanto il PFD dell'architettura 1oo2 si può così formulare:

$$PFD_{1oo2} = 2 \cdot [(1-\beta_D) \cdot \lambda_{DD} + (1-\beta) \cdot \lambda_{DU}]^2 \cdot t_{CE} \cdot t_{GE} + \beta_D \cdot \lambda_{DD} \cdot MTTR + \beta \cdot \lambda_{DU} \cdot \left(\frac{TI}{2} + MTTR\right)$$

Figura 3.3 – Schema a blocchi - Ipotesi 2



Il PFD_{SYS} del sistema è dato dalla somma dei PFD dei sottosistemi:

$$PFD_{SYS} = PFD_{S1,S2} + PFD_{RL} + PFD_{A1} + PFD_{A2} + PFD_{A3} + PFD_{A4} = 3{,}39\cdot10^{-3} + 4{,}85\cdot10^{-3} + 4{,}39\cdot10^{-4} + 4{,}39\cdot10^{-3} + 1{,}84\cdot10^{-2} + 2{,}19\cdot10^{-3} = 3{,}37\cdot10^{-2}$$

Il livello di integrità della sicurezza del sistema di monitoraggio e controllo in condizioni di funzionamento a bassa richiesta di intervento (su domanda), risulta compatibile con SIL 1 secondo la Tabella 2.1. Inoltre i vincoli architetturali dei sottosistemi sono rispettati.

3.4 Analisi LOPA 3.B – dopo l'applicazione delle misure di prevenzione

Viene ripetuta l'analisi LOPA, implementata con il livello di protezione offerto dal sistema strumentato di sicurezza per il monitoraggio e controllo dell'atmosfera sotto ossigenata.

3.4.1 Foglio di lavoro LOPA 3.B – Dopo l'applicazione delle misure di prevenzione

1	2	3	4	5	6	7	8	9	10			11	12		13
ID/Rif. pericolo	Descrizione zona	Descrizione evento (pericolo)	Conseguenze	Categoria di gravità	Massimo rischio tollerabile	Causa scatenante	Frequenza della causa scatenante	Probabilità del verificarsi delle conseguenze	Livelli di protezione indipendenti			Frequenza delle conseguenze	Sistema relativo alla sicurezza (SrS)		Commenti
									Sistema BPCS	Segnale visivo-allarme acustico-blocco azoto	Mitigazione aggiuntiva: livelli di presidio		PFD richiesta	SIL richiesto	
					(/anno)		(/anno)					(/anno)			
[a]	[b]	[c]	[d]	[e]	[f]	[g]	[h]	[i]	[l]	[m]	[n]	[o]	[p]	[q]	[r]
101	Celle di conservazione della frutta in *atmosfera controllata* (AC)	Accesso di un lavoratore nella cella in regime di AC	Possibile incedente mortale per asfissia	P4	1,00E-04	Errore del lavoratore	1,20E-02	1	1	3,37E-02	0,16	6,47E-05	Nessuna	Nessuno	[h] La frequenza di presenza alla zona di ingresso alle celle è considerata mensile (n. 12 all'anno) [i] Dato il bassissimo tenore di ossigeno si considera il 100% di probabilità di morte [l] Il sistema base di controllo del processo non ha influenza sull'evento [n] Si considera l'area occupata 4 ore al giorno
102	Celle di conservazione della frutta in atmosfera normale (ambiente bonificato)	Accesso di più lavoratori nella cella bonificata con possibile insufflazione involontaria di azoto	Possibile incedente mortale per asfissia	P5	1,00E-05	Guasto, anomalia nel processo	1,60E-02	0,5	0,1	3,37E-02	0,33	8,90E-06	Nessuna	Nessuno	[h] Guasto/perdita in chiusura della valvola automatica di erogazione azoto considerata in servizio gravoso [i] La probabilità che i lavoratori si trovino in una zona a bassa concentrazione di ossigeno nella cella bonificata e con rilevatori di O2 in funzione è stimata del 50% [l] Si considera che il sistema base di controllo del processo possa evitare 9 eventi (erogazione intempestiva di azoto) su 10 [n] Si considera l'area occupata 8 ore al giorno