POLITECNICO DI MILANO

Scuola di Ingegneria Industriale e dell'Informazione

Corso di Laurea Magistrale in

Ingegneria della Prevenzione e della Sicurezza nell'Industria di Processo

Determinazione di una procedura per la valutazione del Livello di Protezione degli Apparecchi (EPL) per lo sviluppo di apparecchi d'illuminazione Ex costituiti da dispositivi Power LED

Relatore: **Chiar.mo prof. Roberto Faranda**

Correlatore: **Ing. Kim Fumagalli, Ph.D.**

Tesi di Laurea
Magistrale di:
Lorenzo Farnè
Matr. 818647

Anno Accademico 2014-2015

Indice

Indice delle figure

Indice delle tabelle

Abstract

La tecnologia LED, grazie alle sue caratteristiche di lunga durata, alta efficienza e basso consumo, viene utilizzata da diversi anni in molti settori industriali, tra i quali quello delle apparecchiature antideflagranti per atmosfere ATEX. La mancanza di conoscenza degli effetti dei possibili guasti dei LED in presenza di atmosfera esplosiva pone forti limitazioni all'impiego di queste apparecchiature, tanto che in molte aree pericolose è richiesto l'uso di involucri antideflagranti appositi molto costosi.

Con l'idea di superare tali limiti e permettere un utilizzo diretto della tecnologia LED, tre anni fa è nato uno studio sui modi di guasto del LED e sui loro effetti in ambito ATEX. Con questo nuovo lavoro si è costruita una procedura in grado di valutare l'affidabilità del LED ed il suo grado di sicurezza, indicato dall'indice EPL ("*Equipment Protection Level*"), così da verificare l'applicabilità di questa tecnologia anche nei contesti finora esclusi. Identificata la "*Zona 1*" come la categoria di aree pericolose in cui lavorare, si è ricorso all'analisi e alla combinazione di diverse norme per l'individuazione dell'EPL. Sfruttando la metodologia dell'approccio SIL ("*Safety Integrity Level*") descritta nelle norme della serie IEC/EN 61508, e combinando le norme CEI EN 50495:2010 e IEC/EN 61508, la procedura permette di calcolare il livello di protezione necessario partendo dalla conoscenza dei modi e dei tassi di guasto del LED.

Il prossimo traguardo sarà quello di predisporre una campagna di prove sperimentali ad hoc che tengano conto dei diversi modi di guasto del LED e dell'interazione con le atmosfere ATEX, così da ottenere i tassi di guasto richiesti e procedere nella valutazione dell'affidabilità del LED. Dati affidabilistici riguardanti i LED sono limitati e spesso mancanti, tuttavia sono state fatte alcune osservazioni sfruttando dei valori di probabilità di fallimento tratti da documenti Philips Lumileds. Questi dati, seppur estremamente generici, hanno dato riscontri positivi ed incoraggianti sull'affidabilità dei LED.

Introduzione

La richiesta di sistemi sempre più efficienti spinge il mondo industriale verso la ricerca e l'innovazione tecnologica. Le sorgenti luminose LED ne sono uno degli esempi più lampanti. Nell'ultimo decennio l'utilizzo di questi dispositivi è cresciuto in maniera esponenziale grazie alla loro efficienza, la modularità, i bassi consumi ed un prezzo sempre più competitivo e ha interessato molti settori, fra cui quello delle apparecchiature antideflagranti per atmosfere potenzialmente esplosive.

La pericolosità di queste aree a rischio d'esplosione, conosciute con l'acronimo "*ATEX*" ("*ATmosphere EXplosive*"), richiede severe valutazioni e apparecchiature apposite che non siano in grado di innescare le miscele di gas o polveri esplodibili eventualmente presenti nell'atmosfera.

Poiché la tecnologia LED e la sua applicazione in ambiti così particolari sono relativamente recenti, non tutti i suoi aspetti sono ancora noti. Ad oggi gli effetti dei guasti di un apparecchio LED sulla sicurezza, in relazione alla presenza di atmosfere pericolose, sono stati affrontati solo parzialmente. La mancanza di informazioni impone forti limiti in termini di potenza elettrica installabile, o in alternativa richiede l'utilizzo di pesanti custodie metalliche apposite che siano in grado di contenere un'eventuale esplosione innescata dall'apparato elettrico. In questo modo la sicurezza viene posta solo a carico dell'involucro. In conseguenza di ciò non solo si impedisce lo sfruttamento delle piene potenzialità del LED, ma si vanno ad incrementare i costi di produzione, installazione, manutenzione e decommissionamento dell'apparecchio. Solo con l'ultima edizione pubblicata nel 2015 della norma IEC/EN 60079-7 il LED è stato accettato come dispositivo "a *sicurezza aumentata*", in grado cioè di garantire il livello minimo di sicurezza richiesto e permettendone un'installazione in involucri più leggeri ed economici, ma tutto ciò limitatamente alle zone classificate come meno pericolose. Per tali motivi e con la convinzione che la tecnologia LED abbia ancora molto da offrire, è nato tre anni fa uno studio che intende affrontare nella sua interezza il problema dell'integrità della sicurezza dei LED.

I primi risultati sono culminati con la stesura della prima tesi di laurea, dove si sono analizzate le diverse tipologie di LED esistenti, le loro caratteristiche e i loro modi di guasto. Si è indagato sugli effetti teorici che i guasti possono comportare se associati alle atmosfere potenzialmente esplosive, ottenendo dei risultati incoraggianti. Con questo nuovo lavoro si è fatto un altro passo avanti, strutturando un approccio quantitativo che sia in grado di calcolare il livello di sicurezza del LED basandosi sui modi e sui tassi di guasto, rispettando al contempo i requisiti imposti dalle normative vigenti. Seguendo l'approccio proposto, sarà possibile dimostrare, a seguito di test di laboratorio, se la tecnologia LED è davvero sicura e applicabile laddove oggi non è ancora possibile.

Capitolo 1
L’uso dei LED nelle atmosfere potenzialmente esplosive

1.1 LE ATMOSFERE POTENZIALMENTE ESPLOSIVE

Molti settori industriali utilizzano quotidianamente sostanze combustibili in grado di generare gas, vapori, nebbie o polveri che se non controllate ed innescate possono portare, in determinate condizioni, ad una esplosione. Quelle che si vengono a creare sono le cosiddette zone “*ATEX*”, ovvero delle atmosfere potenzialmente esplosive che richiedono l’uso di processi, tecnologie ed accorgimenti tali da ridurre la possibilità di un innesco o limitare la propagazione e gli effetti dell’esplosione.

1.1.1 Incendi ed esplosioni

Esistono diversi tipi di esplosione, ma per quanto riguarda miscele di gas, vapori o polveri esse derivano essenzialmente da una reazione di combustione sufficientemente rapida da provocare un’onda d’urto e non solo un semplice incendio. Un’esplosione è infatti definita come “*un rilascio di una certa quantità di energia in un tempo sufficientemente breve e in un volume sufficientemente ridotto tale da generare un’onda di pressione di entità finita che si allontana dal punto di rilascio e che può essere udita*” [1].

La combustione di un gas combustibile richiede anzitutto la presenza di un comburente (solitamente ossigeno atmosferico) e di un innesco con energia sufficientemente elevata, rappresentato nel caso di apparecchiatura elettrica dal calore emesso da superfici a temperature eccessive o dalla generazione di scintille o archi elettrici. Tale concetto viene riassunto col “*triangolo del fuoco*” (fig. 1.1):

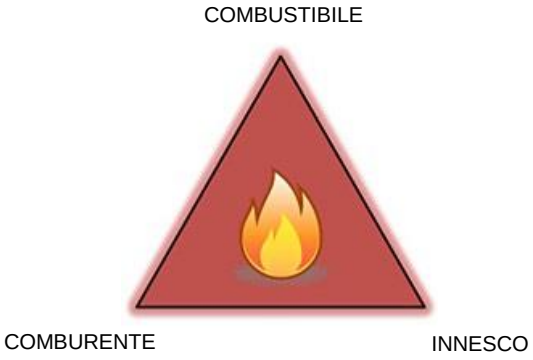

Figura 1.1 - Rappresentazione del "triangolo del fuoco" che indica i tre fattori necessari alla generazione di una reazione di combustione e basilari per un'esplosione di gas e vapori combustibili.

La concentrazione del combustibile nell'atmosfera rispetto al comburente e ad eventuali inerti deve rientrare in un intervallo definito di infiammabilità. Una concentrazione troppo alta (miscela ricca, satura) o troppo bassa (miscela povera) non permette la propagazione della reazione di ossidazione (fig. 1.2). I limiti di infiammabilità definiscono di conseguenza anche i limiti di esplosività [2].

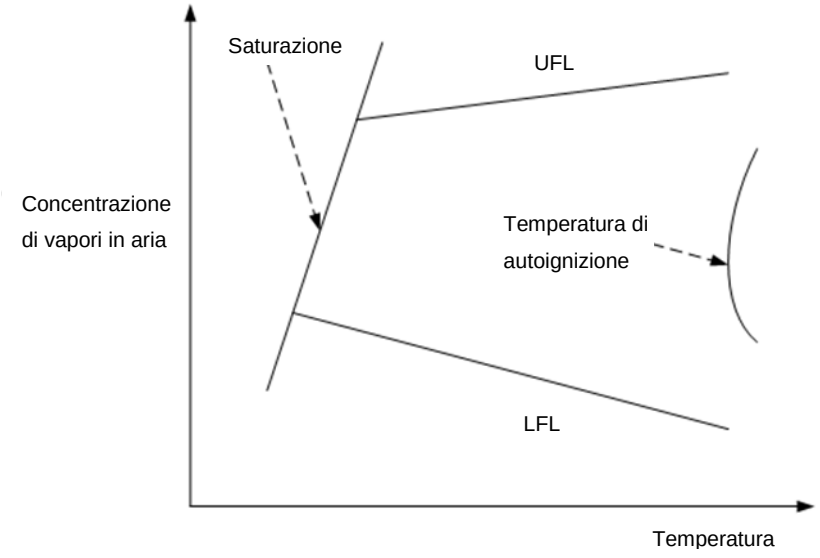

Figura 1.2 - Rappresentazione generica del campo d'infiammabilità di un combustibile al variare della temperatura.

Per quanto riguarda le polveri occorre fare un discorso a parte. Oltre al combustibile, il comburente e l'innesco, sono fattori indispensabili anche una sufficiente dispersione della polvere ed un suo confinamento. Affinché una polvere possa esplodere è infatti necessario che le particelle siano disperse nell'atmosfera da

un'adeguata turbolenza così da formare una nube ben miscelata con il comburente [2]. L'insieme costituisce il "*pentagono dell'esplosione*" (fig. 1.3). È bene ricordare che la congestione ambientale è comunque un parametro che può incidere anche sulle esplosioni di miscele gassose, agendo sulla turbolenza e potendo trasformare una deflagrazione in una ben più potente detonazione.

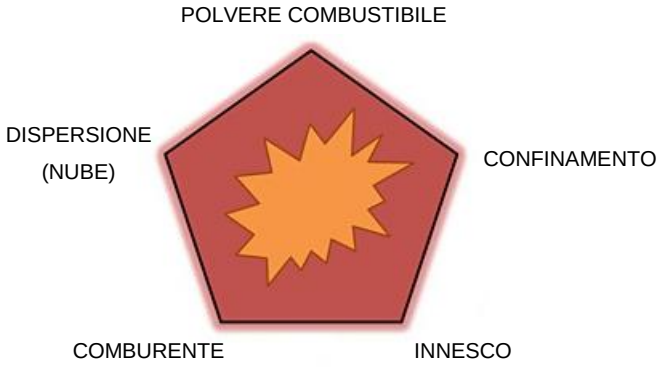

Figura 1.3 - Rappresentazione del "pentagono dell'esplosione da polveri", che raggruppa i cinque fattori necessari alla generazione di un'esplosione da polvere combustibile.

1.1.2 Classificazione delle aree e delle apparecchiature

Alla base del sistema normativo riguardante ogni apparecchiatura elettrica destinata ad un utilizzo in atmosfere potenzialmente esplosive vi è lo schema di certificazione IECEx 60079[1]. Esso è costituito da una serie di norme tecniche specifiche basate sugli standard della "*International Electrotechnical Commission*" ed è stato sviluppato per permettere un'armonizzazione delle procedure di certificazione tra Paesi diversi. In ambito europeo sono state emanate due direttive, la 99/92/CE riferita alla salute e alla sicurezza dei lavoratori e la 2014/34/UE (ex 94/9/CE) riferita ai prodotti e ai sistemi di protezione[2] venduti sul territorio europeo. Il loro scopo è fornire i "*requisiti essenziali di sicurezza*" in modo tale da garantire l'adeguata protezione ai soggetti interessati e al contempo favorire e regolare la

[1] Si fa riferimento ai Paesi UE ed extra UE partecipanti nell'IEC, principale organizzazione nell'ambito dell'elettrotecnica di rilevanza mondiale. Esistono comunque altri importanti standard come quelli di USA e Canada.

[2] La Direttiva ATEX si riferisce a tutti i prodotti destinati all'uso in atmosfere esplosive, quindi anche materiale non elettrico.

vendita di materiale Ex nel mercato UE. Le direttive ATEX non forniscono specifiche tecniche e si affiancano alle norme vigenti.

Il sistema IEC prevede una classificazione delle aree a rischio esplosivo e delle apparecchiature che dovranno operarvi.

Escludendo le atmosfere relative agli impianti minerari con presenza di gas grisù (per cui data la pericolosità elevata vi sono delle specifiche apposite), le aree pericolose vengono distinte tra atmosfere esplosive "*gassose"* e "*polverose"* e suddivise in tre "*Zone*", ciascuna in funzione delle probabilità di formazione e di persistenza dell'atmosfera esplosiva (tab. 1.1).

Tabella 1.1 – Classificazione in Zone delle aree a rischio esplosivo secondo lo schema IEC.

Atmosfera gassosa	**Atmosfera polverosa**	**Descrizione**
ZONA 0	ZONA 20	Area in cui l'atmosfera esplosiva è presente continuamente o frequentemente (>1000 h/anno)
ZONA 1	ZONA 21	Area in cui è probabile la presenza dell'atmosfera esplosiva durante le normali attività (10-1000 h/anno)
ZONA 2	ZONA 22	Area in cui vi è bassa probabilità di presenza dell'atmosfera esplosiva durante la normale attività (<10 h/anno)

La classificazione delle apparecchiature riguarda diversi aspetti. Si distinguono tre "*Gruppi*" a seconda della sostanza che costituisce l'atmosfera esplosiva in cui l'apparecchio dovrà operare:

- Gruppo I, per applicazioni in miniere con presenza di gas grisuosi;
- Gruppo II, per applicazioni in presenza di miscele di gas, nebbie e vapori;
- Gruppo III, per applicazioni in presenza di polveri.

Sono distinte sei "*Classi di temperatura*", relative alla temperatura superficiale massima ammissibile dell'apparecchio affinché non vi sia l'innesco dell'atmosfera (tab. 1.2). Questa suddivisione è valida solo per le atmosfere gassose, poiché nel caso di polveri occorre considerare due temperature di innesco caratteristiche, quali la

temperatura d'innesco della nube di polvere e la temperatura d'innesco dello strato depositato.

Tabella 1.2 – Classi di temperatura delle apparecchiature per atmosfere gassose e relativa temperatura superficiale massima ammissibile.

Classe di temperatura	**Massima temperatura superficiale**
T1	450°C
T2	300°C
T3	200°C
T4	135°C
T5	100°C
T6	85°C

L'ultimo aspetto riguardo la classificazione delle apparecchiature si concentra sulla costruzione dell'apparecchio e sulla sua capacità di non diventare una fonte d'innesco dell'atmosfera pericolosa. Sono definiti tre diversi "*livelli di protezione*" ("*Equipment Protection Level*", EPL):

- EPL a: apparecchio con un livello di protezione molto alto, che non sia fonte di innesco in condizioni normali o a seguito di guasti anche rari;
- EPL b: apparecchio con un livello di protezione alto, che non sia fonte di innesco in condizioni normali o a seguito di guasti prevedibili;
- EPL c: apparecchio con un livello di protezione aumentato, che non sia fonte di innesco in condizioni normali.

La Direttiva ATEX basa la classificazione delle aree pericolose sul sistema di classificazione IEC. Invece per quanto riguarda le apparecchiature, distingue due gruppi in relazione alla tipologia di atmosfera esplosiva ("*miniera*" con grisou e "*superficie*" con gas e polveri), suddivisi a loro volta in "*Categorie*" relative al funzionamento del macchinario e alla protezione contro l'innesco in presenza dell'atmosfera esplosiva (tab. 1.3).

Tabella 1.3 – Suddivisione delle apparecchiature in Categorie secondo la Direttiva ATEX.

Gruppo	Categoria	Protezione	Funzionamento
I *Miniere* (grisou)	M1	Due mezzi di protezione indipendenti o sicurezza garantita anche qualora si manifestino due guasti indipendenti	Apparecchi alimentati e in funzione in presenza di atmosfera esplosiva
	M2	Protezione adatta al funzionamento normale e in condizioni gravose	In presenza di atmosfera potenzialmente esplosiva, l'alimentazione di energia di questi apparecchi deve essere interrotta
II *Superficie* (gas e polveri)	1	Due mezzi di protezione indipendente o sicurezza garantita anche qualora si manifestino due guasti indipendenti	Apparecchi alimentati e in funzione in presenza di atmosfera esplosiva
	2	Protezione adatta al funzionamento normale e in caso di disturbi frequenti	Apparecchi alimentati e in funzione in presenza di tmosfera esplosiva
	3	Protezione adatta al funzionamento normale	Apparecchi alimentati e in funzione in presenza di atmosfera esplosiva

Complessivamente è possibile riassumere i diversi criteri di classificazione confrontando le indicazioni degli standard IEC e della Direttiva ATEX (tab. 1.4)

Tabella 1.4 - Correlazione tra Gruppi,Categorie, Zone ed EPL.

Gruppo	Categoria *(ATEX)*	Zona		EPL *(IEC)*		Livello di protezione	Presenza di atmosfera pericolosa
		G	D	G	D		
I (miniere)	M1	…		Ma		Molto elevato	Presente
	M2	…		Mb		Elevato	Probabile
II (superficie)	1	0	20	Ga	Da	Molto elevato	> 1000 h/anno
	2	1	21	Gb	Db	Elevato	10 < h/anno < 1000
	3	2	22	Gc	Dc	Normale	< 10 h/anno

Nella Direttiva ATEX si fa riferimento alle Categorie per la distinzione dei prodotti anziché all'Equipment Protection Level, ma da un punto di vista puramente pratico Categorie ed EPL sono equivalenti ed intercambiabili al fine di una classificazione di un dispositivo.

1.2 FUNZIONALITÀ E VANTAGGI DELLA TECNOLOGIA LED

I diodi ad emissione luminosa, o LED, sono dei dispositivi optoelettronici funzionanti tramite corrente continua, costruiti sfruttando diversi materiali semiconduttori, in grado di generare della radiazione elettromagnetica nell'intorno dello spettro del visibile. La struttura di un LED (fig. 1.4) è essenzialmente composta da:

- una giunzione p-n, costituita dall'assieme dei materiali semiconduttori a formare un chip;
- un supporto per il chip, con funzione di sostegno, di riflessione della luce e nel caso di LED di potenza congiunto ad un dissipatore di calore;
- due contatti elettrici costituenti l'anodo e il catodo;
- un filo d'oro per il collegamento elettrico tra chip e anodo, sottile così da non limitare l'emissione luminosa;
- un involucro protettivo di materiale epossidico o siliconico.

In base ai tipi di materiali usati si coprono diverse zone dello spettro visibile e quindi diverse colorazioni, mentre per la generazione di luce bianca il metodo più usato si basa sull'aggiunta di uno strato di polvere fosforica capace di convertire la luce emessa (di solito blu) in bianca.

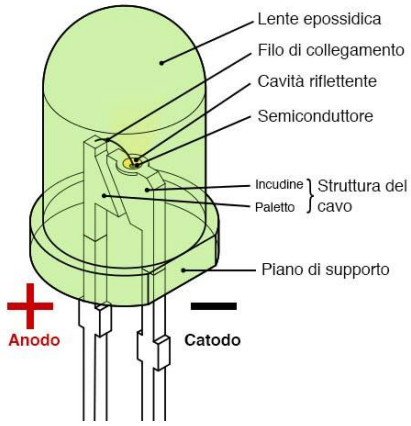

Figura 1.4 – Struttura elementare di un comune LED.

In origine l'emissione luminosa di un LED era molto ridotta e questi dispositivi trovavano applicazione come spie luminose. Il progresso tecnologico ha portato nel corso degli anni ad un incremento esponenziale delle capacità in termini di efficienza e flusso luminoso emesso, fino a rendere i LED delle valide alternative alle normali sorgenti d'illuminazione. L'aumento di flusso luminoso emesso è andato di pari passo con la necessità di smaltire il calore prodotto dal chip. La giunzione è in grado di raggiungere temperature anche superiori al centinaio di gradi, ma ciò va a limitare le prestazioni del dispositivo fino a danneggiarlo seriamente. La struttura stessa dei diodi ha avuto un'evoluzione notevole, passando dalla "Through Hole Technology" THT alla "Surface Mounted Technology" SMD, più efficiente e che ha permesso lo sviluppo di dissipatori di calore direttamente alla base del LED (fig. 1.5) [3].

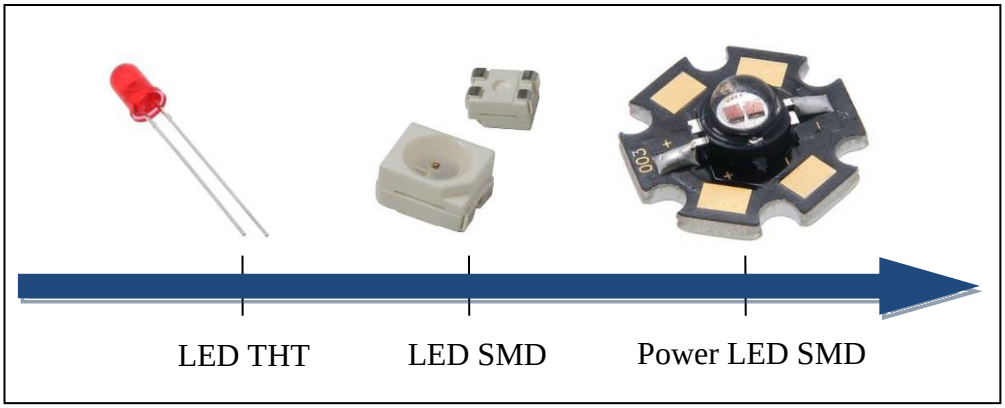

Figura 1.5 – Evoluzione della tecnologia LED, dalla più obsoleta THT fino alla SMD, che ha permesso lo sviluppo dei LED di potenza.

Il miglioramento più recente ha riguardato la conformazione del chip interno del diodo: precedentemente la giunzione era collegata alla base al catodo e superiormente all'anodo tramite l'ausilio di un filamento d'oro. La tecnologia "*Flip Chip*" ha consentito di ribaltare i collegamenti elettrici modificando la struttura del chip, così da consentire un contatto elettrico alla base per entrambi i terminali. Questa configurazione permette di raggiungere efficienze migliori ma soprattutto garantisce un incremento notevole della resistenza meccanica della struttura complessiva. Inoltre, in assenza del delicato filamento d'oro, è stata annullata la possibilità di avere un guasto per circuito aperto all'interno del LED (fig. 1.6) [4].

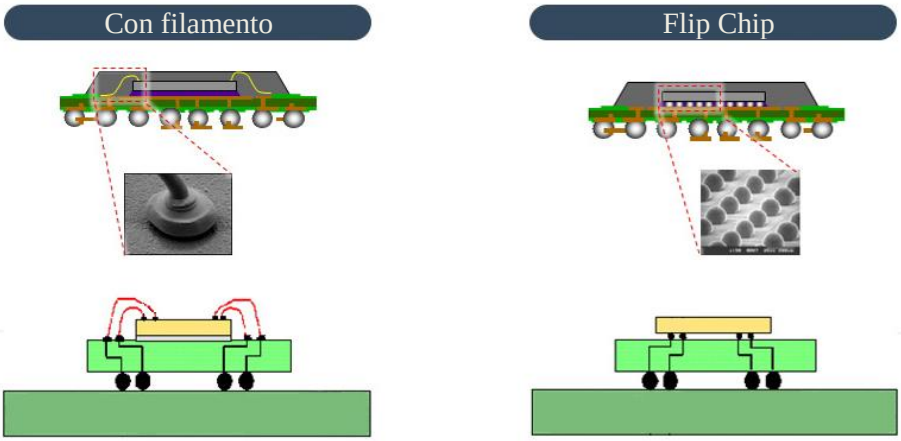

Figura 1.6 – Schematizzazione della struttura di un LED a filamento e di un LED Flip Chip.

Rispetto alle tradizionali sorgenti d'illuminazione i LED presentano i seguenti vantaggi e svantaggi [3] [4] [5] [6]:

- *Vantaggi:*
  - efficienza luminosa molto elevata, solitamente tra i 100lm/W e 160lm/W per singolo LED, che si traduce in un basso consumo energetico;
  - vita utile elevata, commercialmente indicata tra le 50kh e le 60kh ma virtualmente anche fino a 100kh;
  - alimentazione in corrente continua con tensioni di qualche Volt e correnti tra i 350mA e 1,5A per singolo LED;
  - robustezza della struttura;

- dimming tramite controllo "*PWM"* ("*Pulse With Modulation*");
- accensione istantanea senza circuiti ausiliari e insensibilità alle continue commutazioni di accensione/spegnimento;
- dimensioni estremamente ridotte e modularità;
- luce direzionale;
- luce colorata senza filtri;
- assenza di mercurio, gas, raggi infrarossi o UV (salvo che nei LED appositi).

- *Svantaggi*:
  - flusso luminoso limitato per singolo LED rispetto a sorgenti tradizionali;
  - costo per lumen installato relativamente elevato, anche se negli ultimi anni la diffusione di questa tecnologia sta facendo diminuire notevolmente i costi.

1.3 LA SCELTA DEL MODO DI PROTEZIONE EX e

Le apparecchiature elettriche destinate ad un uso in un'atmosfera potenzialmente esplosiva necessitano di adeguati sistemi di protezione al fine di non innescare le miscele di gas o le polveri esplodibili [7]. I modi di protezione possono agire secondo diverse strategie:

- Contenimento: il materiale elettrico in grado di innescare la miscela è contenuto in un involucro stagno in grado di resistere alla pressione dell'eventuale esplosione e impedire la propagazione della fiamma;
- Prevenzione: il materiale elettrico è studiato appositamente per non essere in grado di innescare l'atmosfera, limitandone la potenza o la capacità di generare scintille, archi elettrici e sovratemperature;
- Segregazione: vengono utilizzati materiali riempitivi per inglobare il materiale elettrico o una sovrapressione interna all'involucro che impedisce l'ingresso di ossigeno, gas o polveri.

I principali modi di protezione sono riassunti in tabella 1.5.

Tabella 1.5 – Principali modi di protezione e relative Zone di applicazione.

Metodo	**Modo di protezione**	**Descrizione**	**Zone di applicazione**
Contenimento	Ex da Ex db Ex dc	Custodia a prova di esplosione.	0 – 20 1 – 21 2 – 22
Prevenzione	Ex eb Ex ec	Sicurezza aumentata. Nessun arco elettrico o sovratemperatura in condizioni di normale funzionamento.	1 – 21 2 – 22
	Ex ia Ex ib Ex ic	Sicurezza intrinseca. Viene limitata l'energia elettrica del dispositivo.	0 – 20 1 – 21 2 – 22
Segregazione	Ex ma Ex mb Ex mc	Incapsulamento tramite resina.	0 – 20 1 – 21 2 – 22
	Ex p	Sovrappressione interna che impedisce l'ingresso della miscela.	1 – 21
	Ex o	Immersione in olio.	1 – 21
	Ex q	Sotto sabbia.	1 – 21
	Ex n	Semplice. Apparecchiature non scintillanti per aree a bassa probabilità di presenza di atmosfere pericolose.	2 – 22

Per gli apparecchi d'illuminazione, i modi di protezione utilizzati sono "*Ex d*", "*Ex e*", "*Ex i*" ed "*Ex m*" poiché sono gli unici compatibili con la struttura e la funzionalità di una sorgente luminosa. I sistemi Power LED per l'illuminazione vengono già utilizzati da diversi anni nelle apparecchiature Ex, ma risentono di alcune limitazioni. Dipendentemente dalla Zona, è richiesto un EPL c, b o a all'apparecchio, cioè un livello di protezione crescente con la pericolosità dell'area. La lettera aggiuntiva per i modi di protezione Ex d, Ex e, Ex i, ed Ex m permette di distinguere l'EPL richiesto.

Per quanto riguarda specificatamente i LED, in Zona 0 vengono normalmente impiegati in torce portatili e da elmetto con modo di protezione Ex ia, cioè con forte limitazione in potenza poiché è richiesta una protezione particolarmente alta. In Zona 1 viene richiesta una protezione elevata ed è possibile adottare modi di protezione Ex ib, Ex db ed Ex mb. Il primo modo di protezione agisce analogamente

a quanto già visto ma con delle specifiche meno restrittive. Il modo di protezione Ex d è normalmente il più usato per le alte potenze installabili. Infatti l'apparecchiatura elettrica non risente di particolari limiti, poiché viene contenuta in speciali custodie metalliche stagne, molto spesse e pesanti che garantiscono il contenimento dell'eventuale esplosione (fig. 1.7).

Figura 1.7 – Apparecchio d'illuminazione LED con modo di protezione Ex d.

Il modo Ex m prevede invece l'incapsulamento dei LED tramite resine trasparenti che isolano il materiale elettrico dall'atmosfera. Se da un lato questo sistema permette l'uso di custodie più leggere, dall'altro richiede un accurato isolamento dei componenti elettrici ed influisce negativamente sull'emissione luminosa e sullo smaltimento di calore, ponendo dei limiti sulle potenze raggiungibili dal singolo apparecchio.

In Zona 2, i modi di protezione implementabili sono Ex dc, Ex ic, ed Ex mc, a cui si aggiunge il modo Ex ec. Questo richiede che sia il materiale elettrico stesso a garantire la sicurezza necessaria, non innescando l'atmosfera esplosiva attraverso archi elettrici, scintille o sovratemperature superficiali. Di conseguenza non occorrono soluzioni aggiuntive e la custodia utilizzabile è più leggera ed economica rispetto alle custodie Ex d (fig. 1.8).

I diversi modi in cui un LED può fallire sono stati studiati da tempo, ma la pericolosità di tali guasti in relazione alle atmosfere esplosive non è nota. Per questo motivo l'apparecchiatura LED non può essere installata sfruttando il modo di protezione Ex ea o Ex eb, ma solo tramite il modo Ex ec in Zona 2, la meno pericolosa, poiché la sicurezza richiesta al dispositivo è sufficientemente bassa da

non necessitare di accorgimenti particolari. In tutti gli altri casi occorrerà necessariamente utilizzare gli altri modi di protezione.

Figura 1.8 – Apparecchio d'illuminazione LED con modo di protezione Ex ec.

Volendo considerare apparecchiature non limitate in potenza, è chiaro come la scelta si restringa al modo di protezione Ex d. Gli svantaggi di un simile modo di protezione ricadono essenzialmente sull'involucro, che risulta molto costoso, pesante e che influisce sull'efficienza dell'apparecchiatura d'illuminazione, limitando il flusso luminoso a causa degli spessi vetri temperati utilizzati.
La volontà di utilizzare apparecchiatura Ex e deriva da importanti vantaggi rispetto al modo di protezione Ex d [6]:

- custodie molto più sottili e leggere, di alluminio o materiale plastico;
- costi dei materiali e d'installazione contenuti;
- installabilità e manutenzione facilitate;
- interferenza col flusso luminoso emesso ridotta grazie all'uso di plastiche o vetri più sottili.

Capitolo 2

Norme

Per consentire un'analisi completa del problema, è stato necessario prendere visione di alcune norme [3] di riferimento concernenti diversi aspetti delle apparecchiature elettriche antideflagranti.

Il concetto di "*Equipment Protection Level*" (EPL) viene definito per la prima volta nella norma IEC/EN 60079-0 come un <<*livello di protezione assegnato all'apparecchiatura in base alla sua probabilità di diventare una sorgente d'innesco, distinguendo tra atmosfere esplosive gassose, polverose e atmosfere esplosive in miniera*>> (*IEC/EN 60079-0 Atmosfere esplosive Parte 0: prescrizioni generali, art. 3.26*) [8].

Come già introdotto nel primo capitolo, l'EPL è utilizzato per la selezione dei dispositivi elettrici Ex, sfruttando un approccio basato sul rischio d'innesco dell'atmosfera pericolosa. La descrizione del solo indice EPL ha però il limite di fornire un'informazione prettamente qualitativa, poiché si parla di "*protezione molto alta, alta o aumentata*". Per una sua corretta e completa valutazione è possibile ricorrere ad altre norme che, richiamando l'EPL, lo legano ad altri fattori quantitativi. Per lo studio dell'affidabilità del dispositivo Power LED, le informazioni che possono essere messe a disposizione sono una valutazione dei modi di guasto del dispositivo e i tassi di guasto ottenibili da test sperimentali. Con l'idea di sviluppare un metodo che possa legare tali informazioni all'EPL, si è giunti all'individuazione e all'analisi di queste norme:

- norme IEC/EN 61508 - 1, - 2, - 3, - 4, - 5, - 6, - 7: "*Sicurezza funzionale dei sistemi elettrici, elettronici ed elettronici programmabili per applicazioni di sicurezza*".

[3] Una norma è "*una specifica tecnica, adottata da un organismo di normazione riconosciuto, per applicazione ripetuta o continua, alla quale non è obbligatorio conformarsi*" [Regolamento UE 1025 del Parlamento Europeo e del Consiglio del 25 ottobre 2012]. E' dunque un riferimento volontario. Diversamente le Direttive Europee, le quali sono leggi emanate dal Parlamento e dal Consiglio Europeo, vengono recepite e trasformate in leggi nazionali dagli Stati membri, ed applicate in quanto tali.

- norma CEI EN 50495:2010: "*Dispositivi di sicurezza richiesti per il funzionamento sicuro degli apparecchi in relazione al rischio di esplosione*";
- norma IEC/EN 60079 - 28: "*Atmosfere esplosive – Parte 28: Protezione delle apparecchiature e dei sistemi di trasmissione che utilizzano radiazione ottica*".

La prima famiglia di norme descrive l'indice noto come "*SIL*" ("*Safety Integrity Level*") che, essendo legato ai tassi di guasto, è in grado di fornire informazioni riguardo l'affidabilità di un dispositivo di sicurezza associato ad un apparecchio [9]. Il SIL è un numero discreto, compreso tra 1 e 4, che fornisce un'appropriata scala di riduzione del rischio che un sistema di sicurezza elettrico/elettronico deve poter garantire. La seconda norma è riferita al controllo attivo delle sorgenti d'innesco in atmosfere Ex e fa riferimento proprio al SIL come elemento chiave per valutare la categoria di appartenenza di un apparecchio. L'ultima norma descrive diversi modi di protezione per apparecchiature ottiche e d'illuminazione in atmosfere esplosive, e uno di essi è basato proprio sul controllo attivo delle sorgenti d'innesco. Sfruttando l'approccio basato sul rischio descritto nelle norme IEC/EN 61508 permette di categorizzare ciascun apparecchio ottico con il corrispettivo indice EPL.

2.1 NORME IEC/EN 61508

In molti contesti industriali l'utilizzo di apparecchiature elettriche o elettroniche specifiche permette di garantire la sicurezza degli impianti e dei macchinari. Tali sistemi sono chiamati a svolgere funzioni di sicurezza, cioè azioni che consentano di ottenere un livello di rischio residuo inferiore a quello ritenuto tollerabile nel contesto in esame.

La logica alla base delle strategie di sicurezza adottate da questi sistemi viene descritta dalla famiglia di norme IEC/EN 61508, denominata "Sicurezza funzionale di sistemi Elettrici/Elettronici/Elettronici Programmabili". Si adotta un approccio basato sul rischio, fissando dei limiti minimi di integrità della sicurezza, cioè di probabilità che il sistema di sicurezza esegua le corrette funzioni sotto specifiche condizioni e in uno specifico periodo di tempo [10]. Obiettivo di queste Norme è fornire un metodo per la valutazione dei requisiti minimi necessari che garantiscano

l'attivazione delle suddette funzioni di sicurezza. Il Safety Integrity Level (SIL) è l'indice affidabilistico che racchiude tali requisiti. La Norma non è intesa a specificare l'esatto SIL per ogni funzione di sicurezza, da determinarsi in base al contesto, ma a fornire un quadro concettuale che ne permetta la valutazione.

I principi formulati nelle norme sono generali e applicabili a molti settori industriali (come industria di processo, trasporti, macchinari ecc…) tra cui anche quello delle apparecchiature elettriche antideflagranti. Formalmente riguardano dispositivi di sicurezza elettrici, elettronici ed elettronici programmabili (E/E/PE), ma viene chiaramente enunciato il concetto per cui tali linee guida possono dare indicazioni per sistemi di sicurezza basati su altre tecnologie, dovendo considerare tutte le possibili strategie di sicurezza e le loro combinazioni. La loro generalità è alla base dello scopo per cui sono state redatte: fornire uno strumento non solo per un corretto sviluppo del prodotto, ma anche come fondamento per la stesura di eventuali altre norme specifiche per ciascun campo di applicazione.

Le diverse parti che costituiscono la IEC/EN 61508 trattano argomenti peculiari, articolati come segue:

- Parte 1: Requisiti generali;
- Parte 2: Requisiti per dispositivi E/E/EP di sicurezza;
- Parte 3: Requisiti software;
- Parte 4: Definizioni e abbreviazioni;
- Parte 5: Esempi di metodi per la determinazione del Livello d'Integrità della Sicurezza;
- Parte 6: Linee guida per l'applicazione delle parti 2 e 3;
- Parte 7: Panoramica delle tecniche e delle misurazioni.

Macroscopicamente, il fascio di norme si snoda in due argomenti principali [11]:

- Definizioni del Sistema Qualità Aziendale rispetto alla Sicurezza Funzionale dei Prodotti (FSMS – Functional Safety Management System);
- Definizione e metodologia di calcolo dei valori PFD (Probability of Failure on Demand) o PFH (Probability of Failure per Hour), da cui è derivato il SIL (Safety Integrity Level).

L’analisi dei documenti si concentrerà sul secondo aspetto e verranno discusse solo le sezioni inerenti allo scopo del lavoro di Tesi.

2.1.1 IEC/EN 61508-1: Requisiti generali

L’obiettivo di questa prima norma è dare le nozioni generali basilari per permettere un corretto sviluppo di sistemi di sicurezza E/E/PE, in grado di assicurare la prevenzione e/o il controllo dei guasti del sistema.

Con particolare riferimento ai sistemi E/E/EP non particolarmente complessi, è possibile esentarsi dal rispetto di alcuni requisiti specificati dalla norma se esistono altri documenti settoriali che già implementano specifiche regolamentazioni o dove comunque l’esperienza maturata sul campo ne consente un’esenzione giustificata [12].

Al fine di dare un’idea globale di quali sono tutte le fasi che riguardano lo sviluppo di un dispositivo di sicurezza, viene costruito un “*ciclo di vita della sicurezza globale*”. Esso è da intendersi come linea guida per affrontare in modo sistematico tutte le attività necessarie a raggiungere l'integrità di sicurezza richiesta dal contesto, per le funzioni eseguite dai sistemi di sicurezza E/E/PE (fig. 2.1).

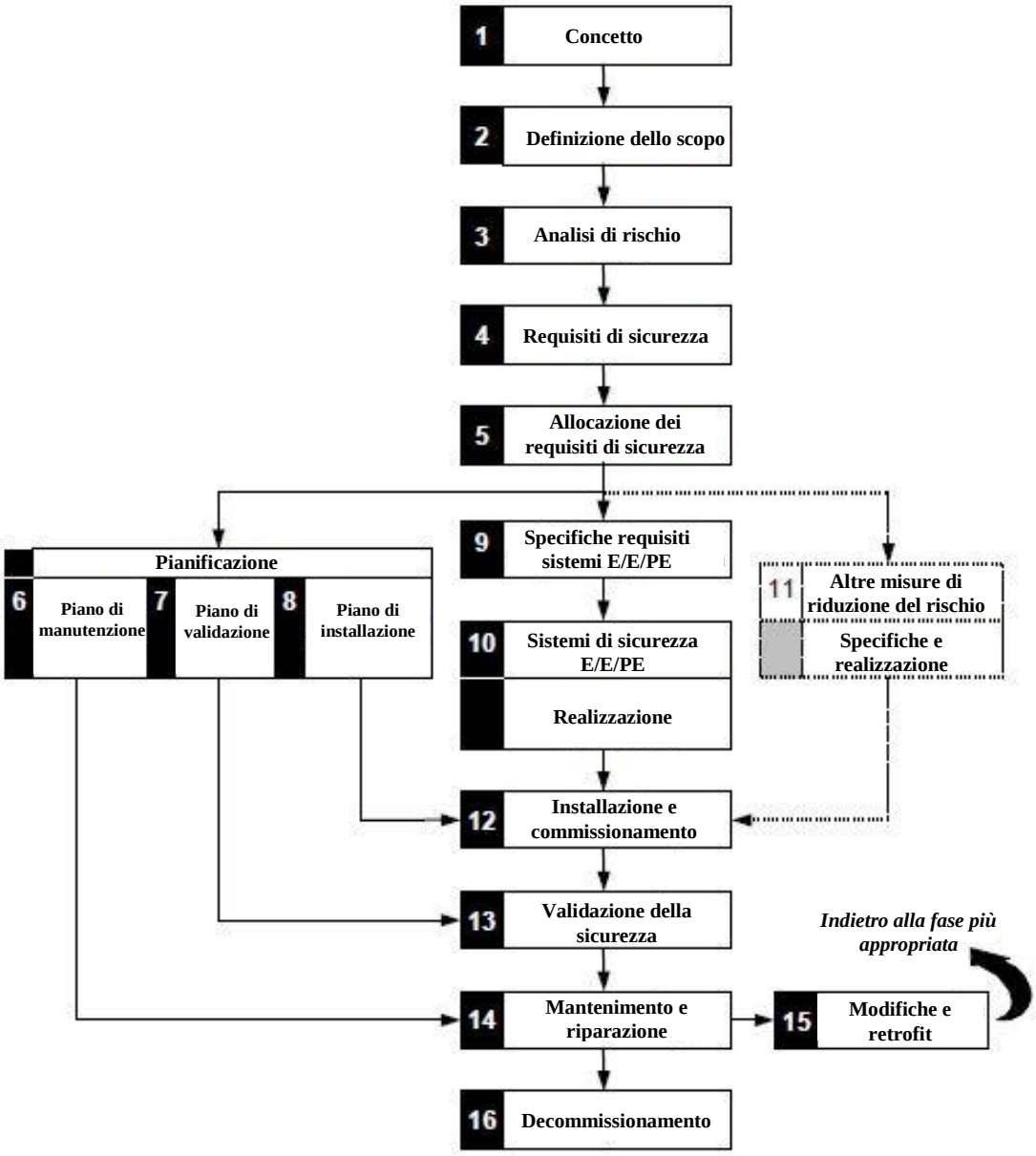

Figura 2.1 - Rappresentazione schematica globale delle varie fasi di vita di un sistema di sicurezza E/E/EP, dalla progettazione con l'analisi del contesto dove è richiesto il sistema di sicurezza, passando per la realizzazione, fino al decommissionamento.

Le prime fasi riguardano la contestualizzazione del problema e la definizione degli obiettivi di sicurezza voluti. Questo vuol dire raggiungere un livello di rischio tollerabile, in considerazione del fatto che il rischio zero non può mai essere ottenuto.

Viene effettuata un'analisi di rischio per valutare tutte le possibili fonti di guasti pericolosi, la loro influenza sul sistema e quindi la riduzione del rischio necessaria

per raggiungere gli obiettivi prefissati. Il rischio è quantificabile poiché funzione della frequenza, o meglio della probabilità di accadimento di un evento pericoloso, e della sua magnitudo, cioè l'intensità delle conseguenze che tale evento comporta. Dall'analisi di rischio condotta vengono dedotti i requisiti fondamentali che le funzioni di sicurezza dovranno possedere per garantire l'integrità della sicurezza stessa.

Le funzioni di sicurezza vengono allocate, cioè associate ad uno o più sistemi di sicurezza E/E/EP corrispondenti in base al contesto. L'insieme dei sistemi di sicurezza, tramite le loro funzioni, dovranno ridurre il rischio sotto il limite tollerabile. L'allocazione è eseguita in modo iterativo: se il livello di rischio tollerabile non è raggiunto, occorre modificare le specifiche ed i relativi sistemi ripetendo l'allocazione. Tutti i sistemi devono possedere la propria funzione di sicurezza e devono essere considerati anche gli effetti combinatori dei diversi sistemi e delle cause di guasto.

Normalmente è necessario fare una distinzione tra sistemi di sicurezza e sistemi di controllo di un EUC ("*Equipment Under Control*", qualsiasi dispositivo, apparato, macchinario o impianto usato nell'attività industriale sottoposto al controllo per il normale funzionamento [10]). Nel caso di applicazioni dove l'integrità della sicurezza richiesta sia molto alta, è a volte possibile ottenere sistemi di controllo particolarmente affidabili e con ratei di guasto molto bassi, così che essi possano essere catalogati come sistemi di sicurezza. Questa promozione può trovare luogo solo se il valore massimo di rateo di guasto pericoloso, per una singola funzione di controllo, è inferiore a 10^{-5} guasti per ora. I sistemi di controllo o di sicurezza sono considerati indipendenti se funzionalmente e tecnologicamente diversi, esenti da parti, funzionamento o alimentazione in comune e con probabilità di guasti simultanei sufficientemente bassa da essere irrisoria.

Per dare un indice quantitativo ai requisiti di integrità della sicurezza per una funzione di sicurezza, viene associato il Livello di Integrità della Sicurezza (SIL) in base a:

- probabilità media di guasto pericoloso alla richiesta della funzione di sicurezza (PFD_{avg}), nel caso di bassa richiesta d'intervento (frequenza non superiore ad una volta l'anno [13]);

- frequenza media di guasto pericoloso alla richiesta della funzione di sicurezza (PFH) [h^{-1}], nel caso di richiesta d'intervento alta (frequenza superiore ad una volta l'anno [13]) o continua (tab. 2.1).

Tabella 2.1 – Relazione tra SIL, probabilità media di guasto (PFD_{avg}) e frequenza media di guasto (PFH). Un SIL più alto è indice di una richiesta di affidabilità maggiore.

Livello di Integrità della Sicurezza	**Funzionamento in frequenza di richiesta bassa: PFD_{avg}**	**Funzionamento in frequenza di richiesta alta o continua: PFH**
SIL 4	da $\geq 10^{-5}$ a $< 10^{-4}$	da $\geq 10^{-9}$ a $< 10^{-8}$
SIL 3	da $\geq 10^{-4}$ a $< 10^{-3}$	da $\geq 10^{-8}$ a $< 10^{-7}$
SIL 2	da $\geq 10^{-3}$ a $< 10^{-2}$	da $\geq 10^{-7}$ a $< 10^{-6}$
SIL 1	da $\geq 10^{-2}$ a 10^{-1}	da $\geq 10^{-6}$ a 10^{-5}

Il livello SIL è quindi un indice dell'affidabilità minima richiesta per quel particolare sistema di sicurezza. Predire quantitativamente e con esattezza l'integrità della sicurezza di tutti gli aspetti di un sistema E/E/EP non è sempre possibile: l'uso di tecniche qualitative, misurazioni e giudizi devono essere fatti con l'adeguata precauzione del caso. Dal punto di vista dell'hardware, si ricorre a opportune tecniche quantitative di stima dell'affidabilità. Si richiama alle informazioni contenute nelle parti IEC/EN 61508-2 e IEC/EN 61508-5 della presente famiglia di norme.

Data la severità nel caso di applicazione del più alto SIL 4, la norma richiede una riconsiderazione per verificare se parametri come misure di sicurezza addizionali, probabilità e severità delle conseguenze possano essere modificati per evitare questo livello particolarmente restrittivo. Se confermato il livello 4, un'ulteriore valutazione del rischio deve essere eseguita considerando potenziali cause comuni di guasto tra sistemi E/E/EP e qualsiasi sistema il cui guasto richieda il loro intervento o altro sistema di sicurezza diverso.

Tralasciando la sezione riguardante le pianificazioni di manutenzione, installazione e validazione (box da 6 a 8 in fig. 2.1) si passa alle specifiche dei requisiti di sicurezza del sistema E/E/EP (box 9).

Grazie all'allocazione delle funzioni di sicurezza ai rispettivi sistemi, è possibile studiare e derivare i requisiti per la sicurezza specifici di ciascun sistema. Essi devono comprendere:

- una descrizione di tutte le funzioni di sicurezza necessarie al raggiungimento della sicurezza funzionale, specificando il modo in cui esse garantiscano la sicurezza ed i periodi di funzionamento;
- il tempo di risposta del sistema;
- indicazione di sistemi secondari, d'interfaccia e informazioni rilevanti al funzionamento del sistema E/E/EP;
- descrizione dei comportamenti del sistema nelle varie fasi (a riposo, in caso di richiesta d'intervento o guasto);

Oltre che alle indicazioni relative alle funzioni svolte dai sistemi E/E/EP, vi sono dei requisiti riguardo l'integrità stessa della sicurezza. Queste ulteriori specifiche devono contenere in particolare:

- il SIL di ciascuna funzione;
- il modo di intervento (richiesta bassa, alta, continua);
- il valore del duty cycle (ciclo di lavoro utile) ed il tempo di vita;
- gli estremi dei valori delle grandezze fisiche riferite alle condizioni ambientali che ci si aspetta il sistema di sicurezza incontrerà;
- limiti e vincoli influenti sulla realizzazione del sistema capaci di portare a guasti.

Per quanto concerne i requisiti della fase di realizzazione (box 10) si fa riferimento alla parte 2 della normativa. Le sezioni successive (box da 11 a 16) riguardano informazioni a corollario del sistema di sicurezza (installazione, validazione, manutenzione e decommissionamento) e non riguardano gli obiettivi della tesi.

2.1.2 IEC/EN 61508-2: Requisiti per dispositivi E/E/EP di sicurezza

La realizzazione di un sistema di sicurezza E/E/EP passa attraverso diverse fasi (fig. 2.2), principalmente:

- specifica dei requisiti di progettazione del sistema;
- sviluppo;
- integrazione con gli altri sistemi e/o programmi software
- installazione e validazione.

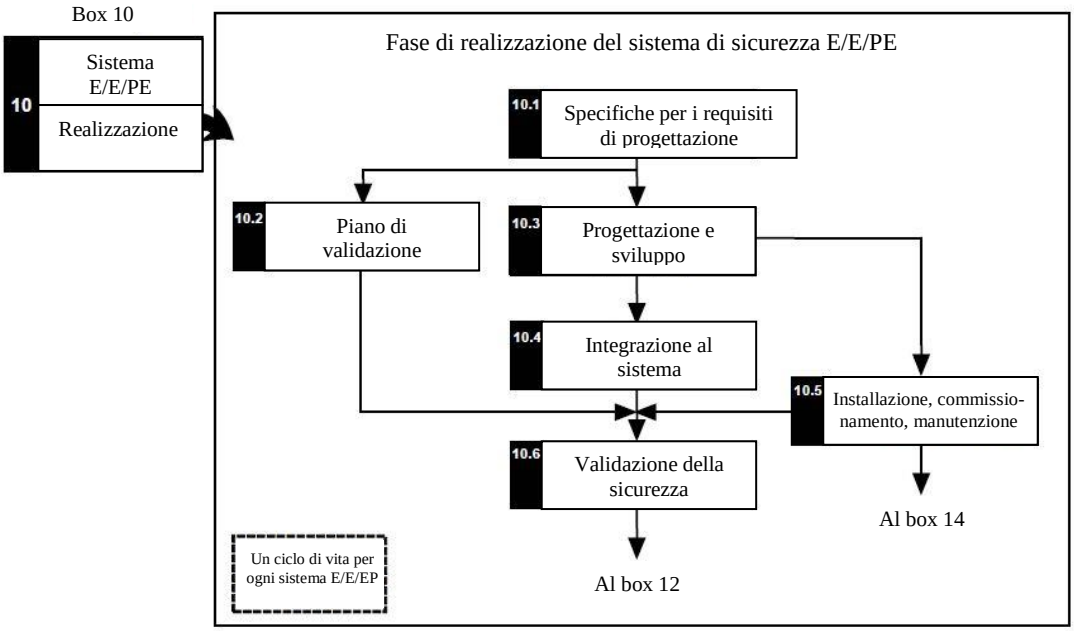

Figura 2.2 - Rappresentazione schematica delle fasi che stanno alla base della realizzazione del sistema di sicurezza (espansione del Box 10 di figura 2.1).

I requisiti di progettazione devono essere derivati dai requisiti di sicurezza del sistema ottenuti nella fase precedente. Essi comprendono principalmente informazioni riguardo:

- gli elementi costituenti il sistema o i sottosistemi;
- l'integrazione e l'interazione di essi;
- le interfacce;

- i modi di comportamento del sistema E/E/EP in particolare a seguito di guasto;
- i limiti e vincoli del sistema;
- l'architettura dei sottosistemi;
- i parametri affidabilistici necessari, come ad esempio la frequenza dei test di prova necessari per garantire una corretta valutazione dei guasti;
- le azioni da intraprendere nel caso di guasto rilevato;
- l'immunità elettromagnetica.

Le diverse funzioni di sicurezza implementate possono agire in modo dipendente tra di loro, portando a guasti comuni. Fintanto che non sia possibile dimostrare sufficiente indipendenza, le specifiche hardware del sistema vengono derivate basandosi sulla funzione con il valore SIL più elevato, in favore della sicurezza. Nel caso in cui la probabilità di guasto comune sia talmente bassa da essere trascurabile, è possibile accettare l'indipendenza tra le funzioni. Il suo valore deve essere molto più basso rispetto a quello di probabilità associato al SIL più alto tra quelli delle funzioni coinvolte.

La progettazione è basata sulla decomposizione del sistema di sicurezza in diversi sottosistemi. A progettazione iniziale compiuta, è necessaria un'analisi per verificare se un qualsiasi guasto al sistema E/E/EP possa portare ad una situazione pericolosa, o richieda l'intervento di altre misure di controllo. L'obiettivo è infatti quello di raggiungere il target di sicurezza richiesto dal contesto: se non raggiunto occorre modificare il progetto. Se una modifica non è possibile, è necessario introdurre misure aggiuntive così da raggiungere gli obiettivi di sicurezza prefissati.

2.1.2.1 Raggiungimento della capacità sistematica richiesta

Il primo parametro su cui agire è il numero di guasti "*sistematici*". Questi sono guasti attribuibili ad errori nelle fasi di progettazione o costruzione di un apparecchio. Al contrario, i guasti "*casuali*" fanno parte della vita del dispositivo e dipendono da invecchiamento e fattori esterni [14]. L'obiettivo primario nella progettazione dell'apparecchio è ridurre al minimo i guasti sistematici. La capacità sistematica di un dispositivo determina il numero di guasti sistematici che sono necessari

all'inattivazione della funzione di sicurezza. Viene indicata come SC N, dove N (numero di guasti) può assumere i valori 1, 2 o 3. Per un elemento dove un guasto sistematico porta al fallimento della funzione di sicurezza solo in combinazione con un secondo elemento con capacità sistematica SC N, la capacità sistematica complessiva può essere trattata come SC (N+1), a patto che vi sia sufficiente indipendenza tra i due elementi. Questa logica vale solo per due elementi: non è permesso raggiungere una SC (N+2) o superiore semplicemente aggiungendo successivamente ulteriori dispositivi con una certa capacità sistematica. L'indipendenza richiesta è necessaria affinché i diversi guasti non interferiscano tra loro col rischio di concatenarsi, diventando anziché un vantaggio un problema per la sicurezza. Tale indipendenza è dimostrata quando la probabilità di guasto da interferenza è molto più bassa rispetto a quella relativa al livello SIL corrente.

2.1.2.2 Vincoli strutturali all'integrità della sicurezza hardware

Trattati i guasti sistematici, occorre valutare le problematiche legate ai guasti casuali. È utile classificarli nei seguenti sottogruppi:

- **Sicuri / Pericolosi**: si ritengono "*pericolosi*" i guasti che causano l'inadempimento della funzione di sicurezza o la sua attivazione ad un set point più alto dell'originale, creando in questo modo una situazione pericolosa. Viceversa, sono guasti "*sicuri*" quei guasti che non interferiscono con la funzione di sicurezza o che se interferiscono abbassano il punto critico di attivazione, a favore della sicurezza;
- **Rilevati / Non rilevati**: se il guasto è in qualche modo individuabile (ad esempio tramite allarme) durante il normale funzionamento è considerato "*rilevato*", in caso contrario è "*non rilevato*";

Il valore SIL più alto rivendicabile dalla funzione di sicurezza è limitato dalla struttura stessa dell'hardware, che impone dei vincoli all'integrità della sicurezza. Questi vincoli possono essere verificati e soddisfatti in due modi possibili:

- Modo 1H: basato sui concetti di "*tolleranza al guasto dell'hardware*" (HFT) e di "*frazione di guasti sicuri*" (SFF);

- Modo 2H: basato su dati affidabilistici dei componenti ottenuti da "*feedback degli utilizzatori finali*", un "*livello di confidenza incrementato*" e "*tolleranza hardware al guasto*" (HFT) per specifici SIL.

In considerazione della tolleranza al guasto N:

- il numero minimo di guasti che portano alla perdita della funzione di sicurezza è N+1;
- quando un guasto porta direttamente ad uno o più guasti conseguenti, questi vengono considerati come un unico guasto;
- guasti con probabilità di accadimento molto più bassa rispetto a quella minima richiesta per l'integrità della sicurezza, possono essere esclusi.

Gli elementi di un sistema di sicurezza vengono classificati in due tipologie. Si rientra nella tipologia A se:

- i modi di guasto di tutti i componenti sono ben definibili;
- il comportamento sotto condizioni di guasto può essere completamente determinato;
- ci sono sufficienti dati che confermano i tassi di guasto per guasti pericolosi rilevati e non rilevati.

Si rientra nella tipologia B se:

- i modi di guasto di almeno un componente non sono ben definiti;
- il comportamento sotto condizioni di guasto non può essere completamente determinato;
- non ci sono sufficienti dati che confermano i tassi di guasto per guasti pericolosi rilevati e non rilevati.

Date le definizioni, in considerazione che il dispositivo sotto analisi è il Power LED, esso può essere catalogato come dispositivo di tipo A poiché il comportamento in caso di guasto può essere studiato accuratamente.

Si analizza per primo il Modo 1H.

Per determinare il massimo valore del Safety Integrity Level che un dispositivo di sicurezza può assumere, in considerazione della sua specifica funzione di sicurezza, è necessario seguire tale procedura:

- definire i sottosistemi che compongono il sistema di sicurezza;
- singolarmente per ciascun elemento di ogni sottosistema determinare la frazione di guasti sicuri (SFF). Nel caso di elementi ridondanti, la frazione di guasti sicuri può essere calcolata considerando la diagnostica disponibile (ad esempio comparando gli elementi ridondanti);
- per ciascun elemento considerare la SFF ottenuta e una tolleranza ai guasti pari a 0 per determinare il massimo SIL seguendo la tabella 2.2;
- nel caso di elementi combinati in serie, il massimo SIL ottenibile dal sottosistema è limitato dall'elemento con il minor SIL;
- nel caso di elementi in parallelo (più canali) è necessario analizzare prima ciascun canale (valutando gli eventuali elementi in serie che lo compongono come sopra), quindi selezionare il canale con SIL più alto;
- considerare ora il reale numero N di guasti tollerabili dal sottosistema, e spostandosi nella tabella ottenere il numero dell'indice SIL del sottosistema;
- il massimo SIL ottenibile dal sistema di sicurezza corrisponde al valore SIL più basso ottenuto tra tutti i sottosistemi.

Tabella 2.2 – Safety Integrity Level massimo permissibile per una funzione di sicurezza sostenuta da un elemento o sottosistema di tipo A, in funzione della tolleranza al guasto e della frazione di guasti sicuri.

Frazione di guasti sicuri (SFF) di un elemento	Tolleranza al guasto hardware (HFT)		
	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

L'allegato C della norma IEC/EN 61508-2 indica la procedura per il calcolo della SFF per il singolo elemento del sistema di sicurezza, nonché del fattore di copertura

diagnostica DC. Questo fattore indica la capacità da parte del sistema diagnostico di rilevare i guasti, assumendo un valore compreso tra 0 (diagnostica assente) e 1 (diagnostica completa) [10]. I guasti, pericolosi e sicuri, possono infatti essere ulteriormente suddivisi in pericolosi rilevati ("*DD*"), pericolosi non rilevati ("*DU*"), sicuri rilevati ("*SD*") e sicuri non rilevati ("*SU*") da cui derivano i relativi tassi di guasto (λ_{DD}, λ_{DU}, λ_{SD}, λ_{SU}).

Il calcolo della frazione di guasti sicuri prevede i seguenti passi:

a) effettuare un'analisi FMEA ("*Failure Modes and Effects Analysis*") per determinare gli effetti di ciascun modo di guasto di ciascun componente (o gruppo) degli elementi sul sistema di sicurezza E/E/EP in assenza di diagnostica;
b) catalogare ciascun modo di guasto in base ai suoi effetti come guasto sicuro o guasto pericoloso. Guasti che non portano ad effetti non devono essere considerati nel calcolo della SFF;
c) dalla stima dei tassi di guasto e dalla FMEA, suddividere i tassi di guasto sicuri λ_S e pericolosi λ_D. Se non costanti, è necessario stimare il valore mediato sul periodo di analisi;
d) per ciascun componente o gruppo, stimare la frazione di guasti pericolosi che possano essere identificati da test diagnostici (come monitoraggio e comparazione di segnali ridondanti, test con stimoli esterni, ecc…) e il relativo tasso di guasto λ_{DD};
e) per l'elemento calcolare la somma dei tassi di guasto ottenuti $\sum\lambda_D$, $\sum\lambda_S$ e $\sum\lambda_{DD}$;
f) calcolare la copertura diagnostica come (1):

$$\mathrm{DC} = \frac{\sum\lambda_{\mathrm{DD}}}{\sum\lambda_{\mathrm{D}}} \qquad (1)$$

g) calcolare la frazione di guasti sicuri (SFF): essa è definita nella IEC/EN 61508-4 come il rapporto tra i tassi medi di guasti sicuri, sommati con i tassi medi di guasto pericolosi rilevati, e la somma di tutti i tassi medi di guasti sicuri e pericolosi [10] (2):

$$\mathrm{SFF} = \frac{(\Sigma\lambda_{\mathrm{Savg}} + \Sigma\lambda_{\mathrm{DDavg}})}{(\Sigma\lambda_{\mathrm{Savg}} + \Sigma\lambda_{\mathrm{DDavg}} + \Sigma\lambda_{\mathrm{DUavg}})} \quad (2)$$

che nel caso di tassi di guasto costanti si semplifica come (3):

$$\mathrm{SFF} = \frac{(\Sigma\lambda_{\mathrm{S}} + \Sigma\lambda_{\mathrm{DD}})}{(\Sigma\lambda_{\mathrm{S}} + \Sigma\lambda_{\mathrm{DD}} + \Sigma\lambda_{\mathrm{DU}})} \quad (3)$$

Passando ora al Modo 2H, la minima tolleranza al guasto per ogni sottosistema dipende dal SIL richiesto:

- una tolleranza al guasto pari a 2, per una funzione di sicurezza con SIL 4;
- una tolleranza al guasto pari a 1, per una funzione di sicurezza con SIL 3;
- una tolleranza al guasto pari a 1, per una funzione di sicurezza con SIL 2 operante in alta o continua richiesta d'intervento;
- una tolleranza al guasto pari a 0, per una funzione di sicurezza con SIL 2 operante in bassa richiesta d'intervento;
- una tolleranza al guasto pari a 0, per una funzione di sicurezza con SIL 1.

Per i dispositivi di tipo A, se tramite l'analisi di rischio viene determinato che un numero di guasti tollerati è troppo alto poiché porta ad una diminuzione della sicurezza del sistema, occorre modificare l'architettura dei sottosistemi riducendo l'HFT.

I dati affidabilistici utilizzati devono essere basati su feedback provenienti da applicazioni analoghe sul campo e valutati da personale esperto. Occorre stimare il grado di confidenza di ciascun parametro affidabilistico, che dovrà essere superiore al 90%.

2.1.3 IEC/EN 61508-6: Linee guida per l'applicazione delle parti 2 e 3

Questa parte della norma fornisce informazioni supplementari alle norme IEC/EN 61508-1, IEC/EN 61508-2 e IEC/EN 61508-3. In particolare mostra degli esempi di tecniche affidabilistiche per il calcolo della probabilità media di guasto pericoloso su richiesta PFD_{avg} e della frequenza media di guasto pericoloso su richiesta PFH, già

viste nella prima norma [15]. Questi fattori risultano necessari per verificare che la probabilità di guasto pericoloso sia sufficientemente piccola da garantire la sicurezza richiesta, rappresentata dai corrispettivi valori SIL (come visto in tab. 2.2).

Pensando all'oggetto in esame, il Power LED, la sua struttura consente di definire una tolleranza hardware al guasto ("*Harware Fault* Tolerance", HFT) pari a zero [16], e quindi un'architettura cosiddetta "*1 out of 1*" (1oo1). Ciò significa che il dispositivo non sarà in grado di svolgere la sua funzione già dopo un singolo guasto. In accordo con la norma, un metodo analitico interessante per il calcolo della probabilità di guasto consiste nel modello dei diagrammi a blocchi d'affidabilità (RBD). Questo metodo è in grado di descrivere i collegamenti logici tra i guasti elementari ed il guasto del sistema, basandosi su formule derivate da un approccio di tipo Markoviano[4]. Il modello RBD risulta essere conservativo sotto determinate ipotesi, principalmente:

- tassi di guasto assunti costanti durante la vita utile del sistema. Generalmente valido per dispositivi elettronici, descrivibili con funzioni di tipo esponenziale;
- la probabilità media di guasto su richiesta PFD_{avg} e la frequenza media di guasto pericoloso PFH dovranno risultare inferiori rispettivamente a 10^{-1} e 10^{-5} h^{-1}, il che equivarrà ad assumere un SIL 1;
- i tassi di guasto devono essere impiegati per calcoli su di un singolo canale. Nel caso di un sistema multicanale (sottosistemi paralleli, diversi cioè dall'architettura "*1 out of 1*") gli effetti complessivi vengono calcolati a parte successivamente;
- nel sistema multicanale, ogni canale deve rispondere agli stessi tassi di guasto;
- il tasso di guasto complessivo di un canale è la somma dei tassi di guasto pericolosi e sicuri di quel canale;
- per ciascuna funzione di sicurezza sono assunti dei proof test "perfetti" (ogni guasto non rilevato normalmente viene rilevato al primo proof test utile). Con il termine proof test si intende una prova periodica attuata per rilevare guasti pericolosi non evidenti, così che il sistema di sicurezza possa essere riparato [10];

[4] Un processo di Markov è in sintesi un processo stocastico dell'evoluzione di un sistema, in cui la probabilità di transizione da uno stato del sistema ad uno futuro (es. da uno stato funzionante ad uno di guasto) dipende univocamente dallo stato attuale e non dagli stati ancora precedenti.

- l'intervallo di proof test è almeno di un ordine di grandezza superiore rispetto al tempo medio di riparazione MRT;
- per ciascun sottosistema vi è un singolo intervallo di proof test e di MRT;
- l'intervallo atteso tra due richieste d'intervento è almeno di un ordine di grandezza maggiore dell'intervallo di proof test;
- per tutti i sottosistemi operanti in bassa richiesta d'intervento, e per i gruppi 1oo2, 1oo2D, 1oo3 e 2oo3 in continua o alta richiesta, la frazione di guasti specificata dalla copertura diagnostica è sia rilevata che riparata nel periodo di tempo MTTR (*Mean Time To Restoration*) specificato;
- per i gruppi 1oo1 e 2oo2 operanti in continua o alta richiesta d'intervento, il sistema di sicurezza E/E/EP raggiunge sempre uno stato sicuro dopo aver individuato un guasto pericoloso.

2.1.3.1 Probabilità media di guasto su richiesta per bassa richiesta d'intervento e architettura 1oo1

Nel caso generico, un sistema di sicurezza E/E/EP è composto da più sottosistemi (fig. 2.3).

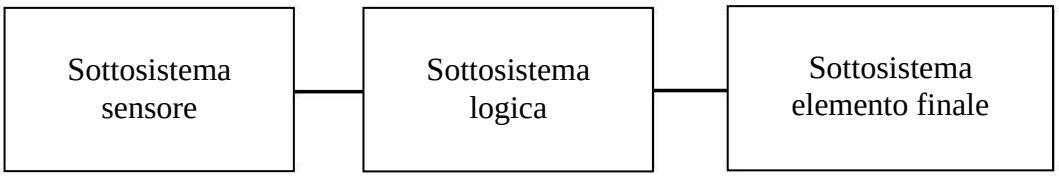

Figura 2.3 – Sottosistemi componenti un generico sistema di sicurezza E/E/EP.

La probabilità media di guasto su richiesta di una funzione di sicurezza, per un sistema di sicurezza E/E/EP, è calcolata combinando la probabilità media di guasto su richiesta dei vari sottosistemi (5):

$$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE} \quad (5)$$

dove:

- PFD_{SYS} è la probabilità media di guasto su richiesta del sistema;
- PFD_S è la probabilità media di guasto su richiesta del sottosistema sensore;

- PFD_L è la probabilità media di guasto su richiesta del sottosistema logica;
- PFD_{FE} è la probabilità media di guasto su richiesta del sottosistema elementi finali.

Nel caso di architettura 1oo1, dove qualsiasi guasto pericoloso porta al fallimento della funzione di sicurezza, il tasso di guasto pericoloso equivale alla somma del rateo dei guasti pericolosi non rilevati e da quello dei guasti pericolosi rilevati (6):

$$\lambda_D = \lambda_{DU} + \lambda_{DD} \tag{6}$$

Virtualmente il canale può essere quindi visto come composizione di due elementi, uno caratterizzato dal tasso di guasto λ_{DU} e uno dal tasso di guasto λ_{DD}. Si calcola dunque il tempo medio in cui il sistema non funziona (t_{CE}, "*down time medio equivalente*") andando a sommare i tempi di non funzionamento dei singoli componenti, proporzionati al contributo del componente alla probabilità di guasto (7):

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \tag{7}$$

dove T_1 rappresenta l'intervallo da due proof test consecutivi.

I tassi di guasto per guasti rilevati e guasti non rilevati si calcolano tramite il fattore di copertura diagnostica DC (8) (9):

$$\lambda_{DU} = \lambda_D (1 - DC) \tag{8}$$

$$\lambda_{DD} = \lambda_D DC \tag{9}$$

La probabilità di guasto su richiesta del sistema equivale alla inaffidabilità, che nel caso di componenti elettronici, descritti da una funzione di tipo esponenziale, risulta essere (approssimando tramite serie di McLaurin troncata al primo ordine) (10):

$$PFD = 1 - e^{-\lambda_D t_{CE}} \approx \lambda_D t_{CE} \tag{10}$$

Da cui la PDF media per un sistema con architettura 1oo1 si ottiene sostituendo il valore di t_{CE} (11):

$$PFD_{avg} = \lambda_{DU}\left(\frac{T_1}{2} + MRT\right) + \lambda_{DD}MTTR \quad (11)$$

2.1.3.2 Frequenza media di guasto pericoloso per alta o continua richiesta d'intervento e architettura 1oo1

Il calcolo della frequenza media di guasto pericoloso per alta o continua richiesta d'intervento della funzione di sicurezza (PFH_{avg}) risulta identico al calcolo della probabilità media di guasto su richiesta nel caso di bassa richiesta d'intervento. Occorre solo sostituire al termine PFD_{avg} il termine PFH_{avg} e chiaramente, sfruttare le tabelle contenute nella norma relative a questo secondo caso.

2.2 NORMA CEI EN 50495:2010

L'apparecchiatura elettrica utilizzata in atmosfere potenzialmente esplosive può richiedere l'utilizzo di dispositivi elettrici di sicurezza, controllo e regolazione associati all'apparecchio sotto controllo. Scopo di tali dispositivi è garantire una corretta integrità, cioè affidabilità e sicurezza, delle apparecchiature riducendo sotto livelli prestabiliti il rischio d'innesco dell'atmosfera.

Come introdotto dalle norme della serie IEC/EN 61508, i dispositivi di sicurezza sono caratterizzati da una propria funzione di sicurezza, che in questo caso deve rispondere anche ai requisiti della Direttiva ATEX e alle norme della serie IEC/EN 60079 per apparecchi destinati alle atmosfere esplosive. La norma CEI EN 50495 va ad affiancarsi a questi documenti, riprendendone i principi e fornendo informazioni supplementari utili per la progettazione di un apparecchio sicuro.

In generale si classificano due tipi di dispositivi di sicurezza:

- dispositivi inclusi come componenti nell'apparecchio sotto controllo: l'insieme costituisce un apparecchio (ad esempio termistore o termostato che evitano il surriscaldamento);
- dispositivi separati dall'apparecchio sotto controllo: sono esclusivi per uno specifico apparecchio o associati per un specifico modo di protezione.

L'insieme costituisce un sistema (ad esempio driver elettronico per il controllo dell'alimentazione dei dispositivi LED, dispositivo di protezione da sovraccarico per motori elettrici con modo di protezione "Ex e"; sensore di livello per controllo di pompe sommerse).

Vengono esclusi dall'applicazione di questa norma i dispositivi di sicurezza la cui funzione di sicurezza è descrivibile in modo sufficiente dalle norme della serie IEC/EN 60079 (ad esempio dispositivi a sicurezza intrinseca come fusibili), dispositivi/sistemi che prevengono la formazione di atmosfera esplosiva (inertizzazione, ventilazione, ecc…), rilevatori di gas (per cui vi è una normativa specifica).

2.2.1 Termini e definizioni

Il testo della Norma richiama l'attenzione sulle definizioni della Normativa IEC/EN 60079-0, a cui ne aggiunge altre. Per permettere una comprensione sufficientemente esaustiva, vengono qui riassunte le principali:

- Modi di protezione: misure per la protezione di costruzioni elettriche dal rischio d'esplosione;
- Categoria dell'apparecchio: si intende una classificazione dell'apparecchio rispetto al rischio d'innesco dell'atmosfera. Sono possibili due livelli di sicurezza (in ordine decrescente M1 e M2) per il Gruppo I (Miniere) e tre livelli (1, 2, 3) per il Gruppo II (Superficie). Le categorie sono correlate alle Zone a rischio d'esplosione. Sono inoltre equivalenti al pertinente EPL definito dalla IEC/EN 60079-0 [7] (si veda la tab. 1.4).
- Dispositivo di sicurezza: dispositivo di sicurezza, regolazione e/o controllo necessario per il funzionamento in sicurezza associato all'apparecchio principale. Garantisce la protezione dall'esplosione eseguendo una funzione di sicurezza indipendente dalla principale funzione dell'apparecchio sotto controllo. Se il dispositivo è formato da più componenti di sicurezza si parla di SIS (Sistema di Sicurezza Strumentato). Viene composto da sensore/i, risolutore/i logico/i ed elemento/i finale/i;

- Funzione di sicurezza: è la funzione messa in atto dal dispositivo di sicurezza con l'intenzione di mantenere o raggiungere uno stato sicuro del sistema, in relazione al rischio d'innesco.;
- Dispositivo di sicurezza semplice o complesso: la funzione di sicurezza può risultare dall'adozione di tecnologia complessa (ad esempio a microprocessore, software). In tal caso si parla di dispositivo complesso. Viceversa il dispositivo semplice non prevede l'uso di tecnologia complessa. Per essere considerato semplice devono poter essere esclusi guasti sistematici (altrimenti è da considerarsi come complesso ai fini di una valutazione).
- Apparecchio Sotto Controllo (EUC): qualsiasi apparecchiatura, componente, apparato che contiene una potenziale sorgente d'innesco e che viene controllata da un dispositivo di sicurezza[5];
- Stato di sicurezza: stato del dispositivo di sicurezza riferito ad una condizione di sicurezza per l'EUC;
- Condizione di sicurezza: definisce operativamente in che modo il rischio d'innesco ritenuto accettabile sia fornito dall'apparecchio sotto controllo. La condizione di sicurezza è legata all'attivazione della funzione di sicurezza del dispositivo di sicurezza;
- Sicurezza funzionale: parte della sicurezza complessiva, legata al corretto funzionamento degli EUC e dei sistemi di controllo e sicurezza ad essi associati per la riduzione del rischio;
- Apparecchio combinato: assieme di dispositivo di sicurezza ed EUC, come unica unità o come unità separate. In ogni caso il tutto è considerato un apparecchio;
- Livello di Integrità della Sicurezza (SIL): livello numerico discreto che indica l'affidabilità e la sicurezza richiesta ad una o più funzioni di sicurezza. Va da

[5] Nelle Norme IEC/EN 61508-1 e IEC/EN 61508-4 il dispositivo sotto controllo (EUC) è definito come macchinario, dispositivo, apparato o impianto usato in un processo industriale sottoposto a controllo. Un normale sistema di controllo viene distinto da un sistema di sicurezza, salvo nel caso in cui il primo trovi promozione a "sistema di sicurezza" grazie alla bassa probabilità di guasto. Nella norma CEI/EN50495:2010 l'EUC è definito come controllato direttamente da un sistema di sicurezza poiché fonte d'innesco. La definizione trova un'interpretazione coerente poiché nel secondo caso si rientra nell'ambito specifico di dispositivi elettrici per applicazioni antideflagranti, che richiedono un controllo non solo per il normale funzionamento ma proprio per garantire la sicurezza.

1 (livello minore) a 4 (livello maggiore) ed è correlato alla probabilità di avarie pericolose per ora;

- Potenzialità SIL: ci si riferisce al massimo valore SIL che può essere raggiunto da un dispositivo di sicurezza, nel caso questo utilizzi un componente di sicurezza separato in modalità singolo canale;
- Analisi degli Effetti e Modalità di Guasto (FMEA): consiste nell'analisi di tutti i possibili modi di guasto del dispositivo di sicurezza e la valutazione delle conseguenze sul sistema e sulla sicurezza. È un utile strumento che permette di indicare ogni guasto valutato come sicuro o pericoloso, rilevabile o non rilevabile (si intende rilevabile dal sistema di diagnostica automatico o tramite il sistema operativo normale);
- Probabilità di Guasto su Richiesta (PFD): è la probabilità media che avvenga un guasto pericoloso quando viene richiesta la funzione del dispositivo di sicurezza. Viene applicata quando la richiesta di funzionamento del dispositivo di sicurezza è ridotta (da cui il nome 'su richiesta');
- Probabilità di Guasto Pericoloso per Ora (PFH): indica la probabilità di guasto pericoloso per ora quando viene richiesta la funzione di sicurezza. Tale valore è considerato solo quando il dispositivo di sicurezza opera in continuo o con alta frequenza d'intervento (maggiore di una volta all'anno o maggiore del doppio della frequenza di prova di collaudo);
- Frazione di Guasti Sicuri (SFF): è il rapporto percentuale tra la somma dei tassi dei guasti sicuri e dei pericolosi rilevabili, e la somma di tutti i tassi di guasto [17];
- Tolleranza ai Guasti dell'Hardware (HFT): indica il numero di guasti che il dispositivo di sicurezza è capace di sopportare, continuando ad eseguire la sua funzione di sicurezza. Superato tale valore si ha una situazione di guasto pericoloso [17];
- Livello di scatto: valore soglia di uno specifico parametro, impostato nel dispositivo di sicurezza, che se superato attiva la funzione di sicurezza;
- Architettura: indica la specifica configurazione dell'hardware e del software nel sistema;

- Canale: indica il numero di elementi o gruppi di elementi che sono in grado di svolgere una funzione indipendentemente dagli altri elementi o gruppi di elementi. Ad esempio un sistema a doppio canale è composto da due canali che assolvono alla stessa funzione in maniera indipendente;
- Livello di confidenza: costruito un intervallo di confidenza attorno al valore medio di una distribuzione statistica di prove, il livello di confidenza indica la probabilità che il valore reale sia contenuto all'interno di tale intervallo;
- Temperatura ambiente media: è pari al valore medio della temperatura ambiente a cui è sottoposto il componente.

2.2.2 Prevenzione dell'innesco attraverso dispositivi di sicurezza

Per ridurre il rischio d'innesco dell'atmosfera esplosiva ad un livello accettabile, ad ogni dispositivo o sistema viene applicato un appropriato modo di protezione in relazione alla zona d'installazione dell'apparecchio e alle potenziali sorgenti d'innesco presenti (come da indicazioni delle Norme IEC/EN 60079).

Guasti e anomalie nel funzionamento possono creare a loro volta una sorgente d'innesco. Per garantire la sicurezza viene richiesto che il sistema riesca a sopportare un numero definito di guasti, in base alla categoria a cui appartiene l'apparecchio, senza che rappresenti un pericolo. Nel caso in cui un dispositivo non soddisfi tali requisiti è possibile implementare dei dispositivi di sicurezza che aumentino il numero di guasti sopportati[6] (HFT). Complessivamente, la Norma richiede i seguenti standard:

- **Categoria 1**: il sistema deve essere in grado di sopportare 2 guasti distinti senza presentare una sorgente potenziale d'innesco.
- **Categoria 2**: il sistema deve essere in grado di sopportare un guasto senza presentare una sorgente potenziale d'innesco
- **Categoria 3**: al sistema è richiesto solo il funzionamento sicuro in condizioni normali. Non è necessario l'implementazione di un dispositivo di sicurezza.

La riduzione del rischio d'innesco apportata dal dispositivo di sicurezza è indicata da un *Fattore di Riduzione del Rischio Equivalente*, che risulta associato ad un corrispettivo livello SIL (tab. 2.3).

[6] I dispositivi di sicurezza implementati devono essere sempre conformi alle norme IEC/EN 60079.

Tabella 2.3 – Classificazione del SIL e del Fattore di Riduzione del Rischio Equivalente.

Safety Integrity Level	**Fattore di riduzione del rischio equivalente**
N/A	Fino a 10
1	Da 10 a 100
2	Da 100 a 1000
3	Da 1000 a 10000
4	Da 10000 a 100000

Complessivamente sono dunque riassumibili i requisiti di tolleranze al guasto e livello SIL in base alle categorie dell'apparecchio (tabella 2.4).

Tabella 2.4 - Requisiti minimi per SIL e tolleranza al guasto in base alla Categoria.

EUC						
Tolleranza al guasto	2	1	0	1	0	0
Dispositivo di sicurezza						
Tolleranza al guasto	-	0	1	-	0	-
SIL	-	SIL 1	SIL 2	-	SIL 1	-
Categoria apparecchio	M1 1			M2 2		- 3

Note:
"-" indica che non è necessario l'uso di dispositivi di sicurezza;
"0" indica tolleranza al guasto zero, cioè sicuro solo in funzionamento normale;
"1" indica tolleranza al guasto 1, cioè sicuro fino ad un guasto;
"2" indica tolleranza al guasto 2, cioè sicuro fino a due guasti.

Per chiarezza si prenda ad esempio la Categoria 1 e si considerino i diversi casi:

- L'apparecchio principale sopporta già due guasti e pertanto non è necessaria l'implementazione di un dispositivo di sicurezza. Per entrare in una situazione pericolosa occorrono almeno tre fallimenti al dispositivo;

- L'apparecchio sopporta solo un guasto ma viene aggiunto un dispositivo di sicurezza a tolleranza di guasto zero. Per entrare in una situazione pericolosa occorrono almeno due fallimenti all'EUC e uno al dispositivo di sicurezza;
- L'apparecchio è sicuro solo in funzionamento normale e viene associato un dispositivo di sicurezza capace di sopportare un guasto. Occorrono ora almeno un guasto all'EUC e due al dispositivo di sicurezza per presentare un pericolo d'innesco.

Come si vede, occorre sempre almeno un terzo guasto per perdere la garanzia di sicurezza. Un discorso analogo, a scalare, può essere fatto per le altre categorie.

È importante sottolineare che per ogni sorgente d'innesco (anche nella stessa apparecchiatura) è indispensabile effettuare le suddette considerazioni.

2.2.3 Requisiti per ottenere il Livello di Integrità della Sicurezza (SIL)

Il livello SIL di un dispositivo di sicurezza deve essere calcolato tenendo in considerazione le specifiche della Norma IEC/EN 61508. Il SIL viene ricavato da un'analisi statistica dei guasti, la cui probabilità può essere valutata con strumenti statistici come ad esempio FMEA[7] (Analisi dei Modi di Guasto ed Effetti), FTA[8] (Albero dei Guasti), catene di Markov[9].

I tassi di guasto possono essere ottenuti per via sperimentale, da archivi storici o dal produttore. I valori dei ratei di guasto sono definiti in determinate condizioni di riferimento, e devono essere opportunamente modificati se riferiti ad una situazione diversa (ad esempio nel caso di condizioni climatiche estreme, occorrerà considerare la nuova temperatura media).

Come introdotto nelle norme IEC/EN 61508 è possibile classificare i guasti come sicuri/pericolosi e rilevati/non rilevati.

[7] Si fa riferimento alla norma IEC/EN 60812.
[8] Si fa riferimento alla norma IEC/EN 61025.
[9] Si fa riferimento alla norma IEC/EN 61165.

Se gli effetti di un guasto della funzione di sicurezza non sono determinabili, la norma indica di classificare il guasto come pericoloso e suddividerlo come 50% rilevato e 50% non rilevato.

Considerando entrambi gli aspetti, si ottengono guasti sicuri-rilevati (SD), sicuri-non rilevati (SU), pericolosi-rilevati (DD), pericolosi-non rilevati (DU) a cui corrispondono diversi tassi di guasto (λ_{SD}, λ_{SU}, λ_{DD}, λ_{DU}). Questi sono i parametri di partenza da cui è possibile calcolare i parametri di sicurezza PFD/PFH ed SFF, e infine il SIL.

2.2.3.1 Esempio di valutazione del SIL per un dispositivo di sicurezza

La Norma riporta un metodo valido per il calcolo del SIL nell'"*Allegato B: Esempio di una procedura di valutazione per l'integrità della sicurezza hardware di un dispositivo di sicurezza"*.

Il primo step consiste nell'effettuazione di una FMEA, cioè una valutazione dei possibili modi di guasto e dei loro effetti rilevanti ai fini della sicurezza. Parlando di dispositivi elettronici, i tipi di guasto tipici in cui ci si può imbattere sono circuito aperto, cortocircuito e deriva dai valori nominali in senso positivo o negativo.

Calcolato il tasso complessivo dei guasti per un certo componente, questo deve essere suddiviso equamente per ogni tipo di guasto che è possibile incontrare in quel contesto (ad esempio se possibili solo circuito aperto e cortocircuito si avrà un numero di tipi n=2), seguendo la formula (12):

$$\lambda_{\text{tipo di guasto}} = \frac{\lambda_{\text{totale del componente}}}{\text{numero di tipi di guasto}} \tag{12}$$

Come introdotto sopra, durante la valutazione dei guasti è possibile catalogare questi ultimi in base alle caratteristiche di sicurezza e rilevabilità (SD, SU, DD, DU) da cui derivano i relativi tassi di guasto: considerando l'intero sistema, essi sono ottenuti dalla somma dei tassi di guasto di quel tipo per tutti i componenti (tabella 2.5).

Tabella 2.5 – Ratei di guasto in base alle modalità di guasto.

Tipi di guasto	*Rilevati (d)*	*Non rilevati (u)*
Sicuri (S)	$\lambda_{SD} = \sum_{i=1}^{n} \lambda_{SD_i}$	$\lambda_{SU} = \sum_{i=1}^{n} \lambda_{SU_i}$
Pericolosi (D)	$\lambda_{DD} = \sum_{i=1}^{n} \lambda_{DD_i}$	$\lambda_{DU} = \sum_{i=1}^{n} \lambda_{DU_i}$

Si calcola dunque il tasso di guasto totale del sistema λ_{tot} (13) da cui, ipotizzando che λ_{TOT} sia costante nel tempo, si ottiene il Tempo Medio Tra Guasti (MTBF) (14):

$$\lambda_{TOT} = \lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU} \tag{13}$$

$$\text{MTBF} = \frac{1}{\lambda_{TOT}} \tag{14}$$

È ora possibile definire i parametri chiave per la valutazione del SIL.

In base all'architettura del dispositivo di sicurezza, riferendosi sempre alla IEC/EN 61508, si determina il valore della Probabilità di Fallimento su Richiesta (PFD) o della Probabilità di Fallimento pericoloso per Ora (PFH) in base alla frequenza con cui viene chiamato ad operare il dispositivo di sicurezza (rispettivamente bassa e alta/continua).

Si calcola la Frazione dei Guasti Sicuri (SFF) come rapporto tra la somma dei ratei di guasto sicuri (si includono anche i pericolosi rilevabili poiché è possibile intervenire su di essi) e il rateo di guasto totale (15):

$$\text{SFF} = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{TOT}} \tag{15}$$

Infine viene considerata la Tolleranza ai Guasti Hardware (HFT), cioè il numero di guasti indipendenti che il dispositivo sopporta senza perdere la propria funzione di sicurezza (come già visto in tabella 2.2).

A questo punto è possibile associare l'appropriato livello SIL seguendo le indicazioni delle tabelle 2.6 e 2.7.

Tabella 2.6 – Relazione tra livelli SIL e probabilità di guasto su richiesta (bassa o alta/continua) consentita al sistema di sicurezza.

Livello di Integrità della Sicurezza	**Funzionamento in bassa richiesta: PFD**	**Funzionamento in alta frequenza di richiesta o continua: PFH**
SIL 4	da $\geq 10^{-5}$ a $< 10^{-4}$	da $\geq 10^{-9}$ a $< 10^{-8}$
SIL 3	da $\geq 10^{-4}$ a $< 10^{-3}$	da $\geq 10^{-8}$ a $< 10^{-7}$
SIL 2	da $\geq 10^{-3}$ a $< 10^{-2}$	da $\geq 10^{-7}$ a $< 10^{-6}$
SIL 1	da $\geq 10^{-2}$ a 10^{-1}	da $\geq 10^{-6}$ a 10^{-5}

Tabella 2.7 – Vincoli dell'architettura dei sottosistemi legati alla sicurezza. Il SIL associabile al sistema è funzione della tolleranza al guasto hardware (HFT) e della frazione di guasti sicuri (SFF).

SFF	**Sottosistemi Tipo A**			**Sottosistemi Tipo B**		
	HFT			**HFT**		
	0	**1**	**2**	**0**	**1**	**2**
< 60%	SIL 1	SIL 2	SIL 3	Non ammesso	SIL 1	SIL 2
60% - < 90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90% - < 99%	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4
Note: Sottosistemi Tipo A: qualsiasi sistema basato su tecnologia analogica; Sottosistemi Tipo B: qualsiasi sistema basato su uno o più moduli programmabili;						

2.3 NORMA IEC/EN 60079 – 28

La norma IEC/EN 60079-28 introduce la problematica delle apparecchiature che sfruttano radiazione ottica[10] (fibre ottiche, laser e sorgenti di illuminazione tra cui i dispositivi LED) da impiegare in ambientazioni Ex, fornendo indicazioni sulle precauzioni e sui requisiti da adottare [18]. Per quanto riguarda gli apparecchi di illuminazione, le radiazioni emesse possono innescare le atmosfere esplosive cariche di gas o polveri principalmente a causa dell'assorbimento delle radiazioni da parte

[10] Con radiazione ottica si intende la parte di spettro elettromagnetico che comprende la radiazione ultravioletta, quella visibile e quella infrarossa (da 100nm a 1mm).

delle superfici e delle particelle presenti, riscaldandole fino alla temperatura d'innesco.

Storicamente la scelta dell'apparecchiatura da utilizzare in una determinata zona ATEX si basava semplicemente sul tipo di protezione ad essa associato, in considerazione che ogni zona contempla solo determinati modi di protezione. La valutazione era fondata solo su basi statistiche di probabilità di innesco: maggiore è la frequenza di avere un'atmosfera esplosiva, maggiore è la protezione necessaria. Più recentemente ci si è indirizzati verso approcci basati sulla valutazione del rischio, in grado di considerare il problema nella sua interezza, comprese le conseguenze di un'eventuale esplosione. Sfruttando un approccio di questo tipo, è possibile identificare le sorgenti e il meccanismo di ignizione dell'atmosfera, valutare il rischio associato all'apparecchio e quindi il modo di protezione più corretto. Ad ogni zona è associato un diverso livello di rischio accettabile attraverso il concetto di Equipment Protection Level, così che sia possibile selezionare l'apparecchiatura (tab. 2.8).

Tabella 2.8 – Relazione tra zone ATEX, EPL e protezione da innesco richiesta all'apparecchiatura.

Zona	EPL	Protezione richiesta
0 / 20	Ga / Da	Innesco non possibile con due guasti indipendenti o in caso di rari malfunzionamenti. L'apparecchio rimane funzionante nelle zone 0/20, 1/21, 2/22.
1 / 21	Gb / Db	Innesco non possibile con un guasto o in caso di malfunzionamenti prevedibili. L'apparecchio rimane funzionante nelle zone 1/21, 2/22.
2 / 22	Gc / Dc	Innesco non possibile in normali condizioni di funzionamento. L'apparecchio rimane funzionante nelle zone 2/22.

2.3.1 Protezione dell'apparecchiatura

Esistono tre tipologie di protezione dal rischio di innesco dell'atmosfera esplosiva da radiazioni ottiche:

- utilizzo di radiazioni ottiche intrinsecamente sicure. Protezione “op is”;
- confinamento della radiazione ottica. Protezione “op pr”;
- utilizzo di un sistema di interblocco che agisca sulla sorgente. Protezione “op sh”.

Il primo metodo agisce limitando fortemente l’energia del fascio luminoso e quindi la potenza installabile dell’apparecchio.

Il secondo metodo consiste nell’isolamento completo della radiazione luminosa all’interno di un involucro che ne impedisca il contatto con l’atmosfera potenzialmente esplosiva: è un approccio utilizzato per sistemi come fibre ottiche.

Il terzo metodo è il più interessante e presuppone l’utilizzo di un sistema che controlli attivamente la sorgente luminosa, limitandola o disattivandola nel caso diventi una potenziale sorgente di innesco. Le modalità d’intervento dipendono dal sistema esaminato e devono rispettare i requisiti ottenuti dall’analisi di rischio.

Il testo della norma fa chiaramente riferimento alla IEC/EN 61508 come strumento per studiare la sicurezza del sistema, in termini di fattore di riduzione del rischio e di sua disponibilità. Il legame tra questi elementi e l’EPL è mostrato in tabella 2.9.

Tabella 2.9 – Equipment Protection Level e relativi intervalli di disponibilità e del fattore di riduzione del rischio d’innesco richiesti.

EPL	**Disponibilità**	**Fattore di riduzione del rischio d’innesco**
a	da 0,999 a 0,9999	da 1000 a 10000
b	da 0,99 a 0,999	da 100 a 1000
c	da 0,9 a 0,99	da 10 a 100

Capitolo 3

Valutazione della sicurezza del LED

Un apparecchio d'illuminazione a LED è composto essenzialmente dalle sorgenti d'illuminazione e da un driver elettronico. Il driver è in grado di pilotare e controllare i diodi, fornendo una prima protezione contro sovratensioni e sovraccarichi. Tuttavia se il dispositivo fallisce, la sicurezza è demandata ai LEDs. La valutazione della loro affidabilità e della capacità di mantenere uno stato sicuro diventa perciò fondamentale, in particolare in relazione all'applicabilità nelle diverse zone ATEX del sistema.

Negli ultimi anni i dispositivi a diodi luminosi ad alta efficienza sono stati studiati a lungo anche dal punto di vista della sicurezza. La recente quinta revisione della norma IEC/EN 60079-7 "*Atmosfere esplosive - Protezione di apparecchi tramite sicurezza aumentata "e"*", pubblicata in data 26 giugno 2015, ha incluso esplicitamente i LED tra le apparecchiature a sicurezza aumentata, limitando però tale definizione solo all'uso in zona 2 (corrispondente ad un EPL "Gc" per atmosfere con miscele di gas esplodibili). L'ipotesi di un utilizzo dei LED con protezione "Ex e" nella zona 1 non è stato precluso: se in futuro saranno dimostrate l'affidabilità e la sicurezza richieste, sarà possibile anche questa applicazione.

Il concetto di Equipment Protection Level introdotto nel secondo capitolo appare idoneo a essere sfruttato per categorizzare il LED da un punto di vista della sicurezza. Come visto, l'EPL è però formalizzato in modo qualitativo. La procedura di valutazione del SIL è un valido strumento per quantificare e determinare il corretto EPL.

Formalmente il SIL rappresenta l'affidabilità e la riduzione di rischio richiesta a un sistema di controllo attivo associato a un'apparecchiatura sotto controllo, dunque non appare direttamente applicabile a un dispositivo elettrico passivo. Tuttavia

l'approccio numerico sviluppato nel SIL può essere utilizzato per valutare le caratteristiche di un componente indipendente, conoscendo i modi e i tassi di guasto del componente stesso. All'atto pratico è possibile determinare implicitamente l'integrità della sicurezza di un sistema costituito da un componente passivo come il LED. In passato la procedura associata al SIL è già stata applicata per valutare barriere di sicurezza a diodi per applicazioni ATEX. Questi circuiti, utilizzati per limitare tensione e corrente di un circuito elettrico non intrinsecamente sicuro, sono costituiti da resistori e da diodi zener, quindi elementi a semiconduttore passivi [19].

3.1 UTILIZZO DELL'APPROCCIO SIL

3.1.1 Identificazione del Livello d'Integrità della Sicurezza target

Seguendo la linea dettata dall'approccio SIL nel "*ciclo di vita della sicurezza*" di un sistema di sicurezza, viene eseguita un'allocazione dei requisiti di sicurezza a ogni dispositivo in base alla categoria di appartenenza. Da un'analisi di rischio del contesto applicativo sono identificate e classificate le diverse zone, cui corrisponderanno determinate categorie di apparecchi con gli adeguati requisiti di sicurezza. Prima di tutto è richiesta all'apparecchiatura una tolleranza ai guasti (HFT) minima in base alla categoria e all'EPL associati:

a) tolleranza ai guasti "2" per categoria 1 (EPL Ga/Da). L'apparecchio è sicuro fino a due guasti indipendenti.
b) tolleranza ai guasti "1" per categoria 2 (EPL Gb/Db). L'apparecchio è sicuro fino a un guasto;
c) tolleranza ai guasti "0" per categoria 3 (EPL Gc/Dc). L'apparecchio non è più sicuro al primo guasto.

Nel caso in cui l'apparecchio non sia in grado di soddisfare questo vincolo, è possibile associare un dispositivo di sicurezza così che la stessa HFT venga chiesta non più alla singola apparecchiatura ma al sistema complessivo.

Analizzando un sistema pensato per l'installazione in Zona 1, appartenente alla categoria 2, esso potrà essere composto di un apparecchio sotto controllo e da un sistema di sicurezza che abbiano rispettivamente una tolleranza al guasto pari a zero, come mostrato in tabella 3.1. Questo è il caso applicabile a un sistema

d'illuminazione, composto di LED e driver, ipotizzato per l'applicazione in Zona 1. Poiché l'effetto dei guasti del LED sulla sicurezza non sono ancora perfettamente conosciuti, le normative vigenti fissano una tolleranza al guasto del LED pari a zero [16]. Considerando un sistema composto dalla sorgente luminosa e dal driver (a sua volta considerato con un HFT pari a zero), esso è capace, complessivamente, di sopportare un guasto senza diventare una fonte d'innesco dell'atmosfera esplosiva e quindi appartenente alla categoria 1. Per ottenere un sistema pericoloso sarebbero infatti necessari due guasti: uno del driver e uno del LED. La norma CEI EN 50495:2010, cui appartiene la tabella 3.1, indica che il livello d'integrità della sicurezza associato è il SIL 1.

Tabella 3.1 - Secondo la CEI EN 50495:2010 un sistema appartenente a una certa categoria deve possedere una minima tolleranza al guasto, e a esso sarà associato il relativo SIL. È evidenziata la colonna riferita alla categoria 2. Il LED rappresenta l'apparecchio sotto controllo, mentre il driver è il dispositivo di sicurezza.

EUC						
Tolleranza al guasto	2	1	0	1	0	0
Dispositivo di sicurezza						
Tolleranza al guasto	-	0	1	-	0	-
SIL	-	SIL 1	SIL 2	-	SIL 1	-
Categoria apparecchio	M1 1			M2 2		- 3

Note:
"-" indica che non è necessario l'uso di dispositivi di sicurezza;
"0" indica tolleranza al guasto zero, cioè sicuro solo in funzionamento normale;
"1" indica tolleranza al guasto 1, cioè sicuro fino a un guasto;
"2" indica tolleranza al guasto 2, cioè sicuro fino a due guasti.

Lo stesso documento suddivide i dispositivi di sicurezza in due tipologie:

a) dispositivi inclusi come componenti nell'apparecchio sotto controllo;

b) dispositivi installati separatamente dall'apparecchio sotto controllo, specifici per quell'apparecchio o per un tipo di protezione.

Il LED rientra a pieno titolo nella prima categoria poiché è esso stesso il componente sotto controllo ma contemporaneamente viene trattato come un dispositivo di sicurezza, in grado cioè di garantire un certo livello di integrità della sicurezza. Facendo parte del primo tipo di dispositivi, si possono applicare i requisiti di sicurezza al comportamento intrinseco del diodo e valutare quantitativamente la sua affidabilità. Questa idea non trova ostacoli poiché l'integrità della sicurezza e l'affidabilità sono concetti generali. In particolare da un punto di vista numerico le valutazioni previste nella norma CEI EN 50495:2010 sono applicabili a ogni dispositivo, sia esso attivo o passivo. Inoltre le uniche chiare esclusioni imposte riguardano:

- dispositivi di sicurezza la cui funzione di sicurezza è già descritta completamente dalle norme della serie IEC/EN 60079 o da altre norme specifiche;
- dispositivi di protezione come fusibili e interruttori termici;
- sistemi che prevengono la formazione di atmosfere esplosive, come sistemi di ventilazione o inertizzanti;
- sistemi non elettrici di protezione.

3.1.2 Analisi del comportamento dei LED: FMECA/FMEDA

Una volta individuato il SIL 1 come livello equivalente d'integrità della sicurezza richiesto, occorre valutare a fondo la natura ed il comportamento del LED.

Le principali problematiche che portano all'innesco di un'atmosfera esplosiva sono una temperatura eccessiva delle superfici e la creazione di scintille o archi elettrici. In normali condizioni di funzionamento il LED non produce alcun tipo di arco elettrico, mentre le temperature superficiali di un singolo dispositivo possono raggiungere il centinaio di gradi centigradi [20]. In ogni caso il calore è prodotto per effetto Joule e dipende dalla corrente di alimentazione, che può essere opportunamente limitata. Una sovratemperatura può presentarsi nel caso di cortocircuito del chip, per cui il calo della resistenza elettrica consente il passaggio di

una corrente eccessiva. Un guasto di circuito aperto rischia invece di creare un arco elettrico: se la tensione tra due terminali supera la rigidità dielettrica del mezzo interposto, scoccherà una scarica tra i due. Nel caso in cui l'involucro del chip si fratturi ed esponga i terminali all'atmosfera, l'arco potrebbe innescare i gas o le polveri presenti. Per avere un'idea delle percentuali di incidenza dei principali modi di guasto di un normale diodo luminoso si può far riferimento a database affidabilistici come l'FMD-97 (tab. 3.2) [21]:

Tabella 3.2 – Incidenza percentuale dei diversi modi di guasto di un LED standard secondo FMD-97.

Modo di guasto	**Frazione**
Guasto al filamento	50%
Perdita di efficienza luminosa	16,7%
Circuito aperto	14,3%
Mancanza di output luminoso	7,1%
Guasto ai contatti elettrici	6,0%
Crepe e fratture	6,0%

Ogni tipologia di diodo luminoso possiede però delle caratteristiche peculiari che le consentono una risposta diversa ai diversi modi di guasto. Da studi precedenti si è visto come ciascun tipo di LED risponda diversamente ai guasti (tab. 3.3) [4].

Tabella 3.3 - Classificazione dei modi di guasto in base alla tipologia di LED.

Modo di guasto	**LED THT**	**LED SMD**	**Power LED**	**Power LED Flip Chip**
Degradazione della capsula di resina	D	D	D	D
Stress meccanico e deformazione dell'involucro	OC	OC	OC	X
Degradazione dei fosfori	X	X	D	D
Dislocazione e nucleazione nel materiale del semiconduttore	D	D	D	D
Elettromigrazione di particelle metalliche	OC	OC	OC	D
Passivazione vetrosa incompleta	D	D	D	D
Current Crowding e alterazioni di densità di carica nei contatti	D	D	D	D
Scariche elettrostatiche (ESD)	OC-SC	OC-SC	OC-SC	SC
Stress elettrico (EOS) da sovracorrenti o sovratensioni	D-OC-SC	D-OC-SC	D-OC-SC	D-SC
Polarizzazione inversa	OC-SC	OC-SC	OC-SC	SC
Umidità ed effetto popcorn nel chip	X	OC	OC	OC

Legenda:
- D → Degradazione del materiale e diminuzione del flusso luminoso;
- OC → Circuito aperto;
- SC → Cortocircuito;
- X → Nessun effetto apprezzabile.

I Power LED Flip Chip rappresentano l'ultima tecnologia disponibile sul mercato e, grazie alla peculiarità di non possedere alcun filamento interno, sono in grado di sopportare maggiori stress meccanici e garantire un'efficienza migliore ad un costo ragionevole. Come si vede dai risultati riportati sopra, in mancanza del filamento un guasto di circuito aperto si può presentare solo con il cosiddetto "*effetto popcorn*" [5]. Questa condizione consiste in una deformazione del chip di silicio a seguito dell'assorbimento e successiva espansione dell'acqua sotto forma di umidità. È un problema riscontrato raramente durante la produzione di circuiti stampati: dispositivi deformati sono inutilizzabili e vengono scartati, di conseguenza non possono in alcun modo rappresentare un problema per la sicurezza. Archi elettrici pericolosi al'interno

di un LED possono teoricamente presentarsi solo nei modelli con filamento, e solo nel raro caso in cui uno stress meccanico rompa l'involucro ed esponga i terminali spezzati del filo all'atmosfera. Le scariche elettrostatiche possono colpire il dispositivo durante la fase di manipolazione e montaggio dell'apparecchiatura: l'utilizzo di materiali isolanti appropriati riduce il rischio di scariche elettrostatiche. Inoltre i LED di potenza SMD sono generalmente corredati di dispositivi di protezione contro picchi di tensione, come varistori o diodi transil, in grado di gestire tensioni anche di alcuni kV [22]. Polarizzazione inversa e stress elettrici eccessivi possono essere gestiti opportunamente dal driver, ma nel caso questo fallisca tali tipi di guasto rappresentano la maggiore criticità a carico del Power LED. A parità di tensione un cortocircuito comporta un passaggio di corrente maggiore in brevissimo tempo con un conseguente aumento di temperatura a causa dell'effetto Joule. Nel caso di array di LED, si consiglia un pilotaggio in corrente ed un collegamento in serie dei diodi. In tal modo se ne permette il funzionamento anche in caso di cortocircuito di uno o più LED, evitando sovracorrenti e sovratensioni sui dispositivi rimanenti [23]. L'assorbimento di radiazione elettromagnetica da parte dell'involucro del chip, opacizzato ed ingiallito a seguito di degrado termico o chimico, può determinare un'ulteriore surriscaldamento della superficie del dispositivo [24].

In ogni caso questi risultati derivano da studi preliminari realizzati pensando al possibile utilizzo di LED in Zona 1, ma basati su informazioni riferite a dispositivi standards. In futuro sarà opportuno effettuare delle prove sperimentali che tengano conto dell'interazione con le atmosfere esplosive, da cui si potranno estrapolare i valori dei tassi di guasto, indispensabili per completare l'analisi di sicurezza del dispositivo Power LED.

Identificati i diversi modi di guasto, è possibile effettuare un'analisi di criticità dei guasti, ordinandoli in base alla loro pericolosità, e suddividendoli in pericolosi (D) o sicuri (S) dipendentemente dalla loro capacità o meno di innescare l'atmosfera esplosiva con archi elettrici o sovratemperature. Di conseguenza, i relativi ratei di guasto sono a loro volta divisi in pericolosi (λ_D) e sicuri (λ_S). Modi di guasto che determinano solo un circuito aperto tra terminali non esposti all'atmosfera o un degrado dei materiali e del flusso luminoso possono essere considerarsi sicuri. Viceversa cortocircuiti, stress elettrici e circuiti aperti tra terminali esposti compongono i guasti pericolosi.

L'insieme di queste considerazioni porta alla realizzazione di un'analisi FMECA ("*Failure Modes, Effects and Criticality Analysis*").

Un'analisi di diverso tipo nota come FMEDA ("*Failure Modes, Effects and Diagnostic Analisys*") sfrutta la suddivisione dei guasti in base alla possibilità di una loro rilevazione per via diagnostica, distinguendoli in pericolosi rilevati ("*DD*"), pericolosi non rilevati ("*DU*"), sicuri rilevati ("*SD*") e sicuri non rilevati ("*SU*"). Chiaramente i guasti pericolosi non rilevati sono i più importanti ai fini della valutazione dell'integrità della sicurezza.

L'identificazione di un guasto durante il funzionamento del dispositivo controllato dipende dalla presenza di un apparecchio di rilevamento attivo. Nel caso di un sistema d'illuminazione a LED il rilevamento ed il controllo di un guasto, inteso come deviazione di una variabile fisica dai parametri normali, possono essere eseguiti dal driver. Per esempio, questo è in grado di agire tramite un controllo attivo nel caso sia rilevato un passaggio eccessivo di corrente. In tal caso si parlerà di guasto pericoloso rilevato. Il fattore di copertura diagnostica DC, determinato secondo i requisiti della norma IEC/EN 61508-2, per sistemi di controllo elettronici è normalmente compreso tra 0,9 e 0,99. In particolare guasti come circuiti aperti o cortocircuiti sono solitamente rilevabili con una copertura del 100% [25]. Nel caso il driver fallisca, nessuna diagnostica può essere demandata al LED.

Da una prima analisi teorica si sono catalogati i diversi modi di guasto del Power LED Flip Chip in funzione della pericolosità e della rilevabilità (tab. 3.4). In particolare i modi di guasto più critici quali stress elettrici per sovracorrenti e sovratensioni e polarizzazione inversa vengono normalmente gestiti dal driver. D'altronde essi possono diventare pericolosi e non rilevati nel caso in cui il driver abbia un guasto e non sia più in grado di operare un controllo efficace sui parametri elettrici. I restanti modi di guasto possono essere considerati sicuri poiché i loro effetti riguardano essenzialmente fenomeni di degrado dell'efficienza del dispositivo. In ogni caso sarà opportuno confrontare ed eventualmente aggiornare questa classificazione in base alle evidenze sperimentali di test futuri.

Tabella 3.4 - Classificazione dei modi di guasto in base a pericolosità e rilevabilità per un Power LED Flip Chip.

Modo di guasto Power LED Flip Chip	Pericolosità e rilevabilità
Degradazione della capsula di resina	SU
Stress meccanico e deformazione dell'involucro	SU
Degradazione dei fosfori	SU
Dislocazione e nucleazione nel materiale del semiconduttore	SU
Elettromigrazione di particelle metalliche	SU
Passivazione vetrosa incompleta	SU
Current Crowding e alterazioni di densità di carica nei contatti	SU
Scariche elettrostatiche (ESD)	SU
Stress elettrico (EOS) da sovracorrenti o sovratensioni	DD – DU*
Polarizzazione inversa	DD – DU*
Umidità ed effetto popcorn nel chip	SD

Legenda:
- DD → Guasto pericoloso rilevabile;
- DU → Guasto pericoloso non rilevabile;
- SD → Guasto sicuro rilevabile;
- SU → Guasto sicuro non rilevabile;
- * → La doppia sigla fa riferimento ai casi in cui il driver funzioni e fallisca.

3.1.3 Calcolo dei vincoli SIL

L'integrità della sicurezza di un dispositivo in termini di indice SIL è strettamente legata a tre parametri: la tolleranza al guasto del dispositivo (HFT), la frazione di guasti sicuri (SFF) e la probabilità media di guasto pericoloso su richiesta (PFD_{avg}). HFT e SFF rappresentano dei vincoli strutturali che il LED dovrà possedere. La probabilità media di guasto pericoloso su richiesta è usata alternativamente alla frequenza media di guasto pericoloso su richiesta (PFH): entrambi rappresentano i requisiti di integrità della sicurezza in termini di probabilità, o frequenza, che il

sistema al momento della sua entrata in servizio si guasti portandosi in uno stato pericoloso. L'indice PFH viene utilizzato quando la funzione di sicurezza viene richiamata continuamente o frequentemente (superiore ad una volta l'anno). La PFD_{avg} viceversa è associata a funzioni a cui è richiesto al massimo un intervento l'anno.

Per poter fare delle considerazioni sull'affidabilità dell'apparecchio d'illuminazione LED è opportuno considerare anche l'affidabilità del driver posto a controllo e protezione dei LED stessi. Il tasso di fallimento del driver è funzione dei ratei di guasto dei diversi componenti che lo costituiscono e dipendentemente dalla tipologia e dalla qualità, i driver LED possono assumere valori molto diversi di tassi di guasto. Generalmente il valore di MTBF è dell'ordine delle decine di migliaia di ore [26] [27]. Di conseguenza, il driver può essere considerato un elemento sufficientemente affidabile, così che l'ipotesi di un suo fallimento e la richiesta di funzionamento sicuro da parte del solo LED (come dire l'intervento della sua "funzione di sicurezza") è da considerarsi limitata a non più di un anno. Pertanto il parametro da utilizzare per valutare l'integrità della sicurezza su richiesta del LED risulta essere PFD_{avg}. Alcuni driver posti sotto condizioni di temperatura elevate (superiore ai 100°C) hanno però mostrato un decadimento della vita utile stimato essere nell'ordine delle 6000h, inferiori all'anno [28]. Considerando questa situazione l'indice relativo all'integrità della sicurezza del LED dovrà essere il PFH.

3.1.3.1 Tolleranza al guasto e frazione di guasti sicuri

Il livello d'integrità della sicurezza necessario per l'applicazione del dispositivo in Zona 1 è risultato essere il SIL1. Poiché il LED ha una tolleranza ai guasti nulla [16], dalla tabella 3.5 descritta nella norma IEC/EN 61508-2 si può dedurre che la SFF del LED potrà essere inferiore del 60%.

Tabella 3.5 – Classificazione del livello SIL in funzione dell'HFT e della SFF ottenibile dal dispositivo di tipo A. Fissati una tolleranza al guasto 0 ed il target SIL 1 (evidenziati in arancione), viene evidenziata la frazione di guasti sicuri minima necessaria (in giallo).

Frazione di guasti sicuri (SFF) di un elemento	Tolleranza al guasto hardware (HFT)		
	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

Come analizzato al paragrafo 2.1.2.2, per determinare la frazione di guasti sicuri si ricorre all'uso dei tassi di guasto (14):

$$SFF = \frac{(\Sigma\lambda_{SD}+\Sigma\lambda_{SU}+\Sigma\lambda_{DD})}{(\Sigma\lambda_{SD}+\Sigma\lambda_{SU}+\Sigma\lambda_{DD}+\Sigma\lambda_{DU})} = \frac{(\Sigma\lambda_{SD}+\Sigma\lambda_{SU}+\Sigma\lambda_{DD})}{\lambda_{TOT}} \quad (14)$$

Volendo valutare la sicurezza del solo LED, è assunta una situazione in cui il driver fallisca e la diagnostica non venga eseguita. In tali condizioni la formula si semplifica (15):

$$SFF = \frac{\Sigma\lambda_S}{(\Sigma\lambda_S+\Sigma\lambda_D)} = \frac{\Sigma\lambda_S}{\lambda_{TOT}} \quad (15)$$

3.1.3.2 Probabilità media di guasto pericoloso su richiesta e frequenza di guasto pericoloso su richiesta

Determinati i vincoli strutturali, occorre verificare che il LED possa garantire una sufficiente riduzione del rischio calcolando la probabilità media, o la frequenza, di guasto pericoloso su richiesta, come indicato nella IEC/EN 61508-6 [15]. Al dispositivo elettronico è associata una funzione di tipo esponenziale. L'architettura del LED è considerabile del tipo 1oo1 dato che è sufficiente un singolo guasto pericoloso per bloccare la funzione di sicurezza. La PFD_{avg} risulta essere funzione dei tassi di guasto pericoloso, sia rilevati che non rilevati dalla diagnostica e dai tempi necessari alle operazioni di manutenzione (16):

$$\mathrm{PFD_{avg}} = 1 - e^{-\lambda_D t_{CE}} \approx \lambda_{DU}\left(\frac{T_1}{2} + \mathrm{MRT}\right) + \lambda_{DD}\mathrm{MTTR} \qquad (16)$$

dove, in dettaglio:

- t_{CE} è il tempo medio durante cui il sistema non funziona;
- T_1 è l'intervallo temporale tra due proof-tests consecutivi, cioè verifiche al banco periodiche di corretto funzionamento;
- MRT ("*Mean Repair Time*") è il tempo medio richiesto dalle operazioni di riparazione, che comprende i tempi di preparazione alla riparazione, di riparazione effettiva e di completa rimessa in servizio;
- MTTR ("*Mean Time To Repair*") è il tempo medio richiesto dalle operazioni di riparazione, comprensivo anche del tempo necessario al rilevamento dei guasti tramite diagnostica [10].

Considerando la mancanza di diagnostica si considerano tutti i guasti pericolosi come non rilevati, da cui (17):

$$\mathrm{PFD_{avg}} \approx \lambda_D\left(\frac{T_1}{2} + \mathrm{MRT}\right) \qquad (17)$$

Il calcolo del valore PFH è identico a quello di PFD_{avg}, con l'accortezza di utilizzare i relativi valori tabulati differenti che nel primo caso.

Richiamando le norme IEC/EN 61508-1 e CEI EN 50495:2010 (tab. 3.6) è immediato verificare che per rientrare nel SIL 1 è necessario che la probabilità di guasti pericolosi non sia superiore a 0,1 nel caso di bassa richiesta d'intervento, o a 10^{-8} nel caso di alta frequenza d'intervento.

Tabella 3.6 – Relazione tra SIL, probabilità media di guasto pericoloso su richiesta (PFD_{avg}), frequenza di guasto pericoloso su richiesta e fattore di riduzione del rischio equivalente secondo IEC/EN 61508-1 e CEI EN 50495:2010. Viene evidenziato il caso richiesto di SIL 1.

SIL	**PFD_{avg}**	**PFH**	**Fattore di riduzione del rischio equivalente**
N/D	$\geq 10^{-1}$	$\geq 10^{-5}$	fino a 10
SIL 1	da $\geq 10^{-2}$ a $< 10^{-1}$	da $\geq 10^{-6}$ a $< 10^{-5}$	da 10 a 100
SIL 2	da $\geq 10^{-3}$ a $< 10^{-2}$	da $\geq 10^{-7}$ a $< 10^{-6}$	da 100 a 1000
SIL 3	da $\geq 10^{-4}$ a $< 10^{-3}$	da $\geq 10^{-8}$ a $< 10^{-7}$	da 1000 a 10000
SIL 4	da $\geq 10^{-5}$ a $< 10^{-4}$	da $\geq 10^{-9}$ a 10^{-8}	da 10000 a 100000

3.2 CONSIDERAZIONI SULL'APPROCCIO PROPOSTO

Per avere un'idea dell'ordine di grandezza del tasso di guasto pericoloso che occorrerebbe per ottenere tali risultati, è possibile fare alcune osservazioni ed esempi.

Invertendo l'equazione (17) il rateo di guasto pericoloso si calcola come (18):

$$\lambda_D = \frac{PFD_{avg}}{\left(\frac{T_1}{2} + MRT\right)} \tag{18}$$

Normalmente la vita utile di un dispositivo elettronico (in cui si considera λ costante) impiegato in condizioni standard è di circa un decennio, tant'è vero che ufficialmente i tassi di guasto sono considerati costanti solo entro 10 anni di funzionamento del dispositivo in assenza di operazioni di manutenzione [19]. Di conseguenza, in tali condizioni calcoli affidabilistici per tempi superiori ai dieci anni non sono attendibili. A causa degli stress termici (sia che provengano da fonti esterne, sia propri del funzionamento del dispositivo) e in assenza di manutenzione periodica (proof test) la vita utile del dispositivo può ridursi ulteriormente. La scelta del periodo che trascorre tra due proof tests consecutivi (T1) è variabile e funzione di fattori prettamente economici (costi di smontaggio, verifica, manutenzione, ricollocamento del dispositivo, attrezzature e manodopera). Chiaramente, minore è questo tempo più controllato e affidabile sarà il dispositivo ma maggiori saranno i

costi (al limite sproporzionati). L'MRT, dell'ordine di grandezza delle ore, assume un valore molto piccolo rispetto a T1 (migliaia di ore) e può essere trascurato.

Fissata una PFD_{avg} pari a 10^{-1} e ripetendo il calcolo per una PFH pari a 10^{-5} come limiti superiori in favore della sicurezza (da tab. 3.5), imponendo alcuni valori di T1 si ottengono dei tassi di guasto pericoloso indicativi (tab. 3.7).

Tabella 3.7 – A titolo d'esempio vengono calcolati i valori di tasso di guasto pericoloso assumendo un tempo medio di riparazione standard di 24h, una PFD_{avg} di 10^{-1} e una PFH di 10^{-5}. Per rispondere ai requisiti delle norme per il SIL 1, il dispositivo LED deve possedere un tasso di guasto inferiore ai valori indicati.

Tempo tra due proof tests consecutivi T1		**Tasso di guasto pericoloso λ_D**	
		con $PFD_{avg} = 10^{-1}$	**con $PFH = 10^{-5}$**
y	**h**	**h^{-1}**	**h^{-1}**
4	35040	$5{,}69 \cdot 10^{-6}$	$5{,}69 \cdot 10^{-10}$
5	43800	$4.56 \cdot 10^{-6}$	$4.56 \cdot 10^{-10}$
6	52560	$3{,}80 \cdot 10^{-6}$	$3{,}80 \cdot 10^{-10}$
8	70080	$2{,}85 \cdot 10^{-6}$	$2{,}85 \cdot 10^{-10}$
10	87600	$2{,}28 \cdot 10^{-6}$	$2{,}28 \cdot 10^{-10}$

Come si è visto la scelta del driver può influire sulla valutazione generale della sicurezza del sistema, e nel caso l'apparecchio non garantisca un MTTF superiore ad un anno, i tassi di guasto richiesti al LED hanno valori molto bassi difficilmente rispettabili. Di conseguenza sarà opportuno studiare approfonditamente la possibilità di utilizzo di driver con un valore di MTTF sufficientemente elevato anche nelle condizioni operative più gravose in cui l'apparecchio d'illuminazione Ex potrebbe trovarsi.

Per confermare gli studi effettuati sui modi di guasto del LED e valutarne i tassi di guasto, occorre ideare una campagna di prove che permetta di determinare la pericolosità e l'affidabilità del dispositivo in relazione agli scenari tipici in cui esso dovrà operare. I test devono considerare ogni variabile in gioco e ogni guasto deve poter essere identificabile e quantificabile. Al fine di non viziare le prove, per ogni tipologia di LED sotto studio occorre predisporre di più partite di campioni provenienti da diversi produttori. Consultando la letteratura è possibile condurre i

test sapendo le modalità e gli stimoli che devono essere applicati al sistema, principalmente [21] [8]:

- alimentazione elettrica nel range nominale;
- alimentazione elettrica massima prevista dal produttore;
- applicazione di un dissipatore di calore standard;
- applicazione di un dissipatore di calore sovradimensionato;
- temperatura ambiente standard;
- temperatura ambiente minima/massima prevista dal produttore;
- clima rigido e con diversi gradi di umidità;
- assorbimento igroscopico;
- resistenza al calore e al gelo;
- esposizione ai raggi UV;
- resistenza meccanica agli impatti e alle vibrazioni;
- scariche elettrostatiche;
- temperature di saldatura dei contatti errate.

Poiché i tassi di guasto sono valori stimati, caratterizzati da una propria distribuzione di probabilità, occorre fissare un intervallo di confidenza all'interno del quale tali valori siano ritenuti plausibili. Seguendo i requisiti della norma IEC/EN61508-2, viene richiesta una confidenza minima del 90%. La campagna di prove deve essere costruita in modo tale da simulare un ciclo di vita completo del sistema, così da verificarne adeguatamente gli effetti.

La letteratura e in particolare i dati affidabilistici riguardanti i prodotti LED sono ad oggi ancora troppo generici e insufficienti per poter descrivere completamente una situazione in cui un diodo luminoso venga utilizzato senza limitazioni in un'atmosfera potenzialmente esplosiva. Solitamente le aziende produttrici forniscono informazioni inadatte per un riscontro diretto dei tassi di guasto dei loro prodotti, limitandosi ad indicare che i dispositivi non hanno subito nessun guasto in un certo lasso di tempo durante uno stress test. Tuttavia, grazie ad un interessante documento dell'azienda Philips Lumileds "*Evaluating the lifetime behavior of LED systems - The path to a sustainable luminaire business model – White Paper WP15, 2012*", è possibile fare delle speculazioni riguardo l'affidabilità dei LED [23].

Normalmente la vita utile di un LED viene erroneamente valutata solo sulla base del decadimento del flusso luminoso sotto un valore soglia, senza considerare la probabilità di accadimento di alcun guasto. Nel documento è proposto un modello affidabilistico in grado di considerare sia il decadimento luminoso sia i guasti catastrofici[11], basato su una serie di stress tests a diverse temperature di giunzione e correnti di alimentazione. Riferendosi al prodotto "*LUXEON Rebel*" della tipologia Power LED Flip Chip, sono state eseguite delle simulazioni tramite metodo Montecarlo che hanno portato ai risultati esposti in figura 3.1e figura 3.2.

Figura 3.1 – Risultati della simulazione per guasto catastrofico del LED LUXEON Rebel (Philips Lumileds) nelle condizioni operative I = 0,35A, T_j = 85°C. È rappresentato il limite di confidenza inferiore, per una confidenza del 90%.

[11] Un guasto catastrofico è un qualunque fallimento del dispositivo tale per cui si ha un'interruzione completa delle sue funzioni e non semplice degradazione.

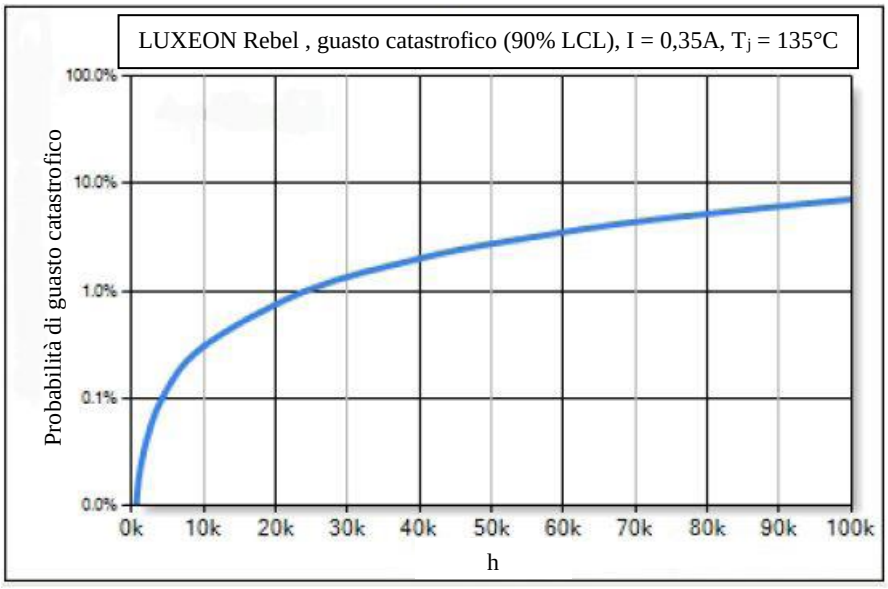

Figura 3.2 – Risultati della simulazione per guasto catastrofico del LED LUXEON Rebel (Philips Lumileds) nelle condizioni operative I = 0,35A, T_j = 135°C. È rappresentato il limite di confidenza inferiore, per una confidenza del 90%.

Come si vede dalla prima immagine, in condizioni operative I = 0,35A e T_j = 85°C, la probabilità di fallimento a 100kh è tra il 2 e il 3%. Incrementata la temperatura di giunzione fino a valori di stress (oltre le condizioni operative normali) a 100kh la probabilità di guasto catastrofico è tra l'8% e il 9% (seconda figura).
Dai risultati della tesi, la probabilità di fallimento richiesta al dispositivo per ottenere un livello di sicurezza SIL 1 (e quindi un livello EPL Gb) deve essere inferiore a 0,1 (si veda la tabella 3.6). Come mostrato, il limite viene rispettato anche oltre le 100kh, cioè oltre gli undici anni di funzionamento del dispositivo.

È fondamentale sottolineare come questi risultati appena proposti siano solo degli esempi, limitati ad un singolo prodotto in determinate condizioni di stress. Inoltre le prove condotte da Philips Lumileds considerano l'insieme dei guasti catastrofici, senza fare una distinzione tra le diverse tipologie di guasto e sulla loro criticità. In conclusione, il confronto eseguito non pone certezze assolute, che invece dovranno ricercarsi in test ideati appositamente in relazione alle atmosfere esplosive, ma fornisce dei risultati incoraggianti sulla sicurezza della tecnologia LED.

Conclusioni

L'utilizzo di apparecchiatura LED in Zona 1 è circoscritto a sistemi che utilizzano protezioni di tipo "*Ex d*", con le conseguenti limitazioni in termini di potenza installabile o degli ingenti costi legati alla custodia protettiva necessaria. Tuttavia le qualità e i vantaggi della tecnologia LED spingono l'industria ad incrementarne l'utilizzo favorendo l'impegno alla ricerca di sistemi sempre più efficienti, duraturi ed economicamente vantaggiosi. La nuova norma IEC/EN 60079-7:2015 ha segnato il primo passo ufficiale per estendere l'utilizzo di LED laddove prima non era possibile: si è riconosciuto al LED un "*Livello di Protezione dell'Apparecchio*" (EPL) Gc, consentendone un'installazione in Zona 2 come componente a sicurezza aumentata "*Ex e*". L'EPL Gb, necessario alla Zona 1, non viene precluso a priori ma per il momento non è accettato, a causa della mancanza di sufficienti informazioni riguardo la pericolosità dei guasti di tali dispositivi. Con l'intenzione di superare questo limite è stata sviluppata una procedura che permetta di valutare quantitativamente l'affidabilità e la sicurezza di un dispositivo LED, rispettando al contempo i requisiti delle norme vigenti. Il grado EPL viene normalmente utilizzato per selezionare le apparecchiature Ex, ma si basa su definizioni puramente qualitative. La procedura sviluppata consente di riconoscere l'EPL sfruttando invece dei valori numerici, quali i tassi di guasto, passando attraverso l'identificazione di un altro indice, il "*Safety Integrity Level*" (SIL).

Seguendo quello che viene chiamato "*ciclo di vita della sicurezza*" è strutturata un'analisi FMECA/FMEDA relativa al LED, indagando sui modi di guasto e i relativi effetti in concomitanza con atmosfere esplosive. Collezionando i tassi di guasto pericoloso per ogni tipo di fallimento riconosciuto, si calcolano i fattori necessari all'individuazione del SIL. Ad esso è poi associato un "F*attore di Riduzione del Rischio*" peculiare delle apparecchiature Ex, a sua volta correlabile all'EPL tramite le prescrizioni della norma IEC/EN 60079-28, specifica dei sistemi Ex utilizzanti radiazione ottica.

Applicando la procedura a ritroso, fissando come obiettivo il raggiungimento del grado EPL Gb, si è mostrato come la probabilità media di guasto pericoloso a carico del singolo LED debba essere inferiore a 0,1. Tale risultato è anche funzione dell'affidabilità del driver, poiché esso dovrà garantire un funzionamento sicuro per un tempo almeno superiore ad un anno. Il driver utilizzato dovrà cioè possedere un tempo medio al guasto maggiore di 8760h.

L'aspettativa è di lavorare sulla categoria di diodi "*Power LED Flip Chip*", riconosciuta come la più prestante, robusta ed efficiente, ma la procedura è applicabile a qualsiasi tipologia di diodo ad emissione di luce. Nonostante i limitati dati affidabilistici forniti dalle maggiori aziende produttrici di LED, è stato eseguito un confronto preliminare con i risultati di alcuni stress tests che hanno evidenziato come il basso tasso di guasto del diodo possa incontrare le richieste delle norme per il grado EPL Gb. Lontano dall'essere una conferma definitiva, il prossimo traguardo sarà quello di implementare una campagna di prove sperimentali specifiche e dai risultati ottenuti si potrà chiarire la bontà della tecnologia LED. Gli sviluppi futuri potranno gettare le basi per un'evoluzione normativa ed il LED potrà essere integralmente riconosciuto come dispositivo Ex e, permettendo lo sviluppo di apparecchi d'illuminazione più efficienti, gestibili ed economici.

Bibliografia

[1] R. Rota e G. Nano, "Introduzione alla Affidabilità e Sicurezza nell'Industria di Processo", Pitagora Editrice Bologna, 2007.

[2] P. Cardillo, "Le esplosioni di gas, vapori e polveri", Stazione sperimentale per i Combustibili, San Donato Milanese.

[3] F. Bisegna, F. Guglielmetti, M. Barbalace e L. Monti, "Stato dell'arte dei LED (Light Emitting Diodes)", ricerca di sistema elettrico per il Ministero dello sviluppo economico, Report Rds/2010/238, Università di Roma La Sapienza, 2010.

[4] K. Fumagalli, R. Faranda e L. Farnè, "Analysis of possible LED failure mode", Paper No. Am-14, PCIC 2014, Amsterdam.

[5] J. Arnold, "When the lights go out: LED failure modes and mechanisms", White Paper, DFR Solution.

[6] L. Farnè, "Studio sulle possibilità di utilizzo di Power LED in atmosfere potenzialmente esplosive in apparecchiature con protezione 'Ex e'", Tesi, Politecnico di Milano, 2013.

[7] Direttiva 94/9/CE "ATEX", 23.03.1994.

[8] IEC/EN 60079-0 "Atmosfere esplosive, Parte 0: prescrizioni generali".

[9] P. G. E. Z. Antonio Pace, "Valutazione di linee guida nella progettazione di un impianto di frazionamento aria rispondente a vincoli di sicurezza integrata (SIL) secondo le norme IEC 61508 e 61511" - Articolo, Politecnico di Milano School of Management, 2006. [Online]. Available: http://it.scribd.com/doc/157730036/1249024587-Articolo-4#scribd.

[10] IEC/EN 61508-4 "Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations", 2010.

[11] TÜV Nord Italia, "Certificazioni di Prodotto - SIL secondo IEC 61508", [Online]. Available: http://www.tuev-nord.it/it/certificazioni-di-

prodotto/sil-secondo-iec-61508-72.htm.

[12] IEC/EN 61508-1 "Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 1: General requirements", 2010.

[13] IEC/EN 61508-5 "Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5: Examples of methods for the determination of safety integrity levels", 2010.

[14] Rockwell Automation, "Progettazione del sistema in base a ISO EN 13849 e SISTEMA - Guasti sistematici", [Online]. Available: http://www.ab.com/it/epub/catalogs/3377539/5866177/3378076/7565826/Guasti-sistematici.html.

[15] IEC/EN 61508-6 "Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 6: "Guidelines on the application of IEC 61508-2 and IEC 61508-3", 2010.

[16] IEC/EN 60079-15:2010 "Costruzioni elettriche per atmosfere esplosive per la presenza di gas, Parte 15: Costruzione, prove e marcatura delle costruzioni elettriche avente modo di protezione "n"".

[17] Rockwell Automation, "Progettazione del sistema in base a IEC/EN 62061", [Online]. Available: http://www.ab.com/it/epub/catalogs/3377539/5866177/3378076/7555771/Introduzione.html.

[18] IEC/EN 90079-28 "Atmosfere esplosive, Parte 28: Protezione delle apparecchiature e dei sistemi di trasmissione che utilizzano radiazione ottica".

[19] A. Wilday, A. Wray, F. Eickhoff, M. Unruh, E. Fae, S. Halama, E. C. Lazaro e P. R. Perbal, "Determination of Safety Categories of Electrical Devices used in Potentially Explosive Atmospheres", (SAFEC) Contract SMT4-CT98-2255, Final Report, 2000.

[20] I. U. Perera, N. Narendran e Y.-w. Liu, "Accurate measurement of LED lens surface temperature", SPIE Vol. 8835, 2013.

[21] K. Fumagalli, M. Martina e P. Corbo, "Light Emitting Diodes (LED) for installation in zone 1: a feasible procedure to determine the Equivalent

Protection Level", Lo-141, PCIC London, 2015.

[22] Cree Inc., "Cree XLamp LEDs Electrical Overstress", CLD-AP29.000, 2009.

[23] Philips Lumileds, "Evaluating the lifetime behavior of LED systems - The path to a sustainable luminaire business model", white paper, 2012.

[24] Cree Inc., "Cree XLamp LEDs Chemical Compatibility", CLD-AP63, 2013.

[25] IEC/EN 61508-2 "Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related-systems", 30.06.2010.

[26] Philips Lumileds, "LED Driver Lifetime and Reliability", 2011.

[27] V. I., J. M.A., M. P.R., S. J.M. e V. G., "Comparative Analysis of the Reliability of Drivers for Power LED" - ROPEC 2015 Electronics, 2015.

[28] H. Lei e N. Nadarajan, "An Accelerated Test Method for Predicting the Useful Life of an LED Driver", IEEE Transaction on Power Electronics, Vol.26, No.8, 2011.

[29] IEC/EN 60079-11 "Atmosfere esplosive - Parte 11: Apparecchiature con modo di protezione a sicurezza intrinseca 'i'".

[30] IEC/EN 60079-14 "Atmosfere esplosive - Parte 14: Progettazione, scelta e gestione degli impianti elettrici".

[31] CEI EN 50495 "Dispositivi di sicurezza richiesti per il funzionamento sicuro degliapparecchi in relazione al rischio di esplosione", 2011.

Ringraziamenti

Due anni volati in un attimo. Sembra ieri, quando ero ancora qui sulla stessa scrivania a scrivere la prima tesi…

Ringrazio il professor Roberto Faranda e l'ingegner Kim Fumagalli per avermi dato l'opportunità e il piacere, oggi come in passato, di lavorare con loro ad un progetto capace di darmi tante soddisfazioni.

Ringrazio i miei genitori, che non hanno mai smesso di spronarmi, dandomi tutto il sostegno, la fiducia e l'affetto (e qualche raddrizzata!) più di quanto abbia mai potuto chiedere.

Ringrazio tutti i miei famigliari, ed in particolare voglio dire grazie a mia nonna per ogni suo sorriso col quale mi fa stare bene.

Ringrazio chi mi sta vicino col cuore ogni giorno e non smette mai di credere in me.

Ringrazio tutti i miei amici, vecchi e nuovi. Grazie per farmi capire con un semplice biglietto quanto può essere forte un'amicizia. Grazie per ascoltare le mie insicurezze e paure senza mai cedere, per poi riprendermi e alzarmi da terra. Grazie per condividere pensieri ed emozioni speciali. Grazie per ogni colazione prima delle lezioni, per i momenti di svago, le grigliate, i pranzi in compagnia, le gite fuoriporta e le vacanze indimenticabili. Grazie per lo studio affrontato assieme in università come a casa, o durante (troppi) simpatici "ritiri spirituali", per l'ospitalità e i momenti di ordinaria follia. Grazie per le giornate passate a Villa Braila, dove lo studio diventa occasione per vedersi e passare del tempo insieme. Grazie per aver condiviso tensioni, ansie e momenti di gioia. Grazie per le uscite del sabato sera che ti fanno dimenticare la stanchezza, nei dintorni di casa come in quel di Milano, con vecchi e nuovi compari di disavventure. Grazie per quei messaggi e telefonate inaspettate che semplicemente dopo tanto tempo ti chiedono se va tutto bene. Grazie a chi è stato lontano e chi lontano lo è adesso, ma non si è dimenticato di noi.