GESTIONE ALLARMI

EEMUA 191

Linee guida

Problematiche e soluzioni

ServiTecno srl – www.servitecno.it

Via F. Koristka 10 – 20154 Milano – tel 02 486141

Sommario

ServiTecno srl – www.servitecno.it

Via F. Koristka 10 – 20154 Milano – tel 02 486141

1. Definizioni

Nel seguito del documento ci atterremo alle definizioni previste da ISA (International Society of Automation www.isa.org):

- Allarme
- An audible or visible means of indicating to the operator an equipment or process malfunction or abnormal condition requiring an action.
- Gestione allarmi (alarm management)
- The processes and practices for determining, documenting, designing, operating, monitoring, and maintaining alarm systems.
- Sistema di allarme (alarm system)
- The collection of hardware and software that detects an alarm state, transmits the indication of that state to the operator, and records changes in the alarm state.

2. La gestione degli allarmi

La gestione degli allarmi (Alarm Management) è oggi uno dei temi che nell' automazione degli impianti sta evolvendosi più rapidamente rispetto agli altri. Ciò si può attribuire ad alcuni fattori chiave che guidano l'attenzione verso questo tema: la riduzione dei rischi e la mitigazione delle conseguenze, la sicurezza del personale e dell'ambiente, la necessità di migliorare e/o ottimizzare i sistemi di allarme presenti in impianto.

In passato l'*alarm management* non era un tema così importante e delicato. Negli anni '60-'70, era improbabile che un operatore dovesse occuparsi di più di 60-100 allarmi. Questi allarmi erano solitamente configurati usando apposite soluzioni hardware, ad esempio scatole di segnalatori luminosi per i diversi allarmi, che erano progettati e costruiti per essere altamente affidabili, con tuttavia la limitazione di essere relativamente costosi e decisamente poco flessibili. Il risultato finale di questa situazione fu la realizzazione di un sistema di allarme più generale, gestibile in funzione della quantità di allarmi che necessitavano di una pronta azione: ancora una volta, però, senza garanzia di flessibilità.

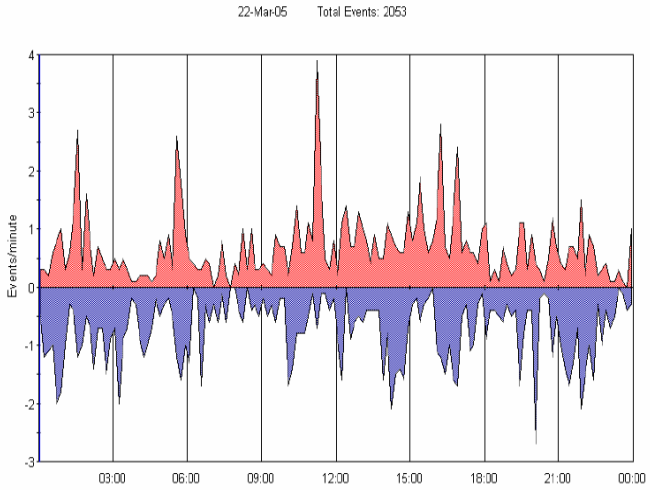
Con l'avvento di Personal Computer (PC), Programmable Logic Controller (PLC), Process Automation Controller (PAC) e Distributed Control System (DCS) affidabili ed economicamente competitivi, l'uso di sistemi *hardware-based* iniziò a declinare e divenne sempre meno comune.

Oggi tutte le funzionalità previste da quei sistemi di allarme sono proposte da sistemi realizzati con PC, PLC/PAC, DCS e il software relativo, con caratteristiche di flessibilità, ridotte dimensioni, minori costi ed utilizzo di componenti software standard e aperti.

Senza volerlo tuttavia, tutti questi vantaggi hanno portato a una crescita non intenzionale di sovraccarico di allarmi, dovuta soprattutto a:

- La richiesta di progettisti e operatori di poter gestire tutti gli allarmi di propria, ciascuno in un modo ritenuto più consono ai propri scopi e il più delle volte "perché si è sempre fatto così";
- Mancanza di coordinate linee guida nella progettazione e sviluppo. Così vengono configurati allarmi per tutte le variabili in gioco oppure per tutto quanto un utente richiede, in modo da evitare successivi reclami. In pratica l'unica linea guida pare essere "se hai un dubbio, fai uscire un allarme ";
- La capacità dei moderni sistemi di controllo di poter configurare numeri elevatissimi di allarmi senza che il sistema ne venga a soffrire in performance;
- Economicità dei sottosistemi di controllo degli allarmi, con la caduta verticale dei costi per punto allarmato;
- Flessibilità dei sottosistemi di controllo degli allarmi, che consentono di inserire e configurare allarmi in modo rapido e semplice.

Alla fine questo sovraccarico diventa però un costo. Invece di delegare la gestione di 60-100 allarmi per operatore, oggi si parla di oltre 1000 allarmi per operatore, con conseguenti effetti negativi.



Un disturbo in un processo, a causa dell'eccessivo numero di allarmi presenti, può durare più del dovuto e questa permanenza eccessiva può rendere un disturbo più grave di quanto non fosse al suo insorgere: cosa che si traduce in una diminuita stabilità e profittabilità dell'impianto, se non addirittura in un vero e proprio problema che mette in crisi l'intero sistema. Non ultimo, l'eccessivo numero di allarmi ha un effetto negative sulla serenità dell'ambiente e in particolare su quella degli operatori, stressati da troppi allarmi non sempre necessari.

Questo stato di cose ha fatto sì che varie aziende abbiano iniziato ad affrontare il problema e a formare gruppi deputati alla ricerca di soluzioni, focalizzandosi sull'analisi e la cura di sistemi di allarme. Tra queste entità (che includono PAS, TiPS, ASM), **EEMUA (Engineering Equipment & Materials Users' Association)** ha pubblicato diversi documenti sull' argomento e tra questi EEMUA 191 "Alarm Systems- A Guide to Design, Management and Procurement" - 2007, "The Alarm Management Handbook" e "Alarm Management: Seven Effective Methods for Optimum Performance", focalizzati sui problemi riscontrati nelle industrie di processo e di produzione di energia. Documento poi aggiornato nel 2014, anche in considerazione di nuovi input provenienti dal comitato ISA18.2 (vedi la White Paper sul sito www.servitecno.it)

Nel seguito di questo documento, vedremo i principi generali di EEMUA 191 e le possibili applicazioni e conseguenze, in termini di sviluppo, implementazione e coordinamento.

3. EEMUA 191: i principi generali

EEMUA ha redatto **EEMUA 191** su input di ASM (Abnormal Situation Management Consortium).

Nel seguito alcuni dei principi generale che dovrebbero guidare lo sviluppo di sistemi di allarme.

3.1. "Lo scopo di un sistema di allarme e di indirizzare l'attenzione dell'operatore verso le condizioni di impianto che richiedono interventi o azioni tempestive"

Il messaggio di questo primo principio è al contempo molto semplice e molto forte: non ci deve essere allarme se non viene poi richiesta un'azione da parte dell'operatore. Lo scopo è che tutte le segnalazioni su eventi che si verificano in impianto ma che non richiedono un intervento, non siano considerate allarmi e vengano rubricate solo come segnalazioni o "*alert*", anche se devono essere registrate in un giornale, raccolte dal sistema di controllo per essere storicizzate in un sistema di trend o visualizzate in una lista simile a quella della lista allarmi. Un segnale di *alert* deve poter essere ignorato dall' operatore senza ripercussioni sulle apparecchiature, i sistemi o le attività di impianto.

3.2. "Ogni allarme deve allertare, informare e guidare."

Questo principio per lo sviluppo di allarmi impone che tutti gli allarmi siano annunciati in modo visibile e/o sonoro, siano corredati di informazioni sull' allarme stesso e di altre che riportino come affrontarlo.

EEMUA 191 a riguardo propone delle linee guida e suggerimenti:

- Uso di liste grafiche standard (differenti colori per ogni livello di priorità);
- Realizzazione sulle workstation di annunciatori grafici a video che simulino indicatori luminosi (con differenti colori secondo la priorità);
- Segnalazioni acustiche sulle stazioni operatore usando gli altoparlanti dei PC (differente tono per ciascun livello di priorità);
- Uso di differenti livelli di priorità da tre "*Light-Medium–High*" fino a quattro "*Critical-High-Medium-Low*".

Usando i quattro livelli si suggerisce una distribuzione di allarmi che preveda 78% low, 15% medium, 5% high e 2% critical. Si sconsiglia l'uso di un maggior numero di priorità perché è dimostrato che diventa un problema per l'operatore il riconoscimento. Ogni allarme quando si presenta deve essere accompagnato da informazioni che lo riguardano - priorità, I/O *point name*, *point description*, soglia di allarme, valore attuale, tempo di insorgenza; la gestione di ogni allarme deve essere facilmente disponibile all' operatore con funzioni di click col tasto destro o su un bottone grafico presente sulla lista o sul sinottico, deve essere completa e concisa per consentirgli di far fronte alla situazione in modo rapido ed accurato.

3.3. "Ogni allarme presentato all'operatore deve essere utile e rilevante per lo stesso operatore"

A prima vista sembra un principio vago e di comune buon senso. Ma c'è di più. Gli allarmi vanno progettati per essere utili e rilevanti per l'operatore secondo le priorità, i raggruppamenti e i modi di funzionamento dell'impianto. Quindi occorre fare attenzione a progettare il sistema nel giusto numero di livelli di priorità e tener conto della distribuzione degli allarmi tra tali livelli, ma anche a discernere con cura tra quanti vanno considerati allarmi e quali vanno considerati solo delle segnalazioni di allerta.

3.4. “Ogni allarme deve avere una risposta definita”

Le risposte agli allarmi vanno progettate così da essere reattive, proattive o cognitive.

Una risposta reattiva va progettata quando un’apparecchiatura o una stato del processo richiedono un intervento dell’operatore per risolvere direttamente la situazione che si è creata (ad esempio una variabile di processo assume valori non corretti).

Una risposta proattiva sarà caratterizzata da apparecchiature o stati di processo che indicano che in un prossimo futuro sarà necessario un intervento dell’operatore per risolvere o aiutare a risolvere una situazione che si verrà a creare (ad esempio il rallentamento del flusso di un olio lubrificante). In questo caso l’operatore ha il tempo per analizzare la situazione, verificare se e dove potrà insorgere il problema e attivare il servizio di manutenzione.

La progettazione di un allarme cognitivo potrebbe essere caratterizzata dallo stato di un’apparecchiatura o di un processo che richiedano all’ operatore di inserire dei cambiamenti di attività o configurazione, anche se non è direttamente richiesta l’azione dell’operatore, che interviene secondo una sua valutazione. Ad esempio il risultato di un allarme cognitivo potrebbe essere l’attivazione d una pompa in standby in funzione di particolari condizioni della pompa primaria o del processo. È molto facile che tali allarmi crescano in quantità: tuttavia si possono trattare come semplici “*alert*” e riportarli in una lista separata.

3.6. “All’operatore deve essere consentito un tempo adeguato per poter dare la risposta definita”

A prima vista questo principio di progettazione appare di puro buon senso. Ma anche in questo caso c’è di più. Ogni allarme va valutato sia per la logica che guida l’allarme, sia per la reazione che il processo può avere a seguito di tale allarme. L’ allarme deve avere una soglia che consenta all’ operatore di avere il tempo necessario per reagire in modo adeguato allo scenario che si presenta, in base a una risposta definita per l’allarme. Ad esempio, un allarme di livello solitamente scatta quando lo stesso livello raggiunge un determinato valore. Secondo le dimensioni dei recipienti o delle vasche e secondo la velocità di riempimento/svuotamento, è bene progettare in modo corretto la soglia di allarme per consentire all’ operatore di intervenire in tempo, e in modo accurato.

3.6.1. “Il sistema di allarme deve essere esplicitamente progettato per tener conto delle limitazioni umane”

Questo principio affronta il tema dei fattori da considerare nella progettazione di un sistema di allarme: la quantità e i relativi livelli di performance, come annunciarli/presentarli. La quantità di allarmi da presentare deve essere tale da consentire al sistema di allarme di rispettare le performance richieste.

3.6.2. I livelli di performance

EEMUA 191 descrive cinque livelli di performance: Overloaded, Reactive, Stable, Robust e Predictive:

Level 1: Overloaded. È un livello che prevede una frequenza alta di allarmi per l’Alarm System con conseguente degrado del sistema. È tipico durante le installazioni di nuovi sistemi di controllo e può essere accettabile se non ci sono significative implicazioni qualora l’operatore ignori per qualche tempo il sistema di allarme, a fronte di modesti benefici (economici, di sicurezza, ambientali) che giustifichino sforzi maggiori.
In questi casi si tende a fornire all’ operatore strumenti che consentano di staccare l’annunciazione degli allarmi per consentirgli di operare su altri fronti.

Level 2: Reactive. Per la maggior parte degli impianti questo è considerabile come il minimo 'entry level'. Si ha tipicamente all' implementazione di un nuovo sistema di controllo con il minimo di *best practices*. È previsto qualcosa in più riguardio alla frquenza media di allarmi, rispetto al Level 1, tuttavia il picco di frequenza rappresenta un'inutile distrazione per gli operatori nel lungo periodo.

Level 3: Stable. È tipicamente frutto sia di attenta selezione delle variabili da allarmare, sia via razionalizzazione degli allarmi in fase di progetto, con miglioramenti sulla media e sui picchi di frequenza degli allarmi rispetto a Level 2. Problemi sono tenuti sotto controllo con revisioni regolari e miglioramento continuo, ma ci sono ancora difficoltà all' impennarsi della frequenza di allarmi. In generale può andar bene se tutto funziona, ma è assai meno utile in casi di difficoltà dell'impianto.

Level 4: Robust. Rappresenta il limite di quanto ottenibile con la tecnologia attualmente disponibile e per molti impianti è l'aspirazione di *level of performance* realizzabile. La frequenza media e di picco sono sotto controllo. Si fa ampio uso di tecniche dinamiche per migliorare la *real time performance* del sistema di allarme.

Level 5: Predictive. Questo *level of performance* mira agli obiettivi cui si aspira in EEMUA 191, ma per molti impianti non è oggi tecnologicamente raggiungibile; dove raggiungibile non è a volte giustificabile. È tipicamente un'area di ricerca e sviluppo ed è un passaggio importante per acquisire paradigmi verso modelli futuri.

Causa il crescere eccessivo degli investimenti per il salto di livello, EEMUA 191 raccomanda di preferire il livello Robust in luogo di Predictive. Nella tabella seguente si riportano gli indicatori (KPis) di livello.

KPI	**Robust**	**Predictive**
Media di allarmi per giorno	1440	144
Media di *standing alarms* per turno	9	9
Picchi di allarmi per periodo di 10 minuti	100	10
Media di allarmi per periodo di 10 minuti	10	1
Percentuale di tempo di allarme fuori target	5%	1%

Il bilancio su investimento di sviluppo e quantità di allarmi (oltre 1400 al giorno possono risultare difficili da gestire) è motivo di disaccordo tra quanto riportato in EEMUA 191 ed in altri documenti. Un ragionevole compromesso prevede di arrivare a 300 allarmi per operatore per giorno, con il livello di performance che può essere identificato come Robust+ o Robust-Predictive.

L'annunciazione degli allarmi deve tener conto del fattore umano. Alcune tecnologie disponibili sono: lista allarmi, annunciatore grafico, "toolbar" di *alarm grouping*, annunciazione sonora e luminosa. I KPI minimi di annunciazione a display su unità Video includono: colore, dimensione del testo, descrizione dell'allarme e descrizione degli indicatori di allarme. Tutte queste indicazioni di base devono mediare i valori di visibilità, angolazione, distanza, brillantezza del video... Se tutti questi fattori vengono rispettati, l'interfaccia grafica del sistema di allarme è facilmente visibile, ergonomicamente corretta e riporta le informazioni necessarie all' operatore per avviare le azioni di intervento.

L'annunciazione sonora dovrà tener conto dell'intensità del suono (circa 20 dB sopra il rumore di ambiente della *control room*), il tono (circa 1000 Hz) e il suono dell'allarme (continuo, a impulsi, crescente, etc., unico per ciascun livello di priorità). Va considerato che si dovrà sempre riportare l'annunciazione sonora della priorità più alta, onde evitare una confusione di suoni.

4. EEMUA 191: un punto di riferimento

Per elevare il *level of performance* del sistema di allarmi, il documento EEMUA 191 è largamente riconosciuto come *industry best practice*. Descrive in modo pratico strumenti e tecniche, insieme a criteri per giudicare i risultati.

Relativamente a performance di *alarm system* durante 'steady operation', EEMUA 191 contiene i seguenti criteri.

Frequenza media di allarmi nel lungo periodo	**Accettabilità**
Più di 1 al minuto	Praticamente inaccettabile
1 ogni 2 minuti	Difficile gestibilità
1 ogni 5 minuti	Gestibile
Meno di 1 ogni 10 minuti	Accettabile

EEMUA 191: Criteri relative a 'steady operation'

Per le performance in impianti con maggiori problemi, i criteri sono i seguenti:

Numero di allarmi a video nei 10 minuti seguenti un problema primario in impianto	**Accettabilità**
Più di 100	Eccessivo. Piò portare l'operatore ad abbandonare l'uso del sistema
20-100	Difficile da gestire
Meno di 10	Gestibile – una difficoltà può derivare dalla necessità di intervenire su molti di questi allarmi con risposte complesse

EEMUA 191: Criteri relativi a condizioni difficili in impianto

Questi target derivano da principi relativi ai fattori umani, ma si adattano ampiamente al ruolo del tipico operatore in un impianto industriale. In una situazione in cui un operatore subisce un sovraccarico e deve operare con un ampio range di task - oltre a monitorare l'impianto via HMI, possono non essere sufficientemente aggressive.

In altri casi di situazioni più "tranquille", possono rivelarsi conservative.

Ma come si può misurare i diversi parametri?

5. Un set di metriche definite per sistema di allarme

Per differenziare i livelli di performance di sistemi di allarme, abbiamo citato molti parametri da tenere sotto controllo. Diventa quindi necessario definire più nel dettaglio le metriche del sistema, ovvero come misurare i parametri in modo quantitativo. Tra le più utili se ne sono scelte tre, sebbene non le si possa considerare completamente indipendenti. Esse caratterizzano l'*Alarm System performance* in modo potente, ma sono anche semplici da calcolare e possono essere calcolate utilizzando programmi che girano in modo autonomo: possono essere calcolate dal giornale degli allarmi, storicizzate sul sistema di controllo o catturate da un archivi separato su PC. Allo scopo si possono utilizzare sistemi specifici, fogli di calcolo Excel o database Access con le opportune *query*.

Le metriche, definite come "numero per operatore", sono le seguenti:

- **Frequenza media di allarme**. Abitualmente espresso in "numero per ora", è il numero totale di allarmi annunciato all' operatore (esclusi gli eventi inviati solamente al giornale) durante il periodo di analisi, diviso per il numero totale di ore considerato.
- **Massima frequenza di allarme**. Abitualmente espresso in "numero per ora", rappresenta il caso peggiore di carico in periodi di dieci minuti. Si suddividono i dati nell' *alarm journal* in piccolo periodi di dieci minuti, si prende il caso peggiore di numero di allarmi annunciato all' operatore (esclusi gli eventi inviati solamente al giornale) e lo si moltiplica per 6, per avere un valore per ora.
- **% di ore in cui si sono presentati più di 30 allarmi per ora**. È la misura semplice che dice la difficoltà subita dal sistema di allarme. Si calcola dividendo l'*alarm journal* in periodi successivi di un'ora e calcolando per ciascun periodo il numero di allarmi che si sono presentati all' operatore (esclusi gli eventi inviati solamente al giornale). Si esprime normalmente in percentuale.

Una volta viste le possibili metriche, vediamo quale può essere il livello di performance appropriato in impianto

6. Quale livello di performance è appropriato?

Il *performance level* che può considerarsi appropriato per ciascun sistema di allarmi, dipende da moti fattori.

Tra questi si segnalano:

6.1. Ruolo e responsabilità dell'operatore di Control Room

Si possono avere due tipi di figure di operatori di *Control Room*, diversificati dalle incombenze di ruolo. In un primo caso l'operatore risiede stabilmente in sala controllo e la sua responsabilità è dedicata a gestire il processo con l'uso di sistemi DCS, SCADA, PLC, … e i relativi Alarm System. In altri casi, però, l'operatore di *Control Room* è anche responsabile di coordinare il traffico (es marina, aviazione) intorno all' impianto, gestire le comunicazioni (es radio, tannoy), autorizzando le attività e muovendosi nell' impianto per misurazioni particolari o attività manuali. Nel primo dei due casi, il livello di performance appropriato non è da considerare una scelta critica: semplificando molto, si può dire che l'operatore può permettersi di dedicare gran parte del suo tempo e della sua attenzione alla gestione dell'*Alarm System*.

6.2. Complessità

La crescita di complessità, a vario titolo, porta alla necessità di incrementare il livello di performance dell'*Alarm System*. Si può semplificare il concetto dicendo che se l'operatore impiega molto tempo a comprendere le

implicazioni e a dare la corretta risposta a ciascun allarme, allora in qualunque periodo di tempo può permettersi di riceverne solo alcuni, e ancora essere in grado di gestirli efficacemente.

6.3. Le conseguenze di mancanza di azioni

Per tutti gli *asset* in impianto esiste un livello di severità associato alla eventuale mancanza di risposta dell'operatore ad un allarme: questo caratterizza le priorità dei diversi allarmi. L'applicazione di standard quali IEC 61508 e il rispetto di criteri di rischio porteranno a una normalizzazione tra i vari *asset*, ma in alcuni casi (vecchi impianti o processi particolari), si continuerà a fare assegnamento sulla capacità di azione dell'operatore in risposta agli allarmi per evitare situazioni di pericolo. È chiaro che in questi casi sarà appropriato un alto livello di performance dell'*Alarm System*.

6.4. La velocità di risposta richiesta

Così come si è visto che possono esserci conseguenze per la mancanza di azioni, occorre anche considerare la velocità con cui l'operatore deve reagire all' allarme per evitare conseguenze all' impianto. Alcuni asset saranno caratterizzati da dinamiche di processo più veloci che per altri (per esempio processi con gas che sono a rischio di instabilità e con reazioni fortemente esotermiche). In questi casi occorre realizzare sistemi di allarme con un livello di performance decisamente elevato.

6.5. "Centralità dell'impianto in allarme

Anche se la conseguenza di una mancata azione porta l'impianto verso uno *shutdown* in sicurezza, non va dimenticato che può essere molto importante anche la relazione tra l'impianto in allarme e altri impianti ad esso collegati e con sistemi di allarme separati. Pensiamo allo *shutdown* di un sistema di trattamento acque: per un periodo non troppo lungo, in funzione delle capacità di recettività, non si creano gravi problemi. Al contrario può essere estremamente grave la caduta di un'unita di processo primaria (es. un processo di *ethylene cracker*) in termini di impatto con le unità associate. Sono due casi in cui I livelli di performance possono essere meno diversi: meno elevate nel primo e decisamente più elevati nel secondo.

6.6. Centralizzazione dell'Alarm Management nel settore Energia

In considerazione di quanto visto e ragionando sul futuro dei sistemi di automazione di impianto nel settore Energia, gli sforzi dovranno tenere in considerazione l'applicazione dei principi sopra menzionati di progettazione dei sistemi di allarme per tutti i sistemi di controllo presenti in impianto –indipendentemente se basati su un'unica piattaforma hardware o piattaforme multiple (ad es., insiemi di DCS, PAS e PLC/SCADA).

Il ragionamento che sta dietro questo assunto è semplice: si raccomanda di avere un sistema di allarmi centralizzato che sia capace di fare il *logging* degli allarmi in impianto e di presentarli all' operatore in un modo unificato e coordinato, così da ottimizzare le operazioni. Per poter sviluppare un sistema di allarmi centralizzato, deve essere applicata una comune base di progettazione per tutti i sottosistemi, così da coprire tutto il sistema di automazione in impianto nella sua generalità. Questa base di progettazione dovrebbe includere i criteri di priorità, i colori per gli allarmi in funzione delle priorità, il metodo di annunciazione sonora per i diversi tipi di allarme, le strategie di tacitazione e l'azione richiesta all' operatore per ciascun allarme. Se tutti i sottosistemi di controllo saranno stati progettati secondo la stessa filosofia di progetto, il sistema centralizzato si rivelerà utile per la gestione dell'impianto.

6.7. Livello di automazione e strategia di fall-back

Al crescere del livello di automazione in impianto, diminuisce la richiesta di intervento manuale dell'operatore: si potrebbe quindi pensare a un più basso livello di performance dell'*Alarm System*. Tuttavia, ciò che è più importante è come avviene la transizione a un sistema di controlli degradato, quando questo sistema ad elevata automazione cade per una qualunque ragione: se la transizione è tranciante (es. si passa direttamente da un controllo predittivo multi variabile, alla manipolazione delle valvole), allora è bene che il livello di performance dell'*Alarm System* venga studiato con attenzione, per poter operare anche con minori livello di automazione.

6.8. I costi di implementazione di più alti livelli di performance

In impianti dove sono operanti vecchi sistemi di controllo (DCS, SCADA, PLC, …) il costo di miglioramento del livello di performance dell'*Alarm System* può essere molto alto. In taluni casi tale azione addirittura non è praticabile. In questi casi, una volta che siano studiati e garantiti gli appropriati criteri di rischio, si possono ottenere maggiori vantaggi dal miglioramento delle performance dell'impianto (economici, di sicurezza ed ambientali) che dagli sforzi necessari per elevare a un più alto livello di performance l'*Alarm System*.

In teoria la scelta del livello di performance è *indipendente* dalle dimensioni dell'impianto e dal numero di operatori. Ciò avviene perché, in questa visione, la definizione di ciascun livello si basa su metriche quantitative che sono espresse in numeri assoluti per operatore (es. numero di allarmi per ora). Al crescere delle dimensioni dell'impianto sotto il controllo di ciascun operatore (ad esempio misurata con il numero di *control loop*) aumenta lo sforzo che si deve porre nell'*Alarm System* per raggiungere un dato livello di performance.

La scelta di quale sia il livello di performance appropriato dell'*Alarm System* potrà variare tra i vari asset, ma come regola generale si consideri che più sono alti i livelli di performance dell'*Alarm System*, più alta sarà la disponibilità e la sicurezza dell'impianto.

7. Strumenti Software - Le caratteristiche

Oltre alla progettazione, per far sì che il sistema di allarmi operi in accordo con i *Key Performance Indicator* e vada incontro ai concetti di *Human Factors Engineering*, saranno necessari degli strumenti software, con caratteristiche e funzioni che assicurino che le performance dell'intero sistema siano in accordo con i risultati desiderati (e specificati). Dovranno quindi essere incluse funzioni quali:

- *Alarm grouping*,
- Soppressione di allarmi ridondanti,
- Schermatura dei numerosi allarmi generate dalla stessa variabile,
- Soppressione degli allarmi dovuti ad una condizione di fuori servizio,
- Soppressione degli allarmi in funzione del modo operativo dell'impianto,
- Soppressione degli allarmi durante eventi particolari (*major event*),
- Gestione degli allarmi dovuti ad apparecchiature sotto test.

Sebbene EEMUA 191 identifichi - come possibili funzioni avanzate per il sistema d' allarme, il rilevamento intelligente di errore e l'automatico *alarm load shedding*, è bene notare che questi metodi sono sia sperimentali sia molto costosi, oppure entrambe le cose: quindi nel seguito si eviterà di trattare questi due argomenti.

Alarm grouping è una funzione facilmente realizzabile in un *alarm system*. In modo simile ai sistemi di annunciazione allarmi realizzati con una serie di luci, è possibile raggruppare allarmi secondo un attributo che abbia senso nel progetto dell'impianto. EEMUA 191 prevede che I raggruppamenti di allarmi siano progettati in modo che tutti i membri del

gruppo abbiano la stessa priorità: obiettivo che diventa non realistico se gli allarmi vengono raggruppati per sistema o area di impianto.

Un paio di raggruppamenti logici possono essere:

- Raggruppamento di allarmi basato su livello di priorità. Quando diventa attivo un allarme con un particolare livello di priorità, si evidenzia il simbolo grafico del gruppo di priorità lampeggia. Se tutti gli allarmi che sono attivi nel gruppo sono riconosciuti (*acknowledged*), ma non resettati, allora il simbolo grafico resta fisso in evidenza. Se tutti gli allarmi del gruppo di priorità sono resettati, allora il simbolo grafico del gruppo tornerà "*inactive*".
- Raggruppamento di allarmi basato su *plant system*. Questo non supporta le raccomandazioni di EEMUA 191 per tutti gli allarmi che hanno la stessa priorità; tuttavia, può essere più logico per l'operatore da indirizzare ed analizzare. Con questo approccio, il simbolo grafico per il gruppo di allarmi dovrà essere multi-stato. Questo elemento grafico multi-stato sarà guidato dal più alto livello di priorità degli allarmi che sono attivi nel gruppo. Ad esempio, se in un *alarm group* sono attivi allarmi di priorità 1, 2 e 3 (*unacknowledged*), lampeggerà il simbolo grafico appropriato per gli allarmi di priorità 1. Se tutti gli allarmi del gruppo sono riconosciuti, allora il simbolo grafico resta evidenziato col colore proprio del più alto livello di priorità. Se gli allarmi sono resettati, o un altro allarme si aggiunge alla lista degli allarmi attivi, l'elemento grafico dovrà essere in grado di monitorare l'*alarm group* e modificare colore e stato (lampeggiante o fisso) in base a queste ultime condizioni.

La soppressione di allarmi va valutata come un addendum alla progettazione prudente del sistema di allarmi, piuttosto che mantenere allarmi che non si uniformano ai principi di progettazione originale.

EEMUA 191 descrive cinque livelli di soppressione di allarmi:

1. La soppressione di allarmi ridondanti si può applicare quando si trovano più punti di I/O usati per un singolo stato. Questa situazione si può ritrovare in *Safety Instrumented Systems* (SIS), sistemi di protezione, etc. In questi casi, lo stato di allarme per gli I/0 ridondanti andrebbe progettato in modo appropriato per ridurre il numero di allarmi e conservare l'integrità degli obiettivi logici di progettazione del sistema. Ad esempio, se un BMS ha input ridondanti per l'avviamento (due su tre per avviare), allora un allarme associate a questa condizione andrebbe condizionato in modo che sia attivo solo quando due su tre input sono attivi.
2. Schermatura logica può essere aggiunta all' *alarm system* per affrontare situazioni in cui una misura nel processo genera vari punti di allarme. Un esempio può essere il livello di una vasca. Se si super ail livello **Hi-Hi** in una vasca, è ovvio che anche il livello High è stato superato. Quindi, in questo caso, l'*alarm system* dovrebbe essere progettato in modo tale che il livello **High** venga mascherato dall' attuazione dell'allarme di livello **Hi-Hi**.
3. Condizioni di fuori servizio (a livello di apparecchiature, sistema o impianto) possono spesso creare allarmi che sono non necessari. Detto questo, l'alarm system dovrebbe essere progettato per includere condizioni di mascheramento degli allarmi in condizioni di stati di fuori servizio. Un esempio di tale condizione si può avere nel monitoraggio di flusso ridotto (low) per una pompa o un insieme di pompe. Quando lo stato della pompa, o dell'insieme di pompe, è di fuori servizio, l'allarme **low** dovrebbe di conseguenza venire mascherato.
4. Sebbene ci sia similarità con la soppressione di allarmi per fuori servizio, la soppressione di allarmi per modalità operativa viene trattato a parte. La soppressione di questi allarmi si può applicare in modo che quei particolari allarmi associati alla modalità operativa, siano abilitati o mascherati in funzione delle condizioni di operazioni in quel momento dell'impianto (sistema, apparecchiature). Tra le modalità per cui si raccomanda di operare una soppressione di allarmi si includono *start up, shut down, steady state operation,* manutenzione o variazione di carico. Siccome alcuni stati si possono sovrapporre, occorre analizzare con molta cura come la soppressione logica viene formulata.
5. La soppressione di allarmi quando ci sono eventi particolari (*major event*) si può applicare per ridurre l'insorgere di molti allarmi nei periodi temporali in cui il traffico di allarmi può crescere in modo troppo elevato. Ad esempio, durante l'avviamento di un impianto numerose azioni avvengono in automatico per garantire che le operazioni avvengano in modo corretto. Queste attività possono però generare molti allarmi perché i valori

controllati in questa fase possono essere diversi da quelli previsti per la conduzione normale dell'impianto. Questa forma di soppressione di allarmi può richiedere grandi sforzi per essere implementata.

Gli allarmi generati dalle apparecchiature sotto test possono essere gestiti con la soppressione attraverso l'aggiunta di maschere logiche. Queste andrebbero aggiunte a livello logico di apparecchiature e dovrebbero tenere in considerazione la necessità di identificare il periodo temporale in cui il test viene condotto, quando un test si è concluso e come gli allarmi andrebbero gestiti se il tempo di test diventasse più lungo del previsto o del ragionevole.

8. Conclusioni

EEMUA 191 'Alarm systems - a guide to design, management and procurement' considera la configurazione degli allarmi, la *human interface* (presentazione degli allarmi), l'*alarm processing* e il controllo del sistema, sia per sistemi di allarme relativi alla sicurezza che per gli altri processi.

Alcune tra le linee guida relative agli *alarm system* si possono così riassumere:

- Il sistema di allarme va progettato in accordo con le norme IEC 61508, a SIL 1 o 2, con la designata affidabilità.
- Il sistema di allarme deve essere indipendente dal *process control system* ed altri sistemi di allarme (salvo riferimenti alla sicurezza).
- Agli allarmi vanno assegnate priorità per garantire che gli allarmi più critici ricevano con massima urgenza l'attenzione dell'operatore.
- L' operatore deve disporre di una chiara e scritta procedura di risposta per ciascun allarme, che sia semplice, inequivocabile e invariata - e sulla quale sia stato istruito.
- Gli allarmi devono essere presentati in modo palese secondo priorità, distinti dagli altri allarmi e restare alla vista finché risultano attivi.
- Il carico di lavoro e la performance dell'operatore vanno definiti e verificati.
- Gli allarmi che non sono designati per sicurezza (*safety*) devono essere attentamente progettati, così da garantire la riduzione di domanda dei sistemi di sicurezza.
- La configurazione degli allarmi (documentata e controllata) deve consentire agli operatori di fare le corrette valutazioni ed intervenire in un tempo appropriato.

Anche la presentazione degli allarmi deve rispondere a determinate linee guida:

- L' interfaccia operatore deve essere adatta a presentare gli allarmi, sia con pannello annunciatore, indicatori individuali per allarme, schermi video, ….
- Le liste degli allarmi vanno correttamente strutturate per garantire che gli allarmi a maggior priorità siano prontamente identificati, che quelli a bassa priorità non vengano dimenticati e che la lista allarmi resti sempre leggibile.
- Gli allarmi devono essere presentati nel campo visivo dell'operatore con uno stile di presentazione consistente (colori, lampeggio, nomenclatura convenzionale).
- Ogni allarme deve fornire all' operatore una informazione sufficiente sulle condizioni dell'allarme, le parti di impianto coinvolte, l'azione richiesta, la priorità, la temporizzazione di insorgenza e lo stato dell'allarme chiaramente identificato.

Alle presentazioni a vista, si possono aggiungere annunci sonori a un livello di volume decisamente più alto del rumore di fondo dell'ambiente. Qualora siano molti gli annunci sonori, occorre che siano tra di loro diversi per essere facilmente identificabili (volume, intensità, tono, …).

9. Bibliografia

- The Engineering Equipment and Materials Users' Association, 2007. "Alarm Systems-A Guide to Design, Management and Procurement". EEMUA Publication 191, Second Edition. Published by CPI Antony Rowe, Eastbourne. ISBN 0-85931-155-4. (http://www.eemua.co.uk)
- https://www.eemua.org/Products/Publications/Digital/EEMUA-Publication-191.aspx
- https://en.wikipedia.org/wiki/Alarm_management
- Hollifield, Bill; Habibi, Eddie, 2006. "The Alarm Management Handbook-A Comprehensive Guide". Published by Fidlar Doubleday, Kalamazoo, MI 49009. ISBN 0-9778969-0-0.
- HSE, Better Alarm Handling, Information Sheet – Chemicals Sheet No 6
- Hollifield, Bill; Habibi, Eddie, 2007. "Alarm Management: Seven Effective Methods for Optimum Performance". Published by ISA, Research Triangle Park, NC 27709. ISBN 978-1-934394-00-7.
- International Society of Automation - ISA, 2000. "Fossil Fuel Power Plant Human Machine Interface: Alarms". Recommended practice ISA-RP77.60.02-2000 (R2005). Published by ISA, Research Triangle Park, NC 27709. ISBN 1-55617-737-2.
- Occupational Safety & Health Administration (OSHA). "Process Safety Management ofHigh1y Hazardous Chemicals". Standard 29 CFR 1910.119. Available via Internet at http://www.osha.gov.
- Bransby ML and Jenkinson J, The Management of Alarm Systems, HSE Contract Research Report 166/1998 ISBN 07176 15154, First published 1998
- International Society of Automation - ISA, 2007. "Alarm Management – Current State and Direction for Alarm Management Guidelines – Presented at ISA EXPO 2007 – Houston, Texas – www.isa.org
- Health & Safety Executive - UK - Control of Major Accident Hazards (COMAH) - Technical Measure Document - CHID circular CC/Tech/Safety/9 –
- ISA draft standard S18.00.02 - Management of Alarm Systems for the Process Industries