

Quaderni Clusit

007

**Introduzione alla protezione di
reti e sistemi di
controllo e automazione
(DCS, SCADA, PLC, ecc.)**

Enzo M. Tieghi



Clusit
Associazione Italiana
per la Sicurezza Informatica

Introduzione alla protezione di reti e sistemi di controllo e automazione (DCS, SCADA, PLC, ecc.)

Enzo M. Tieghi



Quaderni CLUSIT – Maggio 2007

CLUSIT

Il CLUSIT - Associazione Italiana per la Sicurezza Informatica, è una associazione "no profit" con sede presso l'Università degli studi di Milano, Dipartimento di Informatica e Comunicazione, fondata nel luglio 2000.

Le principali attività del CLUSIT sono:

- la diffusione di una cultura della sicurezza informatica rivolta alle Aziende, alla Pubblica Amministrazione ed ai cittadini;
- l'elaborazione sia a livello comunitario che italiano di leggi, norme e regolamenti che coinvolgono la sicurezza informatica;
- la definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza ICT;
- la promozione dell'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

I soci del CLUSIT sono rappresentativi dell'intero "sistema Paese", in particolare della ricerca, dell'industria, del commercio, del settore bancario ed assicurativo, della Pubblica Amministrazione, della Sanità, dei servizi, delle telecomunicazioni e di Internet.

Copyright e Disclaimer

Copyright © 2007 Enzo M. Tieghi.

Copyright © 2007 CLUSIT

Tutti i diritti sull'Opera sono riservati all'Autore e al Clusit.

Sono tuttavia attribuiti i seguenti diritti:

1. I Soci Clusit fruitori dell'Opera hanno il diritto di utilizzare l'Opera nell'ambito della propria attività professionale purchè: a) riconoscano la paternità dell'Opera in capo all'Autore e al Clusit; b) non la utilizzino per scopi commerciali; c) non creino opere derivate e/o alterino l'Opera e/o la trasformino e/o la sviluppino.
2. I diritti attribuiti ai Soci Clusit sopra riportati sono estesi a tutti i fruitori dell'Opera dopo che la stessa sarà rilasciata in forma elettronica sul sito www.clusit.it in area pubblica.

L'Autore e il Clusit non garantiscono che l'Opera sia esente da errori. Qualora vengano segnalati errori, nel limite del possibile si provvederà a correggerli nelle eventuali edizioni successive.

L'Autore e il Clusit non assumono alcuna responsabilità in relazione al contenuto dell'Opera e/o ai risultati attesi e/o ai risultati conseguenti all'uso della stessa e, pertanto, non risponderanno di eventuali e qualsivoglia danni diretti e/o indiretti che dovessero derivarne.

In particolare non viene garantito che il contenuto dell'Opera sia esauriente, completo, preciso o aggiornato.

Eventuali denominazioni di prodotti e/o aziende e/o i loghi e/o i marchi e/o i segni distintivi eventualmente citati nell'Opera sono di esclusiva proprietà dei rispettivi titolari.

Presentazione

I sistemi d'automazione, protezione e controllo sono stati in questi ultimi anni oggetto di particolare attenzione perché si tratta di fatto della componente "intelligente" che governa gran parte delle infrastrutture critiche ed un loro malfunzionamento può riflettersi immediatamente sulla nostra vita di tutti i giorni. Si tratta molto spesso di sistemi caratterizzati da stringenti requisiti di sicurezza: in inglese si usa distinguere fra safety, intendo con ciò tutte le misure atte a ridurre la dannosità del sistema nelle sue operazioni, e security, cioè tutte le misure atte ad impedire che attività volontarie arrechino danni di diversa natura al sistema. Nell'ambito di questi sistemi è stata storicamente prestata molta attenzione alla safety, e diverse metodologie anche particolarmente efficaci sono state predisposte per la progettazione di sistemi safe, mentre molto poco è stato speso in relazione alla security. Lo scenario di riferimento sta però lentamente mutando.

È difatti in continua crescita il numero di sistemi di automazione e controllo che per questioni legate a riduzione dei costi, interoperabilità, standardizzazione tendono ad usare le tecnologie dell'informazione e della comunicazione. Queste tecnologie pur garantendo i vantaggi sopra descritti espongono però gli apparati a tutti i ben noti problemi di security che caratterizzano queste tecnologie. Un virus che infetta questi sistemi potrebbe ad esempio, oltre ai danni che siamo soliti considerare, provocare gravi danni materiali a persone e cose.

Si pone quindi la necessità di individuare metodologie e strumenti che affiancandosi a quelli già da tempo consolidate nel settore della Safety, consentano l'individuazione dei suddetti problemi e la realizzazione di sistemi safety critical che continuino a mantenere le loro proprietà originali nonostante il ricorso alle tecnologie dell'informazione e della comunicazione. Questo significa individuare e rivedere le metodologie oramai consolidate nel settore della progettazione dei sistemi safety critical, alla luce dei nuovi requisiti imposti dal nuovo trend.

Anticipo che il problema è tutt'altro che semplice ed in particolare la sensazione di chi opera nel settore è che la strada da percorrere per giungere ad una soluzione accettabile del problema sia ancora molto lunga. Un esempio che spero consenta al lettore di cogliere la dimensione del problema.

Notevoli sforzi sono stati prodotti in ambito scientifico per cercare di adeguare metodologie tipiche del mondo safety ad operare in ambito security, con particolare attenzione alle metodologie di valutazione del rischio. Ben presto ci si è però scontrati con la diversa concezione che le due discipline hanno di minaccia, e di come la stessa si rifletta su aspetti fondamentali dell'intera disciplina. In ambito safety un sistema è concepito come un sistema chiuso (senza interazioni con l'esterno) le minacce sono di fatto eventi interni al sistema, involontari e che possono modificare il normale funzionamento di un sistema. Stiamo parlando ad esempio di guasti hardware o comportamenti accidentali di hardware, software o di un operatore umano. Nell'ambito della sicurezza i sistemi sono per definizione aperti e le minacce sono invece anche guasti intenzionali quali vandalismi e sabotaggi. Questa diversa concezione di minaccia si riflette nelle tecniche adottate per la stima del rischio nelle due discipline. In un sistema safety critical questa stima si ottiene spesso rifacendosi al cosiddetto "random failure model", che fornisce tra l'altro stime di rischio quantitative molto significative. In ambito security, l'intenzionalità della minaccia, fa sì che questo modello non assuma alcun significato, poiché non riflette assolutamente il comportamento di una minaccia esplicitamente rivolta a sovvertire il comportamento di un sistema. Avrebbe più senso poter stimare la probabilità che un programma contenga una o più vulnerabilità, un problema che è

però risaputo essere indecibile. Quindi, di un sistema safety critical sappiamo calcolare con una certa precisione il suo livello di safety, ma non riusciamo a dire molto di significativo sul suo livello di security. Poiché il secondo può però inficiare il primo, ci troviamo di fatto in una situazione in cui non siamo oggi in grado di stimare con sufficiente precisione il livello di safety di un sistema d'automazione.

Cosa ancora più grave, non siamo nemmeno in grado di prevedere quando questa situazione di empasse potrà essere superata. Per contro, i sistemi d'automazione e controllo sono una realtà, è una realtà il loro sempre maggiore ricorso a tecnologie non propriamente sicure, ed è altrettanto una realtà l'impiego di questi sistemi per governare gli apparati di infrastrutture critiche.

Cosa possiamo fare allora già da oggi o che cosa si sta facendo, per cercare di porre un rimedio ai problemi sopra delineati?

La risposta ci viene fornita dal nostro socio Enzo Tieghi che da diversi anni opera nel settore dei sistemi di automazione, e che ci racconta in questo contributo le strategie attualmente individuate per cercare di ridurre l'impatto di tecnologie insicure sui sistemi di automazione, che devono garantire un certo livello di affidabilità. Cosa da sottolineare, le diverse strategie illustrate prendono tutte spunto da best practice diffuse dai diversi organi internazionali che operano nel settore dei sistemi di automazione, e disegnano quindi lo stato dell'arte in materia a livello internazionale. Il testo è ben articolato, supportato da estratti di standard internazionali nonché da casi di studio riportati nella ricca appendice. Non va inoltre sottovalutata la doppia valenza del contributo. È sicuramente un buon inizio per chi si è sinora occupato di Sicurezza IT e vuole allargare i propri orizzonti con nuove sfide e nuovi problemi, e per contro non può non catturare l'attenzione di chi si è sinora interessato principalmente di sistemi di automazione e si è posto solo marginalmente il problema della loro sicurezza informatica.

Un ultimo accenno per gli esperti di sicurezza informatica. Per loro la lettura di questo manoscritto costituirà un salto nel passato, poiché di fatto le strade che stanno oggi percorrendo "i sicuristi" dei sistemi d'automazione, sono quelle già tracciate nel corso di questi anni in ambito sicurezza informatica. Particolare attenzione assumono in questo contesto le diverse architetture di protezione perimetrale basate firewall, oggi arricchite di ulteriori componenti quali antivirus, IDS e IPS. Quindi in attesa che la ricerca individui e proponga strumenti più efficaci, si è ricorsi ancora una volta ad applicare l'intramontabile principio della "separation of duties", il "prezzemolo" di ogni sana politica di sicurezza.

Prof. Danilo Bruschi

*Presidente del
Comitato Tecnico-Scientifico Clusit*

Abstract

Preparando questo quaderno, ho pensato ad un lettore, professionista dell'automazione, che si avvicina all'argomento "messa in sicurezza" dei suoi sistemi e reti di impianto: deve identificare minacce e vulnerabilità, adottare le contromisure più indicate per la protezione dei sistemi di automazione e controllo.

Dopo un'introduzione al tema (con riferimento a standard dell'industria), vengono affrontate le strategie più utilizzate/consigliate per la protezione dei sistemi di controllo utilizzati in fabbrica: il riferimento dichiarato è quello del documento NISCC/BCIT su tale argomento, con l'aggiunta di commenti e suggerimenti dati dall'esperienza.

Nelle appendici sono raccolti alcune tecnologie e strumenti, oltre ad alcuni articoli e memorie sull'argomento security industriale.

Keywords: industrial cyber security, firewall, switch, router, SCADA, DCS, PLC, VPN, OPC, DMZ, ISA, ISAs99, BS7799, ISO27000,

L'autore

Enzo Maria Tieghi - etieghi@visionautomation.it

Enzo Maria Tieghi è Amministratore Delegato della società ServiTecno (www.servitecno.it, azienda che dal 1985 distribuisce e supporta software e sistemi per applicazioni industriali per controllo di processo ed automazione di fabbrica) e di Vision Automation (www.visionautomation.it, azienda che distribuisce strumenti per nella protezione dei sistemi di controllo e per eManufacturing). Attivo in Associazioni di settore (quali Clusit, ISA, Assintel, ISPE, ANIPLA, etc.), tiene corsi e partecipa come relatore ad eventi specialistici oltre a contribuire con articoli e memorie su riviste specializzate.

INDICE

SEZIONE I Premessa	15
Introduzione: la sicurezza di sistemi e delle informazioni negli impianti di produzione	17
Reti e sistemi di controllo di processi e automazione di fabbrica.....	17
Vulnerabilità comuni in reti di automazione e sistemi di controllo processo	20
Riferimenti a Norme e Standard (ISO27000 e ISA S99).....	21
Le norme ISO/IEC 17799, BS7799 e la serie ISO27000.....	21
Cos'è la sicurezza delle informazioni?.....	22
Valutare e Gestire i Rischi	22
La sicurezza delle informazioni non è un prodotto: è un processo.....	22
Le norme ISO27000 ed i sistemi di controllo	23
Lo standard Industriale ISA S99: Manufacturing and Control System Security.....	24
Considerazioni sulla sicurezza dei Sistemi di controllo ed automazione industriale.....	24
Le “Doti dell’informazione”: Disponibilità, Integrità e Riservatezza.....	25
Dove la Sicurezza IT potrebbe differire da quella “industriale”?	26
SEZIONE II La protezione di reti e sistemi di controllo mediante dispositivi e presidi, la segmentazione e la segregazione	29
2 – Introduzione	31
3 - Cos'è un Firewall?	32
4 - Cos'è un Router	34
5 – Cos'è uno Switch	36
6 - Cos'è una DMZ (Demilitarized zone)	36
7 - Perché usare Firewall (ed altri presidi) per proteggere reti di controllo e sistemi SCADA/DCS	37
8 - Utilizzo di Firewall a due porte tra rete di controllo PCN (Process Control Network) e rete aziendale EN (Enterprise Network)	37
9 - Separazione delle reti PCN ed EN mediante una combinazione di Router e Firewall	39

10 - Firewall con Zona De-Militarizzata (DMZ) tra la rete di controllo PCN e la rete aziendale EN.....	40
11 - Coppia di Firewall in batteria tra la rete di controllo PCN e la rete aziendale EN.....	41
12 - Combinazione con Firewall e reti di controllo PCN basate su V-LAN.....	42
13 – Confronto tra le configurazioni.....	43
14 - Firewall: come installarlo e configurarlo correttamente per proteggere la rete di PCN e SCADA	44
15 – Considerazioni specifiche per Firewall.....	46
16 – Policy adeguate per la gestione dei firewall sulla PCN e reti SCADA.....	47
Appendice A – Protezione di rete di controllo PCN mediante Firewall con funzionalità estese e gestione integrata UTM.....	49
(Unified Threat Management).....	49
Appendice B – Gestione delle anomalie e monitoraggio di reti e sistemi di controllo	51
Un sistema di monitoraggio per reti e sistemi di fabbrica.....	51
Appendice C - Security, configuration management e change control per le applicazioni industriali e software di fabbrica.....	53
Benefici di un sistema di Change Management in Fabbrica.....	53
Gestione di Folder e File.....	53
Sistemi di Fabbrica (Factory Floor)	54
Electronic Records e Audit Trail.....	54
Utilizzo di Electronic Signatures.....	54
Sicurezza Utente.....	54
Sicurezza del PC Client.....	54
Change Control	55
Appendice D - Utilizzo di comunicazioni con standard OPC (con DCOM) attraverso Firewall.....	57
About DCOM and Security.....	57
About DCOM Robustness.....	57
Set-up complexity	57

Solution Description – An Example.....	58
Appendice E – Strumenti Biometrici (Strong Authentication) per identificare ed autorizzare operatori su impianti industriali	61
Premessa.....	61
Strumenti biometrici per il riconoscimento.....	61
Uso del dispositivo biometrico.....	62
Enrollment.....	62
Autenticazione.....	63
Biometria in ambienti regolamentati.....	63
Appendice F – Domande e risposte su cyber security industriale	65
Perché si parla di security anche per i sistemi di controllo ed automazione?	65
È vero che la criminalità informatica inizia a prendere di mira anche i sistemi di controllo e automazione?.....	66
Che differenze ci sono tra la security dei sistemi IT e la security per i sistemi di fabbrica (controllo e automazione)?.....	66
Quali norme o standard internazionali si occupano di cyber security industriale?	67
Perché l’analisi e valutazione del rischio?	68
Chi deve fare l’analisi del rischio?	68
Quando fare l’analisi del rischio?.....	69
Come fare l’analisi del rischio?.....	69
Perché occorre identificare/autenticare gli operatori dei sistemi di fabbrica?	69
Autenticazione Forte e Biometria: come?.....	70
Alta Disponibilità: cos'è?	70
Alta disponibilità o alta affidabilità?	71
Quanto spendere per la disponibilità?	71
Appendice G – 21 Passi per migliorare la sicurezza di reti e sistemi di controllo.....	73
Premessa.....	73
Introduzione	73

21 Passi per migliorare la sicurezza dei sistemi SCADA	74
Parte 1: i passi seguenti sono focalizzati su specifiche azioni da fare per aumentare la sicurezza della rete SCADA.....	74
Parte 2: I passi seguenti sono focalizzati su azioni che la Direzione deve intraprendere per mettere in piedi un efficace programma di sicurezza informatica	75
Appendice H – La lezione dell’uragano Katrina riguardo ai sistemi di controllo: cosa un disastro naturale può insegnare all’industria.....	77
Abstract	77
Introduzione	77
Problemi di sicurezza nel fare ripartire i sistemi di controllo	78
Facciamo ripartire i sistemi in sicurezza (“Safety” & “Security”).....	79
Determinare e mettere in atto una “Sicurezza Fisica”.....	79
Determinare e mettere in atto la “Sicurezza dell’organizzazione”	79
Determinare un sistema o procedura per il controllo delle configurazioni	80
Verifica dell’Hardware.....	80
Verifica del Software	81
Supporto per connessioni remote sicure.....	81
Connessioni sicure con altre reti	82
Ripartenza dei processi controllati in “Safety” e in “Security”	83
La lezione imparata	83
Note finali.....	84
Appendice I – Le Gamp (Good Automated Manufacturing Practices) e la Sicurezza dei sistemi, delle informazioni e delle reti nelle applicazioni industriali e di produzione nel settore Life-Science	85
Premessa.....	85
1 - Introduzione	85
2 - Ambito	85
3 - Responsabilità.....	85
4 – Principi	86

Classificazione dei sistemi	86
Consapevolezza degli utenti.....	86
Gestione degli incidenti.....	86
Politiche per la sicurezza delle informazioni.	86
5 - Requisiti dei sistemi e responsabilità.....	86
Appendice L – Sicurezza dei sistemi acquedottistici nei confronti di possibili atti terroristici: impatto sui sistemi di controllo e telecontrollo	89
Il rapporto ISTISAN.....	89
La minaccia Terrorismo	89
Le minacce per i sistemi di telecontrollo	90
2.3.1. Dispositivi e tecnologie di controllo della sicurezza.....	90
2.3.4. Controllo delle informazioni	91
2.5. Piani di emergenza	91
3. Tipologie impiantistiche e loro protezione.....	92
3.1.2. Impianti di potabilizzazione	92
3.2. Dispositivi di monitoraggio in continuo.....	92
5. DIFFUSIONE DI INFORMAZIONI SENSIBILI SUI SISTEMI ACQUEDOTTISTICI ..	92
Acronimi/Glossario	93
Riferimenti/Bibliografia.....	95
Altri riferimenti e Standard per la security industriale	96
Riferimenti e link internet:.....	97
Ringraziamenti	99

CLUSIT

Associazione Italiana per la Sicurezza Informatica

Sede legale presso:

Dipartimento di Informatica e Comunicazione

Università degli Studi di Milano

Via Comelico 39 - 20135 MILANO

www.clusit.it – info@clusit.it

tel. 347 23 19 285