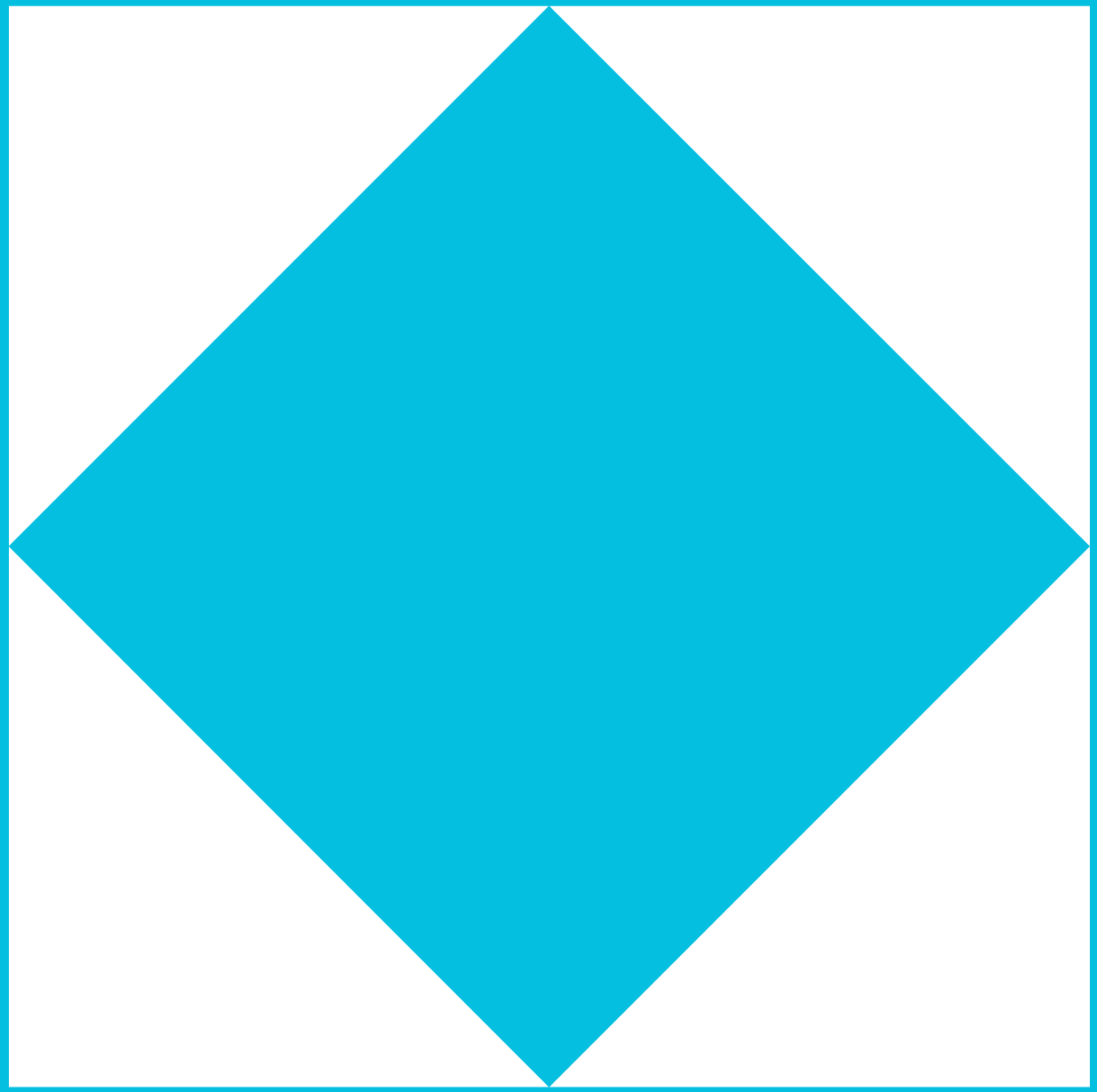
Project Management Institute Malaysia

OPERATIONAL TECHNOLOGY (OT) CYBER SECURITY

Open discussion about project management challenges implementing cyber security in the OT

International Project Management Day Seminar 2019

Jules Vos



About me…

- Head of cyber security strategy and architecture in the Oil & Gas industry
- Cyber security consultant/researcher in (Industrial) IoT and ICS/SCADA
- 10 years control system cyber security authority, author of global standards and reference architecture and automation project lead at Shell Projects & Technology
- 9 years managing consultant and project manager at Capgemini working mainly for Oil & Gas and power industry
- 12 years control system engineer and project manager at Yokogawa

Open

Definition of OT

Operational Technology (OT) and Industrial Automation and Control Systems (IACS) are umbrella terms for the hardware and software monitoring and controlling industrial production processes

Open

OT characteristics

- Health-Safety-Security-Environment criticality
- It is often a 24/7 environment
- Probability of failure on demand close to zero. Highly reliable and robust
- Integrity-availability-confidentiality order of importance
- Complicated hybrid infrastructure…..for specialists only
- IT people lack control knowledge, Control people lack IT knowledge
- It looks like an ordinary ICT environment….but it isn’t
- There will always be an obsolete system causing a headache

OT engineer, managers and operators are people with a mission…

Open

Some statistics

56% of the SME-business suffered from a virus attack in 2003

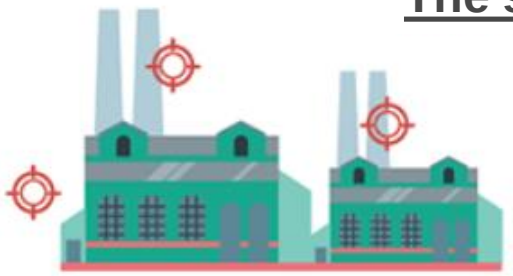
Research among SME companies showed awareness about internet threats and risk:

- ***77,5 % has a security policy to fight viruses, spam, hackers and unauthorised access***
- ***63,5 % has an e-mail security policy***
- ***21,5 % says that securing business data is top priority for the next 12 month***

Source: Trendmicro

What happened to the top priority of 2003?

The state of industrial cyber security 2018



77%
believe they are likely to become a target of a cybersecurity incident involving ICS

but

48%
don't have specific OT/ICS incident response program

31%
experienced one or more incidents last year

Source: Kaspersky

Real or fake….

ASML

Access ***Theft***

Ukraine

Hack ***Disruption***

Maersk

Notpetya ***Ransom***

Industry

Conficker ***Disturbance***

Saudi Arabia

Triton ***safety degration***

Iran

Stuxnet ***Sabotage***

Ransomware: Norsk Hydro ($50 mill, LockerGoga), MSD ($125 mill), Tsjernobyl, Maersk ($350 mill)
Honda/Renault/Nissan (Wannacry)
Disgruntles employees: Tesla, Sewage water control system Australia

It is real …. But stay focused on *your* risk profile

Understand your cyber opponent

Examples

- Cyber criminals who just want to make money (e.g. using ransomware)
- Nation states or people that want to steal knowledge
- Competitors that want to frustrate your business or success
- Disgruntled employees
- Activists that are looking for compromising data (e.g sensitive emission data)
- People that want to hit you for a personal reason
- Nation states, groups or individuals that may want to create mass societal disruption
- ….

But also

- Vulnerabilities or unacceptable cyber dependencies in the supply chain
- ….

Don’t fight against non-existing or imaginary enemies…frame correctly

Open

Integrated domains and data…the future

Ambition

- **Deliver reliable products**
- **Produce reliably**
- **Be a reliable supply chain partner**

Ecosystem

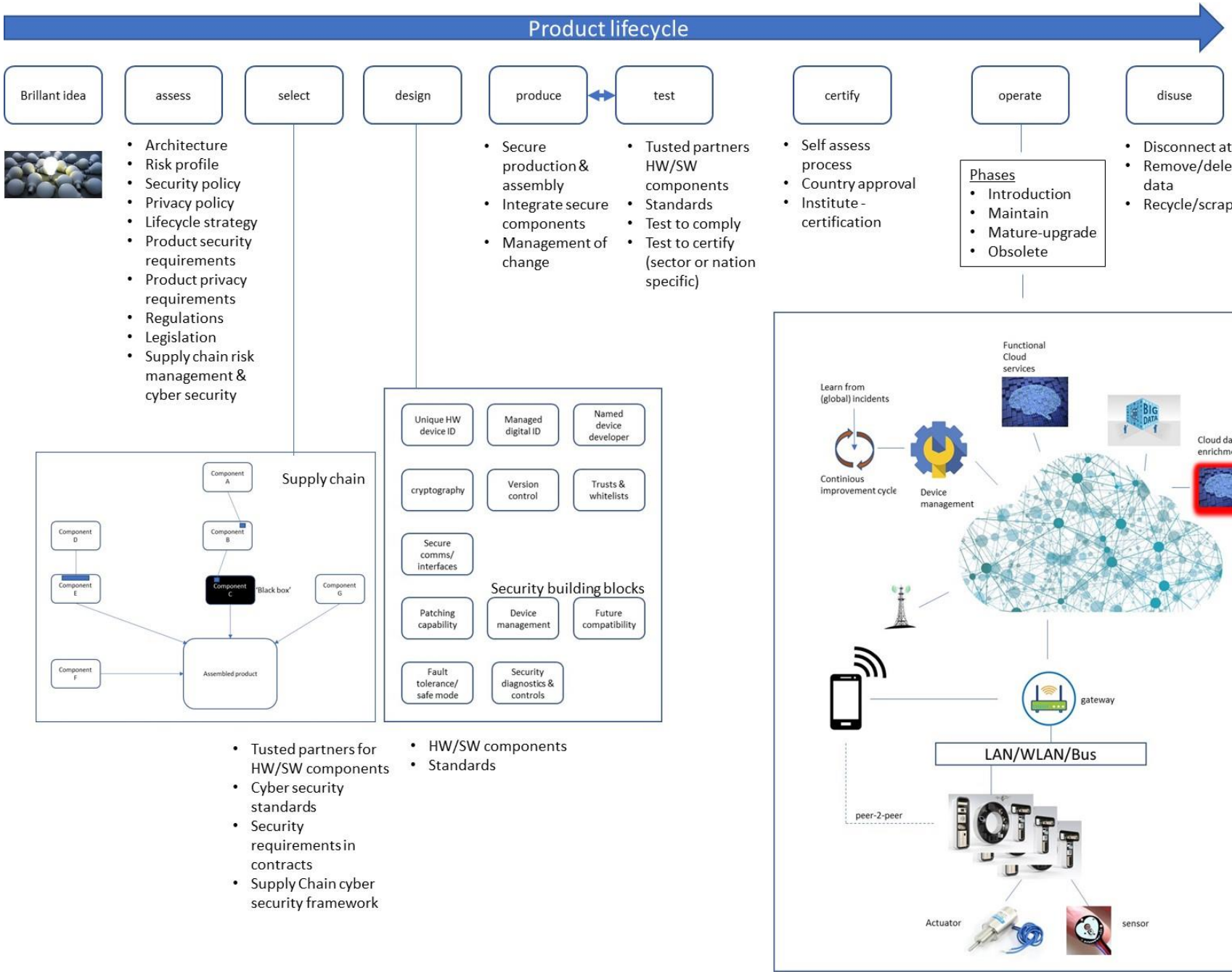
- **Office domain**
- **Software development**
- **Production floor**
- **Supply chain**
- **Cloud..**

OT way forward

- **Architecture incl. security**
- **Secure equipment**
- **Implement/configure/test**
- **Life cycle governance/maintain**

Cyber security must be an obvious part of your daily business

Open



Example of IoT cyber security elements during the product lifecycle

And how about the OT cyber business case?

OT cyber security is the enabler for a safe, secure and robust production:

- Development of digitalization (e.g. IoT, cloud based ecosystems, big data…)
- Use of commercial of the shelf ‘open’ products (so non-proprietary)
- Seamless integration of the production domain with other internal & external domains

OT cyber security facilitates the SME ambition to produce reliable robust products, to produce reliably and to be a reliable and responsible partner in the supply chain
Cyber security is a necessity both in products, production, supply chain and throughout the product lifecycle
The need for cyber security is there to stay…

Open

Lessons learned

- The initial OT cyber security project is the start of integrating security into business operations
- Industrial automation and office automation experts are no obvious partners
- Understand the difference between risk based and compliancy based security
- Based on risk profile pick and choose the relevant topics for your organization
- Appoint a focal point that is trusted by industrial and office automation experts, who understands OT risks and who is fully skilled to translate the risks into business terms that are understood by decision makers
- Outsourcing OT cyber security carries the risk of lacking subject understanding making companies relaxed and thinking that everything is under control
- It will never be enough, 100% secure doesn’t exist, so incident response/Business continuity planning is crucial
- Build on existing processes in your organization

Open

Useful standards

- NIST control framework
- NIST 800-82 standard
- IEC-62443 range of standards

Open