Pitfalls of Security testing

ICS / SCADA / (I)(I)OT

Dieter Sarrazyn
https://secudea.be

Cybersecurity Services for Industry

Consultancy

Do you need help with cybersecurity within industrial environments? Do you require assistance in setting security requirements and guidelines for green fields? We provide independent, business driven industrial security consultancy services.

Assessments

Want to have your industrial environment tested, validated or assessed? Do you want to know what risks there are in your current environment? Need to perform risk or maturity assessments? We can help you identifying your risks through our assessment services.

Training

Whether you would like to learn something new like how to perform hardening of systems within industrial environments or if you want to organize an awareness day on OT security in your organization, we can provide you real experience based training and coaching.

Secudea
Cybersecurity services for Industry

IT Security since 1998

OT Security since 2008

https://secudea.be/blog

About Dieter Sarrazyn

IN CERVISIA VERITAS
EST. 2016
BEER ISAC

Reviewing committee IEC 62443

ISASecure Technical committee

Co-chair OT Focus group CyberSec Coalition

#Nuclear
#Energy
#Mining
#Food
#Utilities
#Transport
#Pharma
#Chemical

Pitfall #1 – Lack of planning

- Security testing is almost always an afterthought …
- Almost NEVER included in project planning …
- Sometimes included in project budgets …

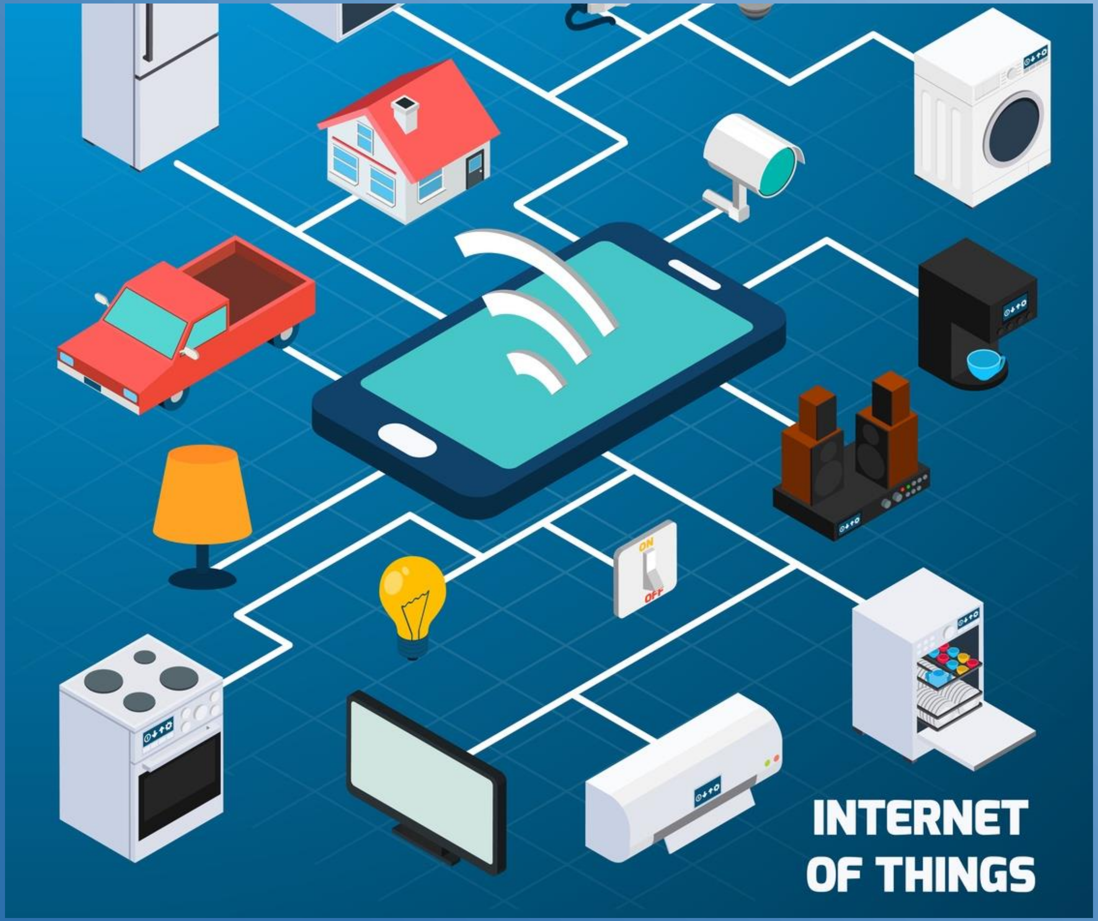
Pitfall #2 – Lack of Sufficient testing time

- Sometimes you don’t need (a lot of) time …
- Sometimes you very much need it …
- Implementation of CRA requirements could increase needed testing time …

Pitfall #3 – Insufficient testing devices

- If you only have a single device to test (play) with … Would you do all tests in your test arsenal ???
- Even DoS attacks that (could) brick the device… ???

- So have multiple test devices at hand !!
- Also important to verify issues



https://www.mistralsolutions.com/blog/iot-testing-processes-building-robust-iot-system/

Pitfall #4 – Lack of Permission

- Important in production environments
- Also sometimes in staging environments
- Have a work permit prior performing tests!!!
  - Testing allowed
  - Testing traced
  - Necessary precautions taken & mentioned

Pitfall #5 – Lack of decent testing checklist

- Include all requirements (CRA, IEC62443 …)
- Security <> Compliancy !!
- So leave room for additional tests/checks

ISTG

IoT Security Testing Guide

Luca Pascal Rotsch
Aaron Guzman

OWASP

Pitfall #6 – Scope creep…

- Don’t just go beyond your scope
- Its not good for you
  - Economically
  - Liability wise

- Either stick to your scope …
- Or stop testing and discuss scope extensions …

How to improve? Security Testing Strategy

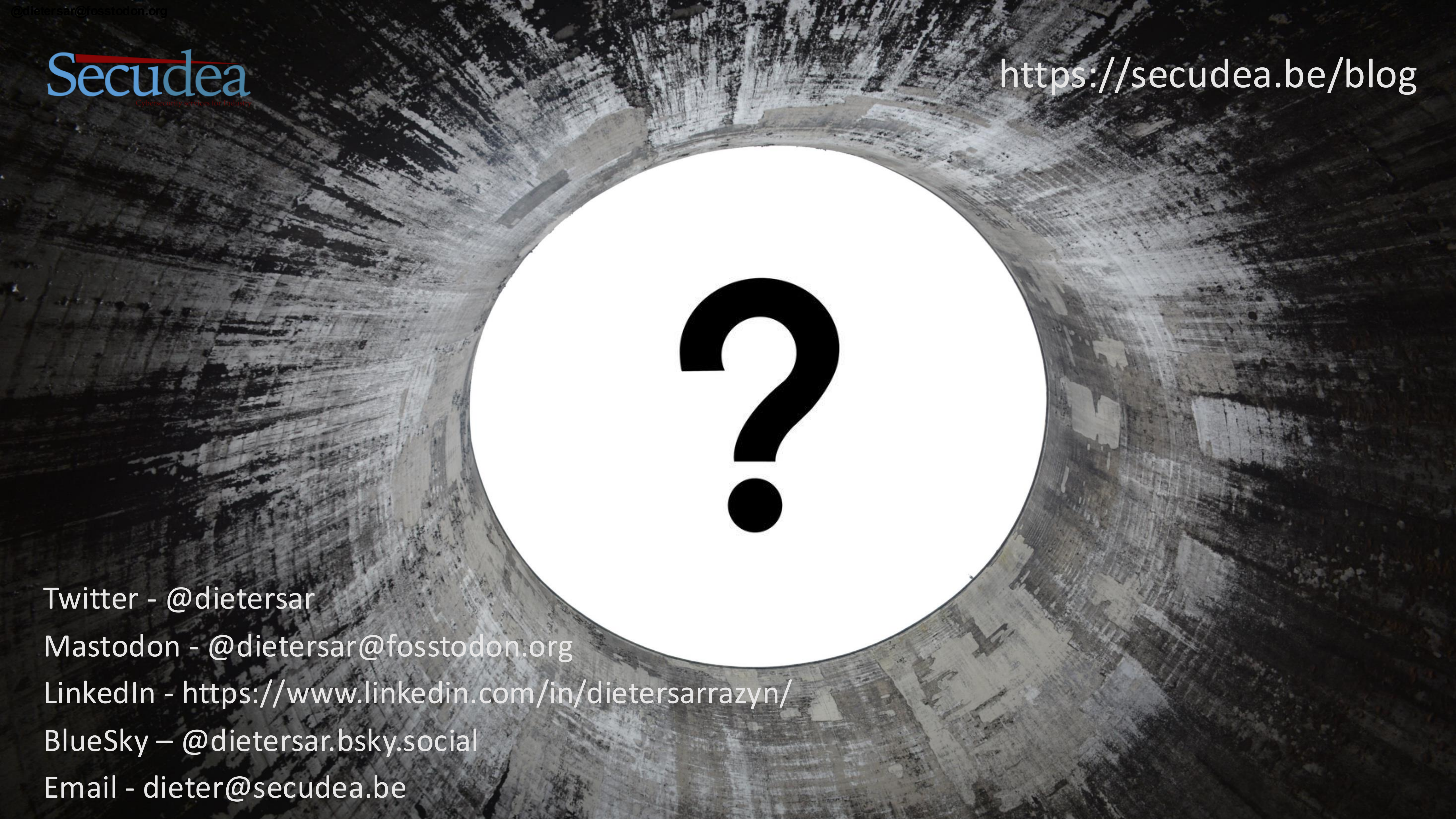
- Standardize your approach
  - Add specific tests after requirements analysis & risk assessments
  - Include the full “Device chain”
  - Include the accessibility of the device

- Be ready to include (& educate) vendor/ops/…
  - Their maturity will increase
  - Future projects will be better on security level
  - Future testing will be better planned…

- Security testing should be embedded within current regular project QA processes

Secudea

https://secudea.be/blog



Twitter - @dietersar

Mastodon - @dietersar@fosstodon.org

LinkedIn - https://www.linkedin.com/in/dietersarrazyn/

BlueSky – @dietersar.bsky.social

Email - dieter@secudea.be