Intellium
Deloitte.

A governance model for ICS and SCADA security

Proposal of a model for evaluating and evolving ICS Cyber Security in Gas Critical Infrastructures

Toto Zammataro, 16th November 2016

Prepared For:

gie
Gas Infrastructure Europe

Agenda

ICS Security Requirements & Governance Model Definition **3 pages**

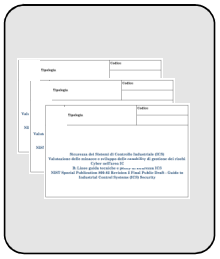
Maturity Evaluation & Roadmap definition **4 pages**

ICS Security Requirements and Governance Model Definition

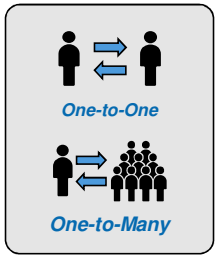
Project activities have delivered to the Client their new ICS Security Requirements and Governance Model

Information Gathering

Documents

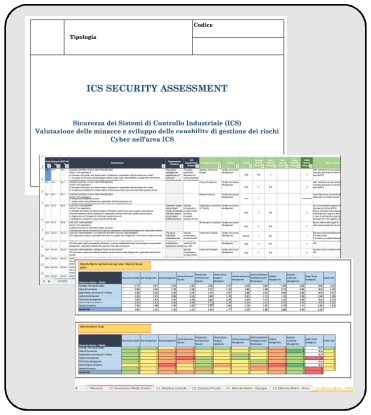


Interviews



Assessment Tool

Assessment Tool Definition

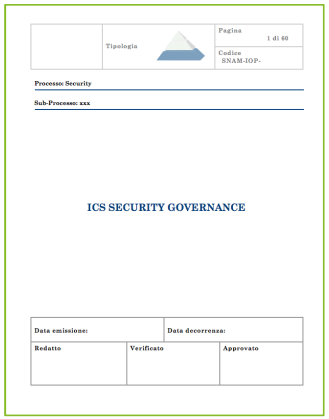


Deliverable

Critical ICS Security Requirements

Deliverable

ICS Security Governance Model



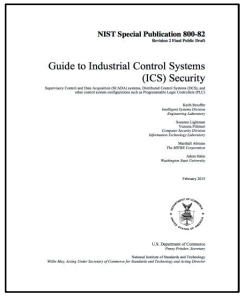
Critical ICS Security Requirements

Critical ICS Security Requirements will help Client to secure future evolutions of their Industrial Control System…

ICS Key Assets

TECHNOLOGY	Critical ICS data-transmission network
	Server and device connected to critical ICS
HUMAN RESOURCES	
FACILITIES	

International Standard
NIST 800-82 r2

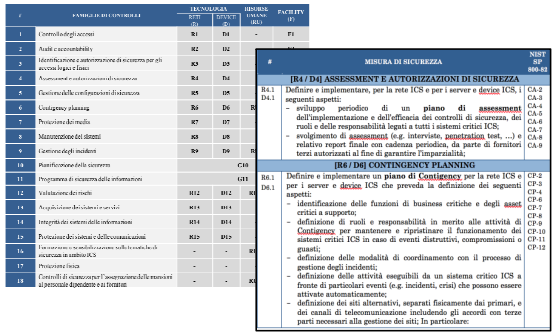

NIST Special Publication 800-82
Revision 2 Final Public Draft

Guide to Industrial Control Systems (ICS) Security

Identification of Security Requirements

Set of detailed requirements derived from NIST Controls (~ 800) and divided in two groups:

- **Governance Requirements:**
  - Applicable to each asset
  - NIST Families: Planning, Program Management
- **Technical and Operative Requirements**:
  - Applicability Matrix: Asset (4) vs NIST Families (16)



#	FAMIGLIE DI CONTROLLI	TECNOLOGIA RETE (T1)	TECNOLOGIA SERVER (T2)	RISORSE UMANE (RU)	FACILITY (F)
1	Controllo degli accessi	R1	D1	-	F1
2	Audit e accountability	R2	D2		
3	Identificazione e autenticazione di sicurezza per gli accessi logici e fisici	R3	D3		
4	Assessment e autorizzazioni di sicurezza	R4	D4		
5	Gestione delle configurazioni di sicurezza	R5	D5		
6	Contingency planning	R6	D6	R	
7	Protezione dei media	R7	D7		
8	Manutenzione dei sistemi	R8	D8		
9	Gestione degli incidenti	R9	D9	R	
10	Pianificazione della sicurezza			C10	
11	Programma di sicurezza delle informazioni			GI1	
12	Valutazione dei rischi	R12	R12	R	
13	Acquisizione dei sistemi e servizi	R13	R13		
14	Integrità dei sistemi delle informazioni	R14	R14		
15	Protezione dei sistemi e delle comunicazioni	R15	R15		
16	Formazione e sensibilizzazione sulla sicurezza in ambito ICS	-	-	R	
17	Protezione fisica	-	-		
18	Controlli di sicurezza per l'assegnazione delle mansioni al personale dipendente e ai fornitori	-	-	R	

#	MISURA DI SICUREZZA	NIST SP 800-82
	[R4 / D4] ASSESSMENT E AUTORIZZAZIONI DI SICUREZZA	
R4.1 D4.1	Definire e implementare, per la rete ICS e per i server e device ICS, i seguenti aspetti: – sviluppo periodico di un **piano di assessment** dell'implementazione e dell'efficacia dei controlli di sicurezza, dei ruoli e delle responsabilità legati a tutti i sistemi critici ICS; – svolgimento di assessment (e.g. interviste, penetration test, …) e relativo report finale con cadenza periodica, da parte di fornitori terzi autorizzati al fine di garantire l'imparzialità;	CA-2 CA-3 CA-4 CA-5 CA-6 CA-7 CA-8 CA-9
	[R6 / D6] CONTINGENCY PLANNING	
R6.1 D6.1	Definire e implementare un **piano di Contigency** per la rete ICS e per i server e device ICS che preveda la definizione dei seguenti aspetti: – identificazione delle funzioni di business critiche e degli asset critici a supporto; – definizione di ruoli e responsabilità in merito alle attività di Contigency per mantenere e ripristinare il funzionamento dei sistemi critici ICS in caso di eventi distruttivi, compromissioni o guasti; – definizione delle modalità di coordinamento con il processo di gestione degli incidenti; – definizione delle attività eseguibili da un sistema critico ICS a fronte di particolari eventi (e.g. incidenti, crisi) che possono essere attivate automaticamente; – definizione dei siti alternativi, separati fisicamente dai primari, e dei canali di telecomunicazione includendo gli accordi con terze parti necessari alla gestione dei siti; In particolare:	CP-2 CP-3 CP-4 CP-6 CP-7 CP-8 CP-9 CP-10 CP-11 CP-12

Key Outcomes

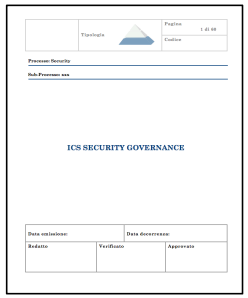
- The set of security requirements is applicable to Group Industrial Control Systems and is based on International Standards
- This approach could inspire the definition of requirements and countermeasures in any ICS environment

ICS Security Governance Model

… while ICS Security Governance Model enables the evaluation of the effectiveness of security measures put in place

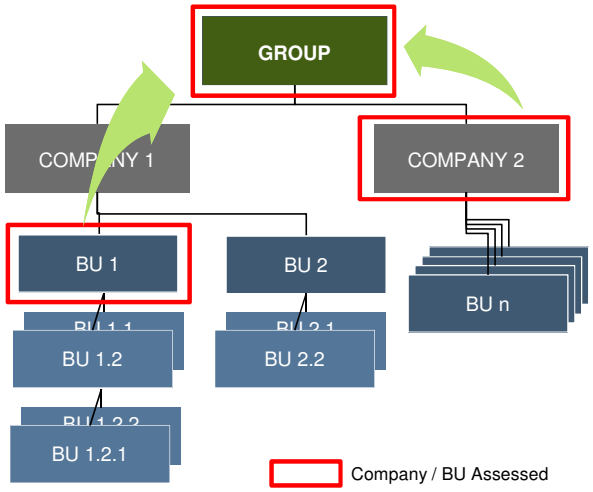
Key Components

- **Security Framework:**
  - Management Processes (7)
  - Security Domains (11)
- **Input Parameters**
  - Weights associated to prioritization levels and Stakeholders
- **Evaluation Process**
  - Control based Assessment



Applicability

- **Overall Organization ICS Security Maturity Level is derived** from maturity levels of Companies / Business Units belonging to the group
- The model is **scalable** to new Client Group Company or BU

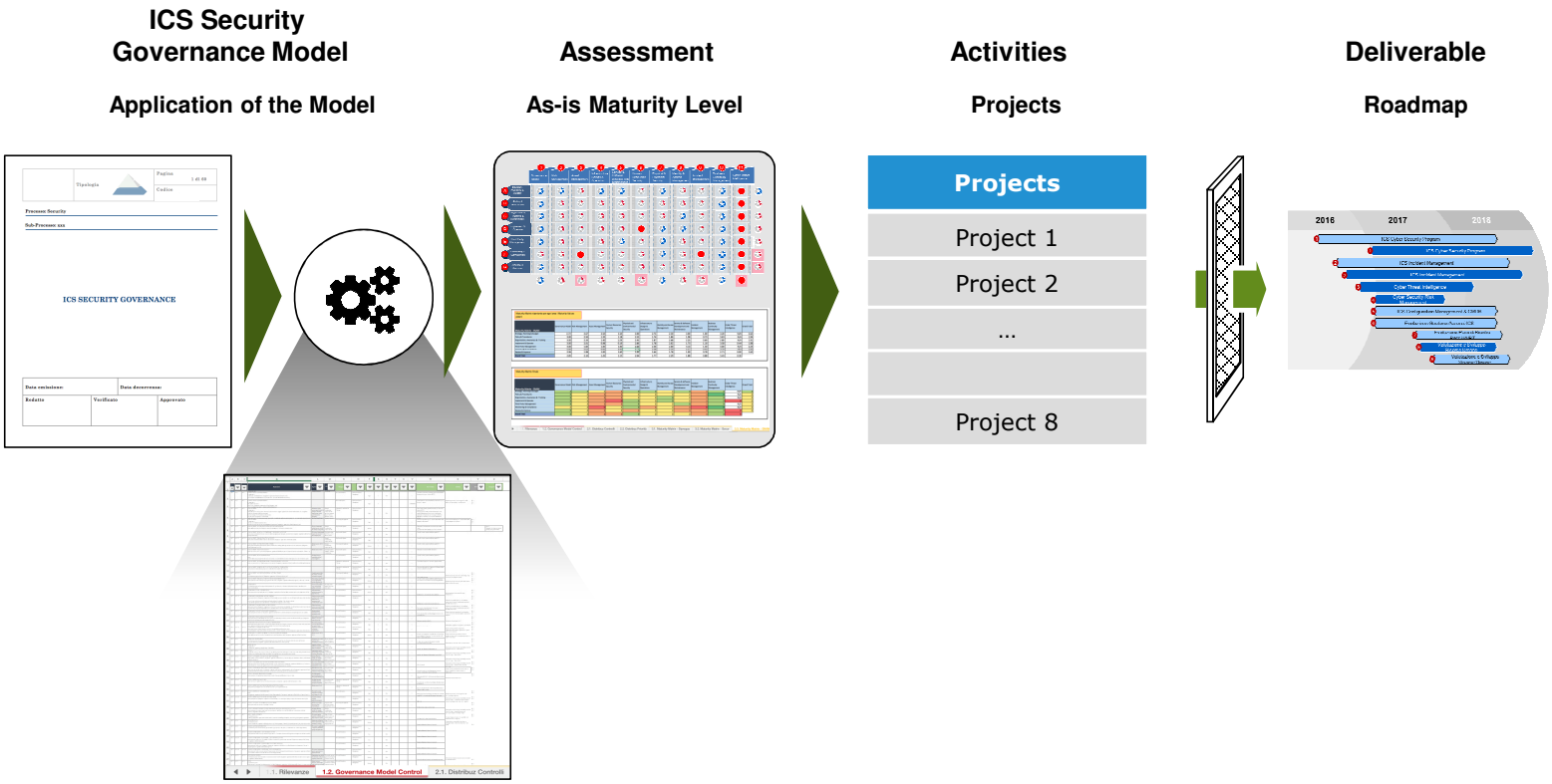


Key Outcomes

- ICS Security Governance model is built to support complex organizations in which many actors contribute to the ICS Security Management
- This model is independent from the particular input parameters chosen

Maturity Evaluation & Roadmap Definition

ICS Security Governance Model has been applied during the project to evaluate current maturity level

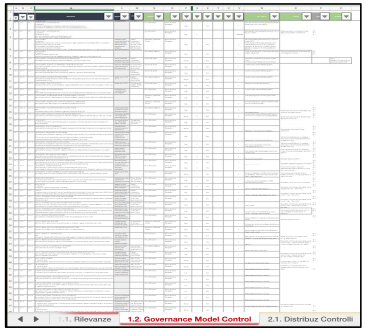


Assessment Tool

We evolved Intellium tool in order to allow the assessment of the ICS Security maturity of every client stakeholder…

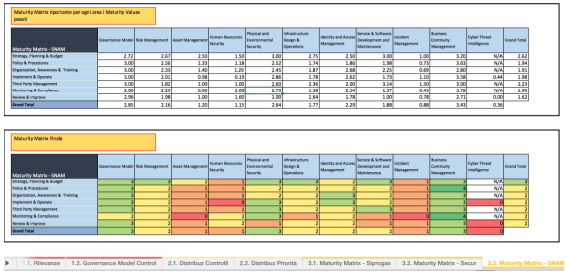
Tool Structure

- ~ **800 Controls**, each associated to a single Mgmt Process and Domain
- **3 Weighted Priority Levels** (High, Medium, Low) derived from NIST evaluation
- **6 "Maturity Levels"** for each control



Evaluation & Results

- Maturity of every control is evaluated through 6 maturity values
- Every control have to be evaluated for every company / Business Unit or set as Not Applicable
- Tool computes a weighted average to provide the maturity level for each area of the framework (single process x single domain)
- Results (valorized framework) are shown in real-time



Key Outcomes

- Excel Tool provides real-time maturity of every company / Business Unit allowing separate evaluations
- The tool is scalable with little effort to new Company or Business Unit to adapt to acquisitions, organizational changes, new strategy

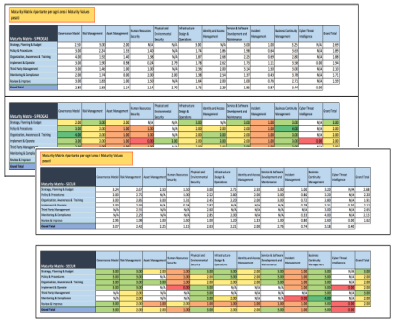
EXAMPLE

As-is Maturity Level

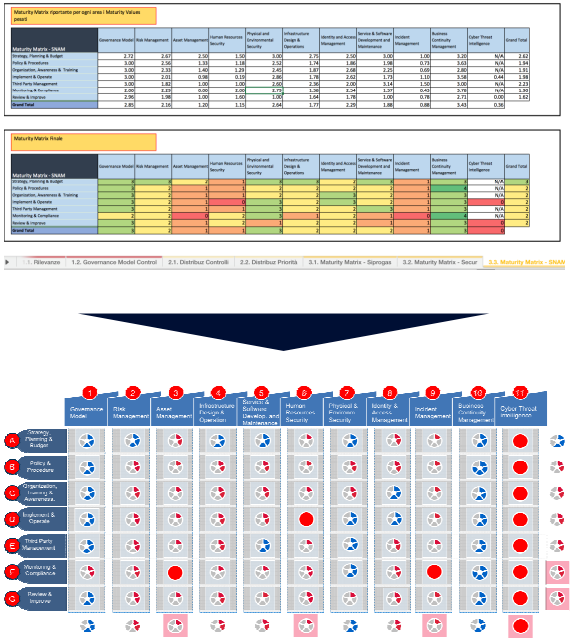
… deriving consequently from these maturities the overall maturity level of the whole Group

Tool Structure

- **Weight (0-1) associated to each company / BU** based on strategy relevance and operating margin
- Overall maturity level calculated as weighted average of maturity levels of each company / BU



Overall Results



Key Outcomes

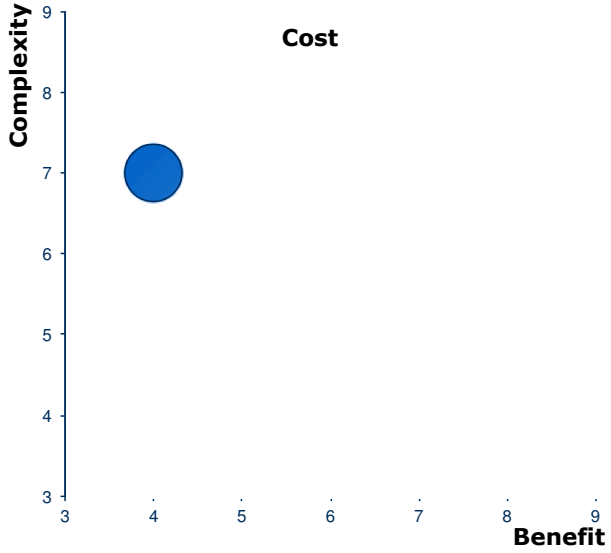
- The tool also provides real-time maturity level of the overall group
- Effective graphical representation:
  - Red: As-is maturity less than target maturity
  - Blue: As-is maturity grater than or equal to target maturity

Strategic Roadmap

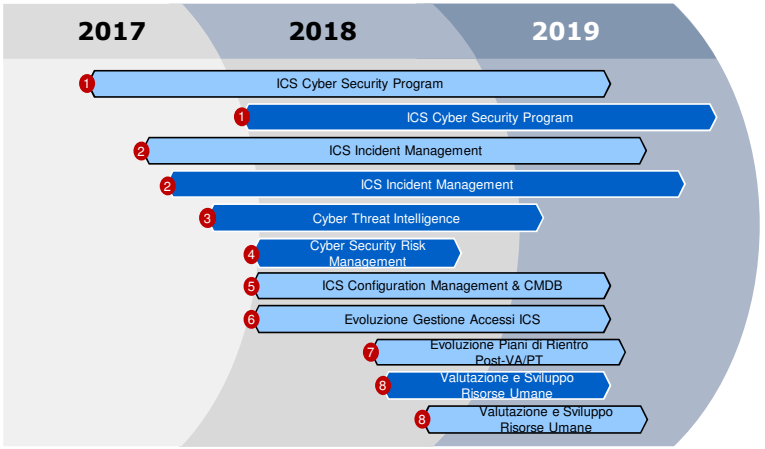
Starting from assessment results we can define a roadmap made of X projects aiming to address areas of improvement

Prioritization

- **Cost** (CAPEX, OPEX, FTE)
- **Complexity** (implementation, organizational,…)
- **Benefit** (maturity level increase, risks mitigation,…)



Three-year Roadmap



Any Question?

Intellium
Deloitte.

- **Toto Zammataro**
- **+39-348-0097164**
- **Email: tzammataro@deloitte.it**
- **LinkedIn : www.linkedin.com/in/totoz[1)]**

1) I'm accepting on linkedin only people I'm aware I met in real world

gie
Gas Infrastructure Europe