SUPPLY CHAIN ATTACKS

– Reflections on risk mitigation

Kim Hyldgaard, Lead Security Architect

11th May 2022

be
think
innovate

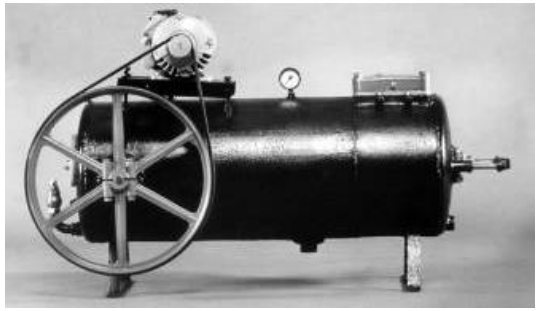
GRUNDFOS

INTRODUCING GRUNDFOS

be
think
innovate

GRUNDFOS

One man’s ambition



1945

“The world is full of problems that can be solved in a better way”

Poul Due Jensen

Grundfos in brief

1945
when it all started

#1
pump manufacturer in the world

19,000
employees

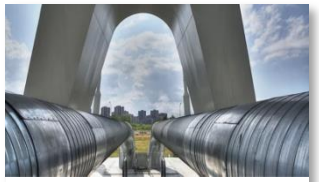
100+
companies worldwide

16,000,000
units produced per year

DKK 26.3
billion net turnover in 2020

Solutions for applications across all customer segments

Commercial buildings
Air conditioning
Heating
Hot water recirculation
Water pressure boosting
Water disinfection
Wastewater



District energy
District cooling
District heating

Domestic buildings
Hot water recirculation
Groundwater intake
Heating
Water pressure boosting
Rainwater harvesting
Wastewater

Industrial processes
Biofuel
Bottle washing
CIP/SIP
Cooling
Desalination
Filing
Leach mining

Industrial utilities
Temperature control
Boiler systems
Fire protection
Heating
Water supply
Water treatment
Wastewater

HVAC OEM
Boiler
Cooling
Domestic Hot Water (DHW)
Heat pump
Heating Interace Units (HIU)
Solar thermal
Space Heating

Municipal water supply
Drinking water treatment
Irrigation
Ground water intake
Solar water solutions
Surface water intake
Community water supply
Water distribution

Municipal wastewater
Flood control
Wastewater treatment
Wastewater transport

Agriculture and irrigation
Fertigation & Chemigation
Drip micro spray
Frost protection
Irrigation groundwater supply
Livestock watering
Pivot pressure boosting
Solar boosting and water supply solutions

Intelligent solutions for pump systems and water technology

GRUNDFOS iSOLUTIONS

PUMP CLOUD SERVICES

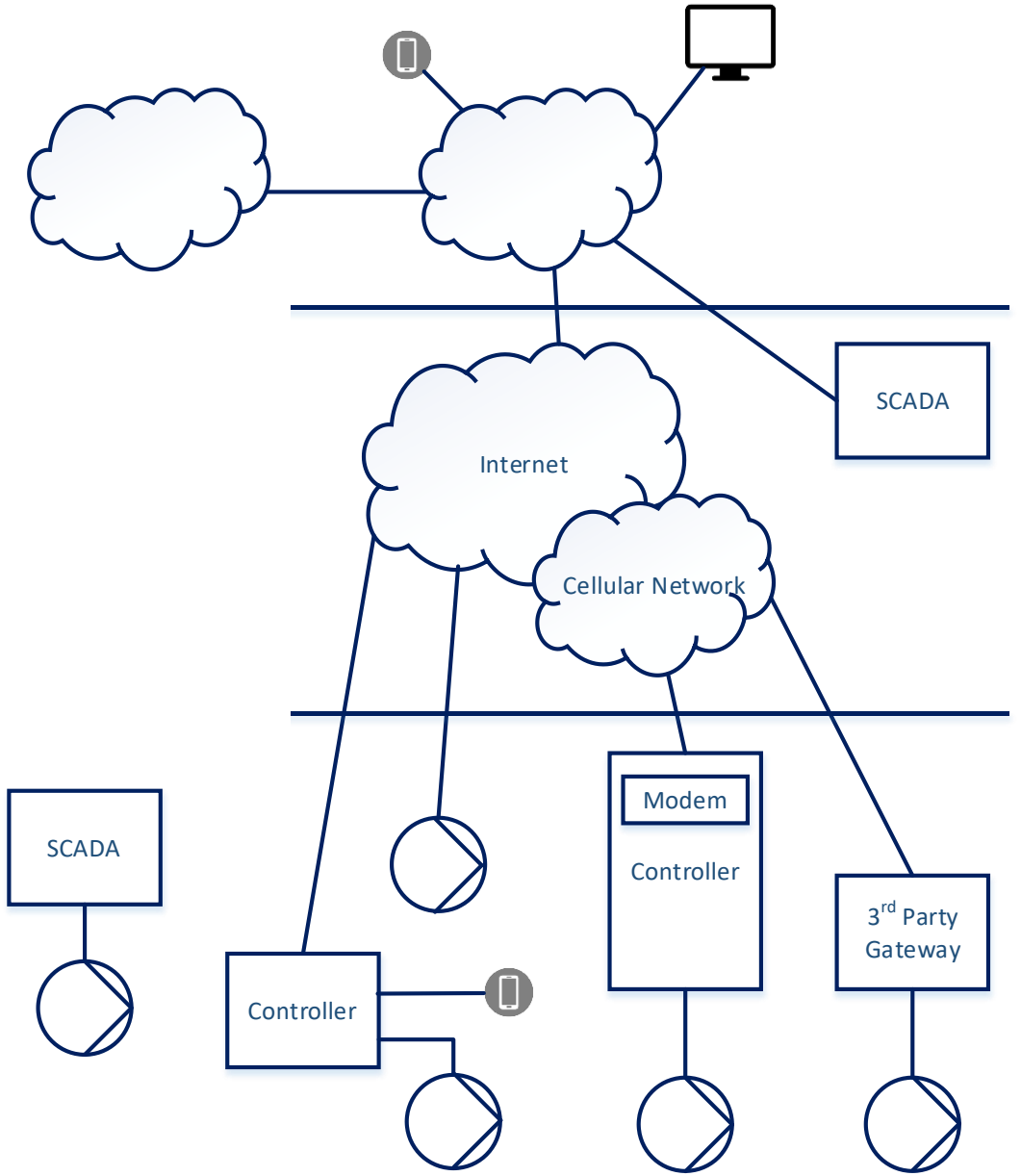
High **energy efficiency**

Improved **reliability**

Complete **system overview** and **control**

Customer specific **digital offerings**

Simple might be complex



The vast supply chain landscape

Hardware suppliers

- Smartphones, servers, laptops, …

Hardware component suppliers

- Chipsets (communication, security, processor, storage, …)

Software suppliers

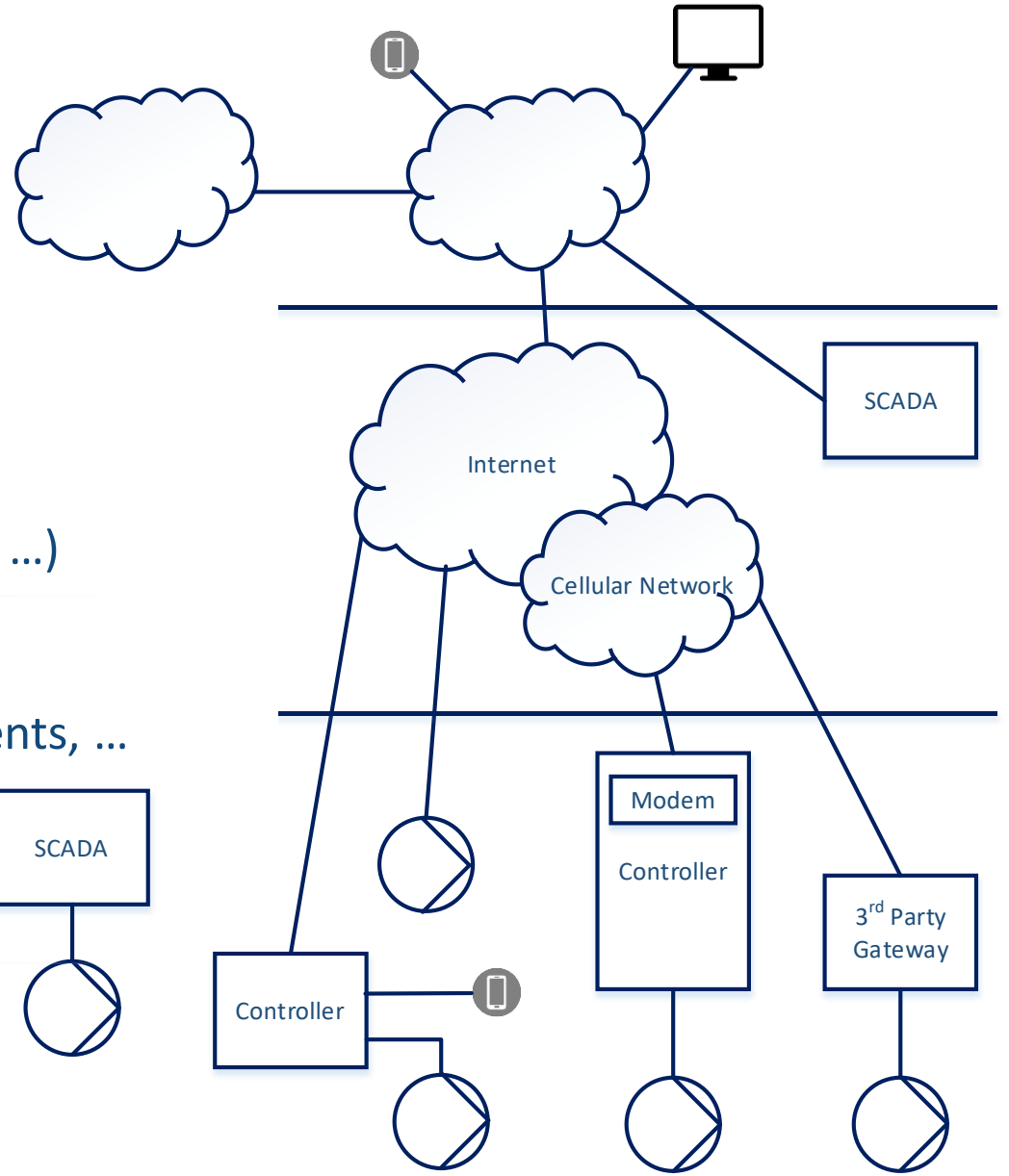
- Cloud, operating systems, protocol stacks, UI components, …

Software tools suppliers

- Develop, control, compile, build, test, deploy, …

Production facilities

- Putting it all together…



The legislation and standards landscape - excerpts

Executive Order
Enhancing Software Supply Chain Security [1)]

NIS2
Addresses security of supply chains [2)]

IEC 62443-4-2
Security requirements for externally provided components [3)]

IoT SF
Secure Supply Chain Production [4)]

1) https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
2) https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333
3) DS/EN IEC 62443-4-1:2018
4) IoT-SF Framework Compliance Version 2.0

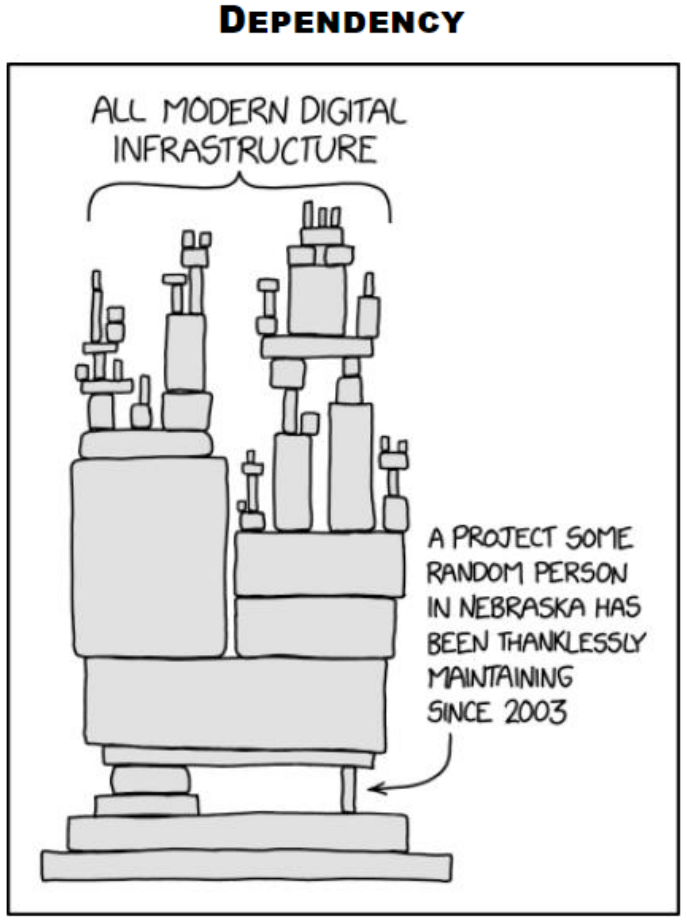
The inventory overview

Why is having an incomplete inventory of your web assets a problem? Because you can't protect something if you don't know you have it.

Tanya Janca, https://wehackpurple.com/the-importance-of-inventory/

The inventory must be

- Automatically obtained
- Complete
- Current
- Reliable
- Searchable
- Providing an overview
- Providing details
- Possible to integrate in your CI/CD pipeline
- **Helping in decision-making**



xkcd.com, https://xkcd.com/2347/

Practical examples 1)

Log4J / Log4Shell

ua-parser-js

Azure OMI / OMIGOD

Using a Software Composition Analysis tool to verify security risks

https://thehackernews.com/2022/01/researchers-find-bugs-in-over-dozen.html

Researchers Find Bugs in Over A Dozen Widely Used URL Parser Libraries

- *Belledonne's SIP Stack (C, CVE-2021-33056)*
- *Video.js (JavaScript, CVE-2021-23414)*
- *Nagios XI (PHP, CVE-2021-37352)*
- *Flask-security (Python, CVE-2021-23385)*
- *Flask-security-too (Python, CVE-2021-32618)*
- *Flask-unchained (Python, CVE-2021-23393)*
- *Flask-User (Python, CVE-2021-23401)*
- *Clearance (Ruby, CVE-2021-23435)*

Practical examples 2)

Log4J / Log4Shell

Azure OMI / OMIGOD

ua-parser-js

Using a Software Composition Analysis*) tool to verify security risks

https://www.cisa.gov/uscert/ncas/current-activity/2021/10/22/malware-discovered-popular-npm-package-ua-parser-js

"CISA urges users and administers using compromised ua-parser-js versions 0.7.29, 0.8.0, and 1.0.0 to update to the respective patched versions: 0.7.30, 0.8.1, 1.0.1 "

https://www.bleepingcomputer.com/news/security/dev-corrupts-npm-libs-colors-and-faker-breaking-thousands-of-apps/

"… users of 'colors' and 'faker' NPM projects should ensure they are not using an unsafe version. Downgrading to an earlier version of colors (e.g. 1.4.0) and faker (e.g. 5.5.3) is one solution."

*) In Grundfos an SCA tool is also used to help identifying license risks with Open-source software, but this a completely different presentation… ☺

Remaining challenges

Despite the tools already available, there are shortcommings

- Authenticity of the 3rd party software
  - Components, build tools, etc.
  - Existing versions do not change
  - Trust indications for new versions
- Update speed of intelligence databases
- Intelligence databases coverage
- Better support in your everyday life working with DevSecOps
- …

Thank you.

Kim Hyldgaard, khyldgaard@grundfos.com