La valutazione dei rischi di cibersicurezza (1) nei sistemi strumentati di sicurezza (SIS) degli impianti di processo

La sempre più diffusa digitalizzazione dei sistemi di automazione industriale, della loro interconnessione ad internet e dell'utilizzo di dispositivi digitali mobili (PC, chiavette USB , LAPTOP ecc) sia per il controllo operativo, sia per le attività di manutenzione locale e/o a distanza, rende gli impianti di processo vulnerabili ad eventuali attacchi informatici interni e/o esterni, intenzionali oppure casuali.

Il numero di incidenti negli impianti di processo e nelle infrastrutture critiche continua ad aumentare rendendo necessaria una gestione dei rischi informatici oltre a quanto previsto nella norma ISO IEC 27000 (Sistemi di gestione della sicurezza delle informazioni) anche in accordo alla IEC 62443 (Security for automation and control systems). Quest'ultima norma, derivata dalla ISA99 (Industrial Automation and Control Systems Security), riguarda in particolare i sistemi di controllo industriale per i quali sono necessari adeguati livelli di sicurezza (Security Level) nell'operatività e nella manutenzione.

Le reti informatiche aziendali IT (Information Technology –relativa al trattamento dei dati aziendali per il personale, gli acquisti, le vendite, l'amministrazione, ecc.) ed OT (Operational Technology -relativa al controllo di processo tramite DCS, PLC,SCADA, SIS, ecc.) nate inizialmente separate sono sempre più interconnesse tra di loro, tramite SAP ad esempio, ed alla rete intranet e/o internet. Si ritiene spesso che la funzione aziendale che si interessa dei sistemi informatici IT, controlli adeguatamente anche la rete OT mediante "fire walls" multipli e/o sistemi di rilevazione intrusioni che non sono spesso sufficienti essendo anch'essi vulnerabili.

I sistemi SIS relativi agli allarmi e blocchi automatici devono avere, secondo quanto previsto dalla IEC 61511 (Sicurezza funzionale-Sistemi strumentati di sicurezza per il settore industria di processo), un adeguato livello di affidabilità SIL (Safety Integrity Level) per ridurre il rischio specifico al valore stabilito. La recente versione IEC 61511 del 2016 prevede due specifici riferimenti per la cibersicurezza dei SIS:

- punto 8.2.4 E' necessario effettuare una valutazione dei rischi di sicurezza (informatica) del SIS e dei suoi componenti
- punto 11.2.12 Il SIS dovrà essere progettato in modo da avere la necessaria resilienza contro i rischi di sicurezza (informatica) identificati.

Sede Legale: Via Lomazzo 51 – 20154 Milano – Tel. +39-02-99702635 – Fax +39-02-91708502
C.F. e P.IVA 08747880964 – email: do.barone@ tiscali.it - Ind.Pec: do.barone@pec.it – N.REA: MI-2046358
Capitale sociale: 20.000 € i.v.

Da quanto sopra ne deriva che è necessario effettuare una valutazione dei rischi di cibersicurezza per i SIS ed adottare i necessari SL (Security Level) in accordo alla IEC 62443-3. Questi SL, a differenza dei SIL che sono valutati numericamente in probabilità, sono definiti da vettori di 7 FR (Requisiti Funzionali) con valori da 1 a 4 che riguardano :

- Controllo autenticazione e identificazione
- Controllo utilizzo
- Integrità sistema
- Confidenzialità dati
- Limitazione flusso dati
- Risposta tempestiva all'emergenza
- Disponibilità risorse

Dopo la definizione dei SL è necessario verificare in campo che i SIS installati abbiano i SL richiesti e se necessario adottare le misure correttive.

La valutazione dei rischi di cibersicurezza e/o la gap analysis secondo la IEC 62443-3 degli allarmi e blocchi automatici ad alta affidabilità degli impianti di processo, può essere effettuata da specialisti (strumentisti) esperti di SIL secondo IEC 61511, con il necessario supporto degli specialisti aziendali della rete IT e OT di stabilimento.

Milano, 23 giugno 2016

Ing. D. Barone

Nota(1) : Cibersicurezza , secondo ISO/IEC, è la protezione della confidenzialità, integrità e disponibilità del ciberspazio che è l'ambiente complesso derivante dalla interazione di persone, software e servizi internet mediante dispositivi tecnologici e reti connesse ad esso, che non esiste in alcuna forma fisica.

Sede Legale: Via Lomazzo 51 – 20154 Milano – Tel. +39-02-99702635 – Fax +39-02-91708502
C.F. e P.IVA 08747880964 – email: do.barone@ tiscali.it - Ind.Pec: do.barone@pec.it – N.REA: MI-2046358
Capitale sociale: 20.000 € i.v.