Orange
Cyberdefense

Securing the digital factory

Tommy Van de Wouwer, Security Officer at Atlas Copco

October 21, 2022

orange™

Not that long ago…

Factories running in a fenced-off environment

- Specific protocols & specific devices
- Very slow changing/stable, but not always benefiting from new features
- Managed by OT engineers

IT serving the ‘corporate world’

- More common protocols
- Fast changing, not always that stable, but quickly implementing features
- Managed by IT geeks

Today (or was it yesterday?)

Things changed over time without a real strategy

Today (or was it yesterday?)

- Attacks increase & impact increases (digital factory)
- IT & OT converge & use of cloud / 5G → introduces new benefits & risks
- Risks spread from IT to OT & from OT to IT → entry points are everywhere
- IIoT brings benefits & risks

Need for an integrated approach

Need for a new approach

OT needs

- Have a stable environment
- Make faster changes, experiment with new technology
- Leave us – we are doing fine
- Production is important

IT & compliance needs

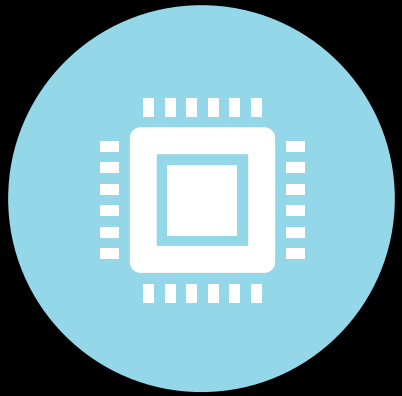
- Reduce risk in the corporate environment
- Help to fulfil needs


Actually the needs are not that different.
Why aren’t we understanding each other?
It’s all about bridging the gap.

Contributing to a more secure environment

Increased safety and reliability

- Access and interference is restricted
- Traffic is monitored

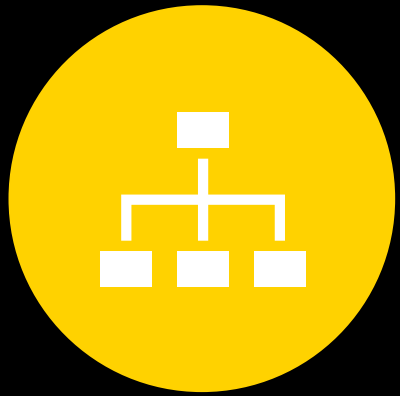


Increased availability

- Disruption will be minimized to the impacted segment(s)
- Improved performance.

Easier onboarding & isolation of OT devices

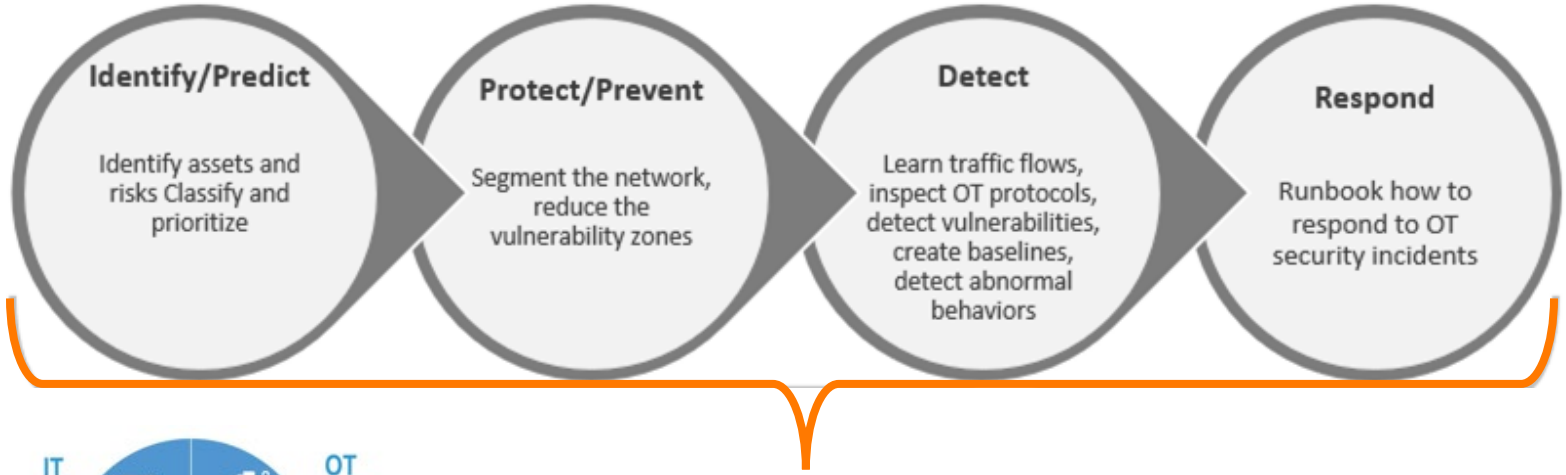
- Guidelines and automatic procedures
- Automatic application of the needed security policies.
- Isolation



Increased ownership & management of OT assets

- Ownership will need to be defined & systems maintained from a business perspective
- Supported with technical tools like a centralized inventory.

OT security program – approach



Manage

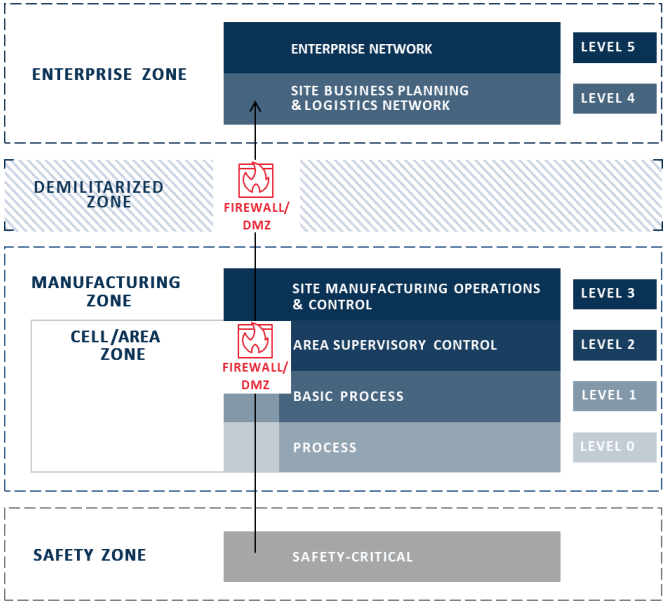
Continuous improvements, changes, needs & challenges

BUSINESS CONTINUITY

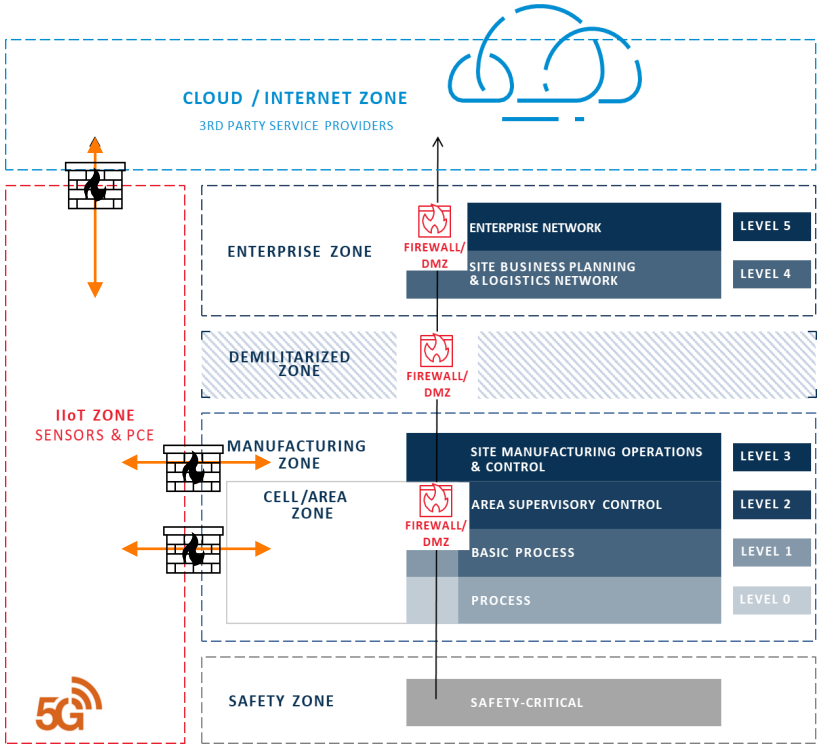
Tip: Follow standards as guidance not as the bible: IEC 62443 & NIST CSF

Evolution towards IIoT and Cloud services

Established Purdue principles
Purdue Enterprise Reference Architecture



Extended model for Cloud connected services and IIoT



Monitoring OT networks

It’s great to collect data but how to find what really matters?

Use a monitoring tool that specialised in OT

Use an External SOC with expertise in OT

OT has other protocols, need for a different approach may be needed

Threat intel is essential to find relevant events

- Monitoring solution with good DB
- Good partner needed
- Integrate IT & OT data in a single viewing pane

Monitoring OT networks

It’s great to collect data but how to find what really matters?

Why you need good asset inventory

- You can only protect what you know
- Assets, data streams,…

You need to baseline

- Lots of false positive & false negatives
- Needs a lot of data as input
- Takes a lot of time and input from the OT engineers

What we noticed

- Lack of OT knowledge in IT and IT knowledge in OT
- Not that much experts that can bridge the gap
- Monitoring solutions are not very mature yet

Final thoughts

The road will be long but every step counts

- Start with the low hanging fruit to get buy-in
- Plan well ahead for the difficult steps

Start small think big

- Keep the end state (Nord star) in mind
- Make sure every decision contributes to the end state

Build trust in the OT community

- They can become your biggest fans or your worst enemy
- Celebrate success

Prepare for the worst

- Have a good incident response
- Keep BCM up to date
- Test DRP