Devising a robust cyber-security strategy to guard against emerging attacks on IEC 61850 enabled infrastructures

Prepared by: Adam Gauci, Cybersecurity Program Manager, Schneider Electric

Trends

Cyber attacks on industrial control systems are growing exponentially

Stuxnet
Iran nuclear plant

45,000 machines infected **PLC** modified and destroyed

Duqu
Iran, Sudan

Espionage malware targeted at Energy sector

Shamoon
Saudi Aramco attack

30,000 Windows-based machines infected

Unknown malware
German steel mill

Uncontrolled **shutdown of a blast furnace** due to control component breakdowns

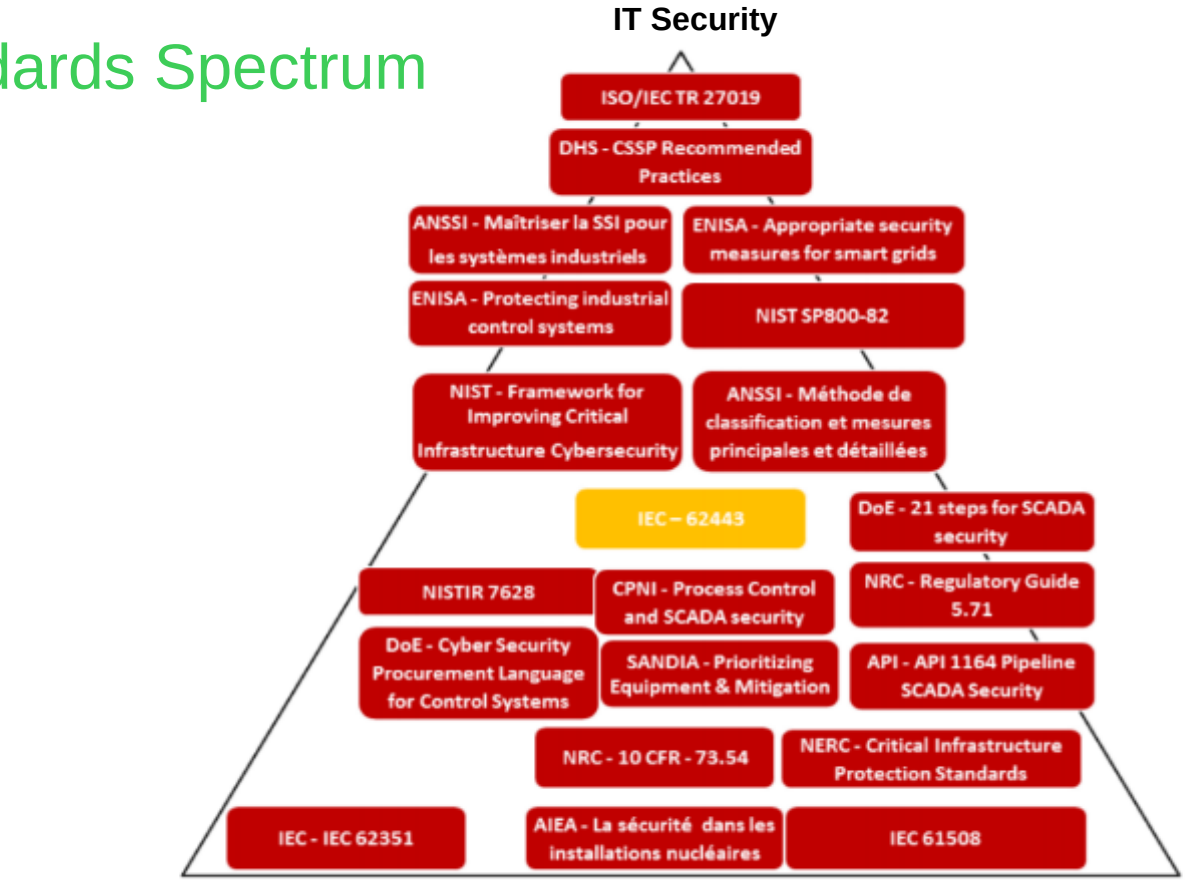
Sandworm, BlackEnergy
Ukraine

200,000 people left without electricity due to **grid blackout**

2010 2012 2014 2015 2016 2017: Who's next ?

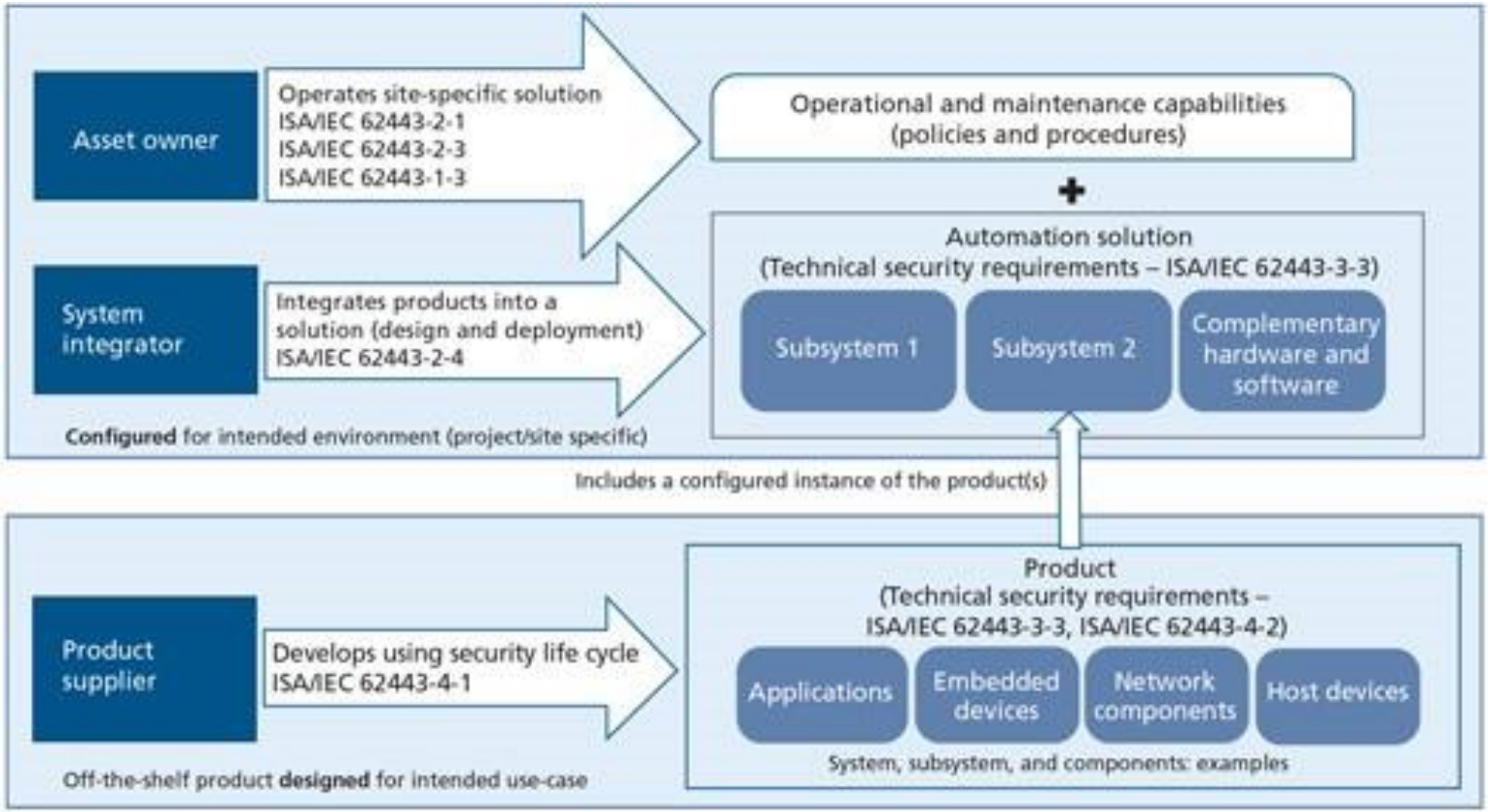
There are many other **Malware specifically targeting PLCs, SCADA and Control Systems,** like Havex, IronGate, Gauss, Duqu, Shamoon, Flame, etc.

Standards Spectrum

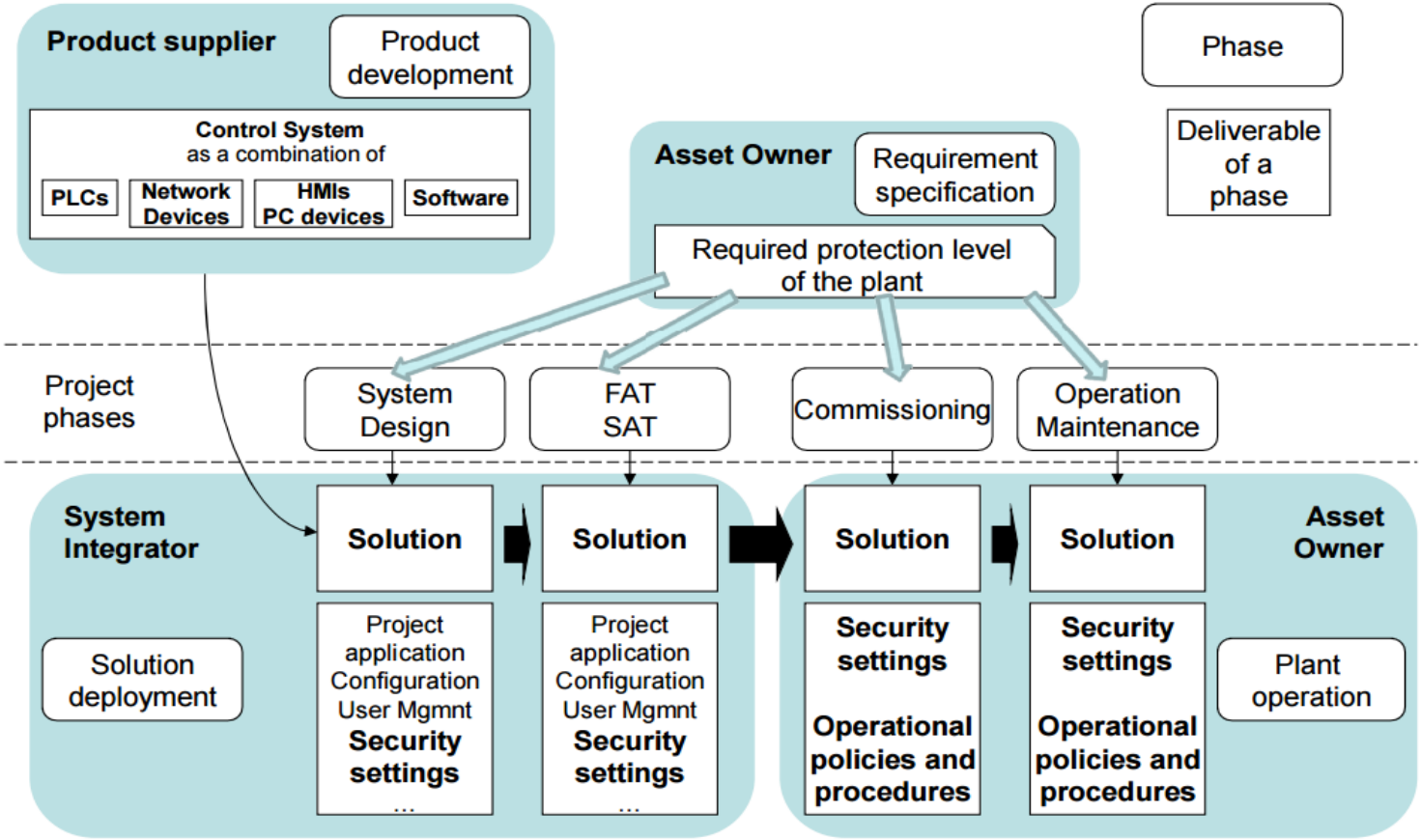


Source: CLUSIF

IEC 62443



All stakeholder are involved in the protection of the plant during plant life cycle



IEC 62443 Security Levels

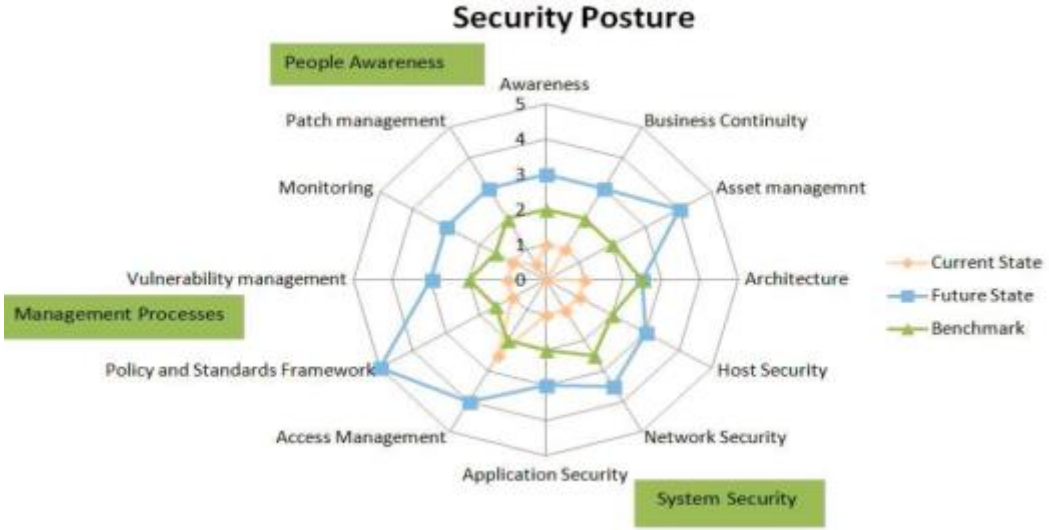
Security Level	Description
SL-4	Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation
SL-3	Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
SL-2	Protection against intentional violation using simple means with low resources, generic skills and low motivation
SL-1	Protection against casual or coincidental violation

Example Risk Matrix

Impact		Likelihood				
		Remote	Unlikely	Possible	Likely	Certain
	Trivial	SL-0	SL-1	SL-1	SL-1	SL-1
	Minor	SL-1	SL-1	SL-2	SL-2	SL-2
	Moderate	SL-1	SL-2	SL-2	SL-3	SL-3
	Major	SL-1	SL-2	SL-3	SL-4	SL-4
	Critical	SL-1	SL-2	SL-3	SL-4	SL-4

Know where to start

- Risk assessments based on ISO 27005 and IEC 62443 methodologies.
- Deliverable: Detailed report highlighting the various risks of the system, its components and processes.



TASK	PRIOR State	POST State
Vulnerability level		
Insecure open ports	TCP 139 NETBIOS TCP 3389 RDP TCP 21 FTP UDP 5004 RTP UDP 445 MS SMB File Sharing	Disabled Managed via FW Policy Closed via FW Policy Required for Application Required for AV Updates
Insecure running services	Internet Information Service FTP Server Service Terminal Services	Uninstalled Closed via FW Policy Uninstalled
AV client	McAfee 8.7	Unchanged
AV DEFs	April 2 2011	Current Date
AV auto update	None	Added to auto ePO update
AV scheduled scan	None	Yes / Monthly / Day 1 / 1AM
AV Scans run recently	None	Yes – Clean
AV buffer overflow protection	Enabled	Unchanged
Security and system logging	Yes / Local / 512KB / 7 days	Yes / Local / 1024KB / 90 days
Complex Admin password	None	Added complex password, shared with site team
Decoy Admin account	None	Decoy admin account created
Default accounts	In use	Disabled
Games	Not installed	Unchanged
Internet Information Services	Installed	Required
Language compilers	Not installed	Unchanged
Unused network components	Not installed	Unchanged

Implement a Cyber Defense

01 Identify critical cyber assets

Minimize access to your most sensitive information 02

03 Control user access

Implement patch management policies 04

05 Prevent malicious software attacks

Develop a disaster recovery and response plan 06

07 Monitor cyber systems for attacks

Life Is On | Schneider Electric