

# Sistemi di Controllo e Supervisione

## Analisi situazioni emergenza e ripristino

### RICAMBI/RIPARAZIONI

Con la verifica in dettaglio del parco ricambi (e dell'installato) sarà possibile individuare potenziali criticità. Capire quali sono le parti obsolete nonché avere la situazione di quali sono state le riparazioni in passato.

### COPIE DI SICUREZZA E DOCUMENTAZIONE

Verifica di quali sono i backup esistenti, il loro stato nonché l'individuazione dell'ubicazione della documentazione di sistema (supervisione e controllo) e la valutazione della creazione di un sistema centralizzato ove salvare documentazione e backups.

### SITUAZIONI CRITICHE

La combinazione di tutte le informazioni acquisite durante la visita ispettiva (da fare prima dell'analisi delle situazioni di emergenza e ripristino) può aiutare ad identificare potenziali situazioni di emergenza e quali potrebbero essere i passi per velocizzare la fase di ripristino. Verrà valutata la preparazione di eventuali procedure specifiche in funzione della tipologia del sistema di supervisione e controllo attualmente installato.

### ACCESSO REMOTO

Verifica della possibilità di un sistema di accesso remoto attivabile su richiesta per attività di supporto tecnico durante situazioni critiche.



### PREREQUISITI

L'analisi di potenziali situazioni di emergenza e ripristino è uno dei risultati naturali di una visita ispettiva. In quest'ottica si assume che tutte le informazioni relative a quanto installato (sistemi di supervisione e controllo) siano già state acquisite.

### PRIMA DELLA VISITA

Vi sono alcune informazioni e documenti che potrebbero essere molto utili se disponibili prima della visita non solo per definire meglio lo scopo della visita ma anche per ottimizzare i tempi e la durata della visita. Di seguito alcuni esempi:

- Copia del registro delle problematiche incontrate durante il servizio dei sistemi di controllo e supervisione,
- Copia dei backup dell'applicazione (se presenti)
- Copia delle procedure di gestione emergenza, di backup e fasi di ripristino (se presenti)
- Valutazione iniziale della possibilità di installare un sistema di accesso remoto su richiesta (da verificare con il personale IT presente in sito sia in funzione delle procedure di cyber-security aziendale sia per le tecnologie utilizzate nell'applicazione).

### CARATTERISTICHE DELL'ANALISI

La gestione di potenziali situazioni di emergenza e delle relative procedure di ripristino è un passo molto importante focalizzato sul ripristino dell'operatività del sistema dopo un guasto di una certa rilevanza, guasto di sistema, situazioni di dati corrotti. Per la maggior parte degli utenti sembra essere sufficiente fare un backup dell'applicazione. In realtà quest'analisi tiene conto di vari aspetti del software applicativo (applicazione e sistema di supervisione), sistema di controllo (n tutti i suoi componenti) e l'infrastruttura di rete.

L'analisi può risultare complessa nel momento in cui l'installato è basato su sistemi e tecnologia obsolete e dove un parco ricambi adeguato gioca un ruolo importante nelle fasi di ripristino dell'operatività del sistema/applicazione.

### PRINCIPALI BENEFICI DELL'ANALISI

Il principale risultato dell'analisi è l'individuazione di potenziali criticità del sistema di controllo e supervisione, la definizione delle procedure per il ripristino dell'operatività e la creazione di un sistema centralizzato ove avere accesso ai vari backups, documenti e procedure.

Dall'acquisizione delle informazioni durante la visita e la relativa analisi posso scaturire elementi utili per la definizione di adeguati piani di manutenzione nonché l'individuazione di potenziali rischi che posso portare a situazioni di emergenza.

### SCOPO LAVORI DURANTE LA VISITA IN SITO

Vi sono varie aree che dovranno essere analizzate, alcune di queste potranno essere specifiche all'applicazione, la tecnologia utilizzata ed altri fattori. Di seguito una lista delle attività di analisi più comuni:

- Verifica della tolleranza del sistema a situazioni di guasto (necessità di UPS, parti ridondanti, immagini HDD, clonazione stazioni etc.);
- Validazione delle copie di emergenza "backup" (copie recenti, gestione versioni, dischi ripristino etc.)
- Analisi della documentazione di sistema (cosa è disponibile, ubicazione documentazione, creazione – ove possibile – della versione elettronica della documentazione);
- Creazione (ove possibile) di un Sistema di centralizzazione delle informazioni ove salvare i backups, la documentazione di impianti e le procedure sia manutentive che di ripristino;
- Validazione delle versioni del Sistema di controllo e supervisione (versioni software, hardware, firmware) per determinare cosa è necessario, cosa è obsoleto ed individuare gli strumenti utili per la fase di ripristino;
- Analizzare con il personale dedicato alla manutenzione potenziali scenari di guasto per meglio identificare le procedure di ripristino necessarie;
- Verifica dell'attuale system di diagnostica e relativa analisi per individuare aree di miglioramento;
- Ove possibile, fare test su potenziali situazioni di emergenza.