COMET CYB

ICS CYBERSECURITY MAINTENANCE

28/09/2018 | Public

SPEAKER: ALEXIS D’USSEL

Senior Manager

Security Architect

Information Security Auditor

In charge of 360° Audit LAB

adussel111@beijaflore.com
+33 (0)6 61 97 90 57

AGENDA

01 STAKES, OBSERVATIONS AND ISSUES

02 FEEDBACKS ON STATE OF ART

03 FUTURES PERSPECTIVES

01 - STAKES, OBSERVATIONS AND ISSUES

EVOLUTION OF ICS RAISES NEW CYBER SECURITY ISSUES

Operational needs have evolved, and continue to evolve

- ICS convergence with ERP leads to interconnections with IT
- Costs are continuously optimized:
  - Remote maintenance is becoming a common practice
  - Technologies are standardized, gradually abandoning proprietary systems and protocols

Connected factories are unprepared for cyber threats

- They find themselves exposed to generic malware
- They are also vulnerable to sophisticated attacks that can have dramatic consequences

Cyber security maturity is still weak

- The OT area of responsibility is often poorly established
- OT cyber security state of the art similar to that of IT 20 years ago
- Automation engineers have little awareness of the cyber risks of connected factories

THE INDUSTRY FACES SEVERAL RISKS FROM CYBER THREATS

Safety incidents

Human impacts due to:

- Exposure to toxic substances
- Collisions with equipment (eg AGV, crane)
- Incidents related to explosive atmospheres (ATEX) and flammable liquids

Quality defects

Deviation from good manufacturing practices:

- Manufacturing error (eg wrong dosage, dimension error)
- Bad labeling, packaging or storage (confusion between products)

Production stoppages

Major dysfunctions:

- Systems in the process bottleneck (eg wrapper, cooling, cutting)
- Industrial application servers
- Utilities (eg electricity, water, HVAC, Compressed air)

Potential consequences

Injuries & deaths

Penal prosecution / Large fines

Corporate image degradation

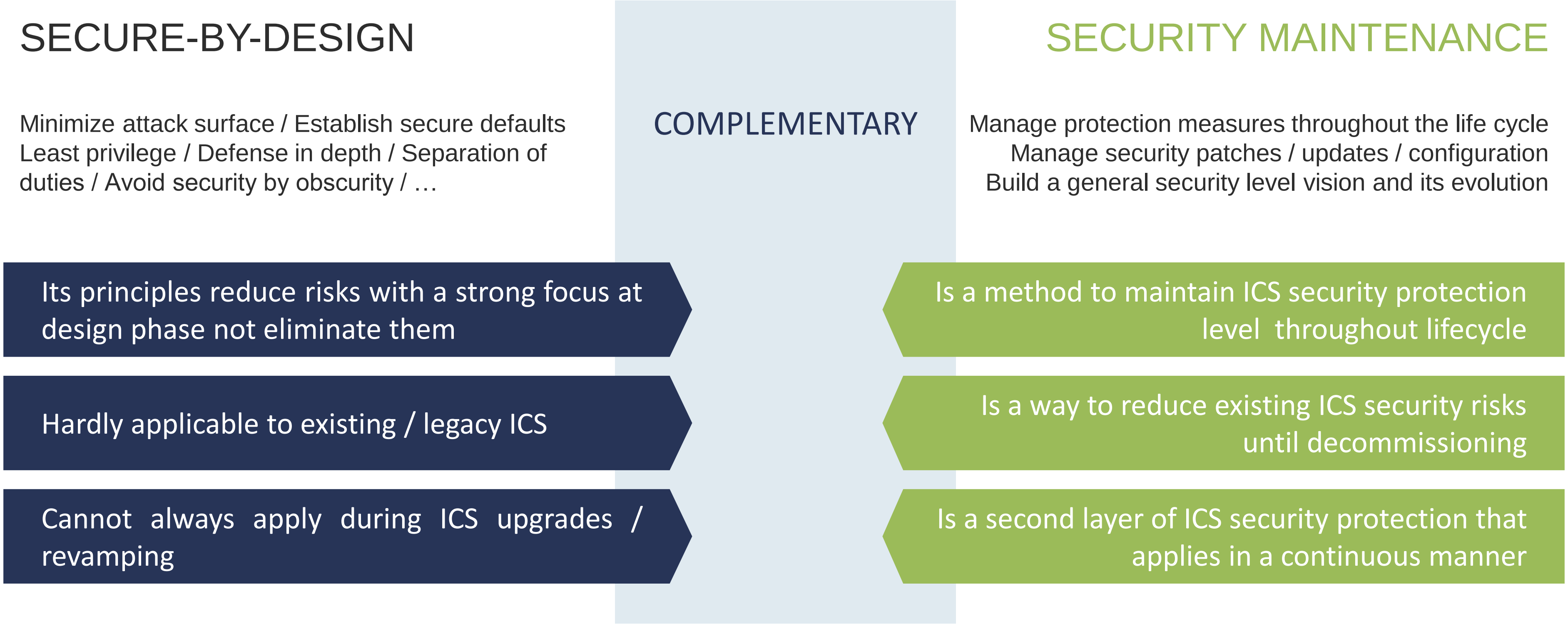
Environmental impacts

Loss of accreditation

Loss of revenue

Data theft

« SECURITY MAINTENANCE » ESSENTIAL ELEMENT OF A CONTROLLED AND SUSTAINABLE CYBER RISK MANAGEMENT



SECURE-BY-DESIGN

Minimize attack surface / Establish secure defaults
Least privilege / Defense in depth / Separation of duties / Avoid security by obscurity / …

- Its principles reduce risks with a strong focus at design phase not eliminate them
- Hardly applicable to existing / legacy ICS
- Cannot always apply during ICS upgrades / revamping

COMPLEMENTARY

SECURITY MAINTENANCE

Manage protection measures throughout the life cycle
Manage security patches / updates / configuration
Build a general security level vision and its evolution

- Is a method to maintain ICS security protection level throughout lifecycle
- Is a way to reduce existing ICS security risks until decommissioning
- Is a second layer of ICS security protection that applies in a continuous manner

WHAT WILL OR WON'T HELP ICS SECURITY MAINTENANCE ?

OPPORTUNITIES

- ✓ Deeply rooted **culture of Dependability** including: Reliability, Maintainability, Availability and Safety.
- ✓ Cyber Security Regulation (eg LPM, NIS)
- ✓ Sector weight over ICS vendors
- ✓ High media coverage of Cyber Security news

- ❑ Strong operational constraints & extended life cycle
- ❑ ICS staff with fragile IT skills
- ❑ Lack of agility
- ❑ Large technological debt
- ❑ Constant flow opening on industrial IS
- ❑ Technology challenges (IoT, cloud, VR)

DIFFICULTIES

02 – FEEDBACKS ON ICS SECURITY MAINTENANCE STATE OF ART

PLANNING IS THE FIRST KEY !

STEP 01: RISK ANALYSIS

COVER YOUR RISKS NOT THE RISKS

Identify "risks", the decision making tool N°1
Define the Cyber Security maintenance strategy

STEP 02: GOVERNANCE

ELIMINATE THE “GREY AREA”

Take into account the multiplicity of stakeholders
Clarify roles and responsibilities (operator, supplier, maintainer)

STEP 03: CONTRACTS

KILL THE PAIN BEFORE IT'S BORN

Foresee security maintenance as of the contracting
Stick security maintenance requirement onto standard contracts

STEP 04: COORDINATION

MINIMIZE OVERLAYS

Fit in existing processes (eg maintain in operational condition)
Identify anchor points with Dependability
Notify all stakeholders

EXECUTE CLEVERLY TO CONTROL THE RISKS

STEP 05: WATCH

STEP AHEAD OF THE THREAT

Keep abreast of the state of the threat
Identify precisely the level of exposure of its infrastructures
Maintain contact with suppliers

STEP 06: PREPARATION

BE READY NOT STEADY

Fully integrate with change management processes
Take into account ALL operational constraints
Identify security upgrade opportunities

STEP 07: INDUSTRIALIZATION

USE SOFT POWER NOT MANPOWER

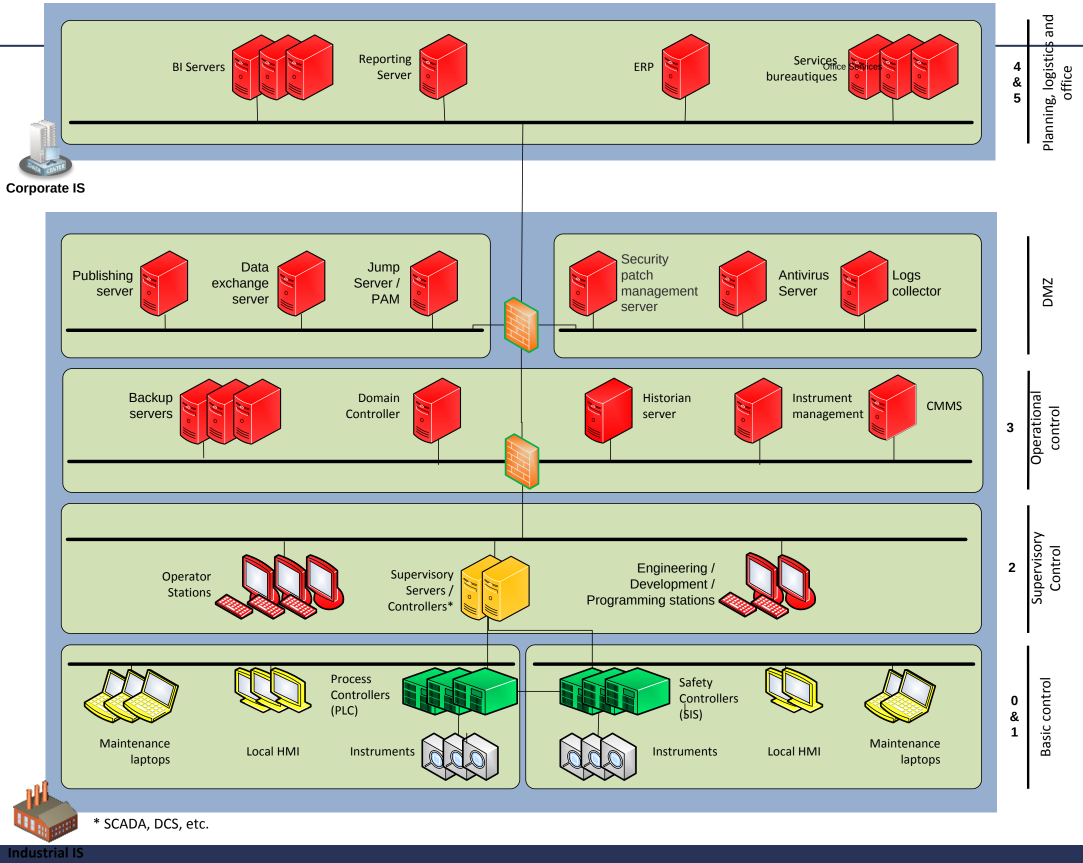
Propose security maintenance automation during the design whenever possible (“secure by design”)
Rely on standard tools

STEP 08: TEST & DEPLOYMENT

TEST, TEST, TEST BEFORE DEPLOY

Perform tests on environments aside production (eg OTS, virtualized environment, spare equipment)
Deploy in stage
Ensure availability of functional test leads

ICS PATCH MANAGEMENT: STRATEGY STRUCTURE



* SCADA, DCS, etc.

EXAMPLE

Acceptable exposure ranges

🟥 Priority 1 : A few hours to 30 days;

🟨 Priority 2: 30 to 90 days;

🟩 Priority 3: 90 days to one year.

SEGMENT YOUR CRITICALITY LEVELS (IE ACCEPTABLE EXPOSURE RANGES) ACCORDING TO THE PROCESS AND ITS RISKS

LONG-TERM MANAGEMENT TO OPTIMIZE EFFORTS

STEP 09: CHECK

LIMIT MALICIOUS ACTIONS & ERRORS

Ensure that documentation is up-to-date and reflects field’s reality

Regularly audit the security maintenance processes

STEP 10: MONITOR

VALUE EFFICIENCY NOT TECHNOLOGY

Define relevant steering indicators in your context

Monitor indicators regularly

STEP 11: EXEMPTIONS

EXEMPTION BETTER THAN OMISSION

Implement a risk-based exemption process

Register exemptions and limit them in time

Ensure exemptions go along with an action plan

STEP 12: IMPROVEMENT

BUILD YOUR NEXT MATURITY LEVEL

Join a continuous improvement process

Prepare the end of life of equipment

Maintain a global vision of security issues and protection level

03 - FUTURES PERSPECTIVES

TIME AND MONEY WILL REMAIN CRUCIAL FOR A WHILE …

ICS maturity increases:

- Automation engineers skills
- IT engineers skills
- ICS vendors maturity and reactivity

ICS Security solutions emerge:

- All-in-One appliances are emerging with encouraging results
- Low footprints on processes
- OT/IT Security solutions convergence

ICS Security threats will multiply:

- Viruses are becoming more sophisticated & numerous, requiring continuous protection effort
- Attacks are also targeting ICS vendors (eg download servers) obliging to check patch integrity & authenticity

Security Maintenance is often neglected:

- Other problematics are prioritized like functional security
- Fast degradation of state of the art infrastructures
- Security first ! Do not forget cyber security

THANK YOU

FOR YOUR ATTENTION

Maxime de Jabrun
Global Executive VP Cyber Risk & Security
M. +33 (0)6 64 65 28 39
mdejabrun410@beijaflore.com

Beijaflore

Cyber Risk & Security Blog
http://blogrisqueetsecurite.beijaflore.com

Headquarters (Paris, France)
Pavillon Bourdan
11-13 avenue du Recteur Poincaré
75016 Paris

Belgium (Brussels)
IT Tower
Avenue Louise/Louizalaan 480
1050 Brussels

Brasil (São Paulo)
Rua Luigi Galvani, 70 – 7°andar
Ed. Alana II, Brooklin
04575-020
São Paulo – SP

Brasil (Rio)
Rua do Passeio, 70 – 6° andar
Centro
20021-290
Rio de Janeiro – RJ

Switzerland (Geneva)
Rue de la Corraterie 26,
1204 Genève

US (New York)
733 Third Avenue, Floor 15
New York, NY 10017