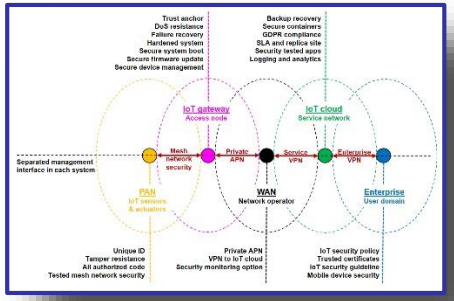
TLP:WHITE — RAJOITTAMATON
Tieto voidaan jakaa pakottavasta lainsäädännöstä johtuvat rajoitukset huomioiden vapaasti. Edellä tarkoitettuja rajoituksia tiedon jakelemiselle voidaan asettaa esimerkiksi tekijänoikeuslaissa. Tyypillisesti TLP:WHITE-luokiteltu tieto on jo saatavilla julkisista lähteistä.



KYBER-ENE 2017, Energia-alan kyberturvaaminen

Cyber security for lean IoT procurements

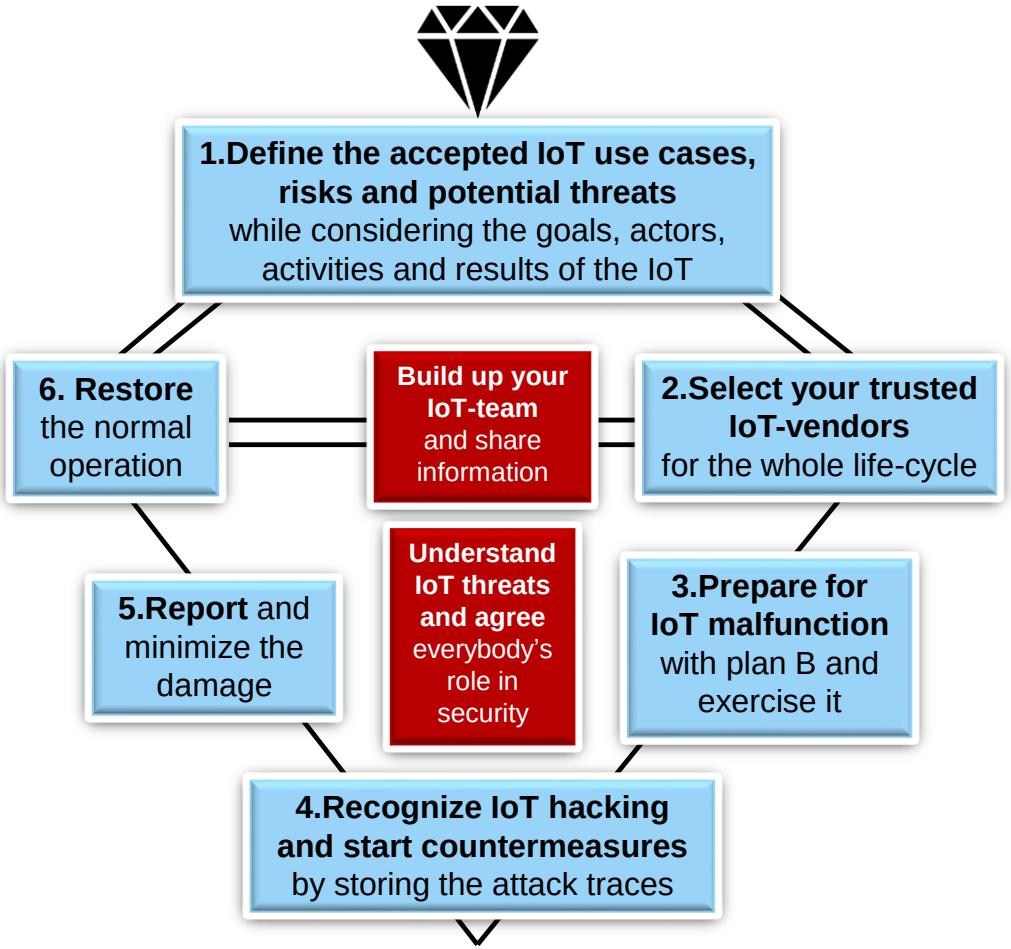
v. 20.4.2018

Editor: Pasi Ahonen, Principal scientist
VTT Technical Research Centre of Finland

INTENDED USERS:
Energy sector companies who need to negotiate and contract the CYBER SECURITY with their potential IoT service or solution providers.

Please, tailor and edit the presentation as you wish – to support your own requirements and use cases!

The steps to lean & secure IoT



Start by defining your IoT use cases!

Step 1:

1.Define the accepted IoT use cases, risks and potential threats
while considering the goals, actors, activities and results of the IoT

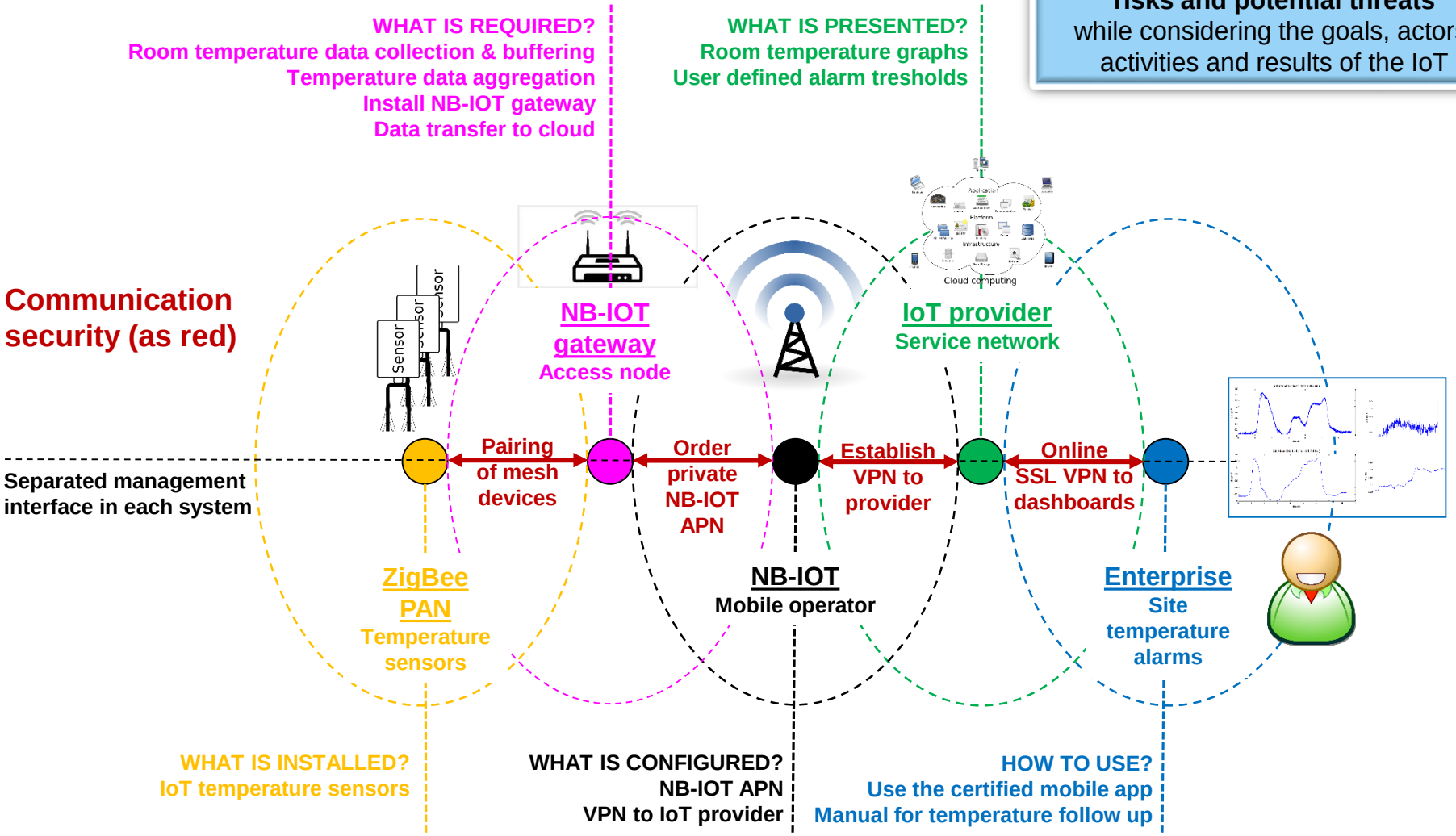
USE CASE shall determine the characteristics of the purchased IoT system!

USE CASE DESCRIPTION
Purpose: Do you need data collection, remote access, process control, or perhaps analytics…?
Actors: Operator, developer, m2m comm., security, vendor, end-user…?
Connection type: Always-on, on-demand, tiny, bulk, batch, real-time …?
Activities: Uploading data, reviewing production, configuring settings…?
Results: Alarms, fast responses, optimized energy consumption…?

EXAMPLE USE CASE (you may skip this): ”Remote site temperature follow up”

Step 1:

1.Define the accepted IoT use cases, risks and potential threats while considering the goals, actors, activities and results of the IoT



Then, check how IoT impacts to your business models?

(the approach to money making…)

Step 1:

1.Define the accepted IoT use cases, risks and potential threats while considering the goals, actors, activities and results of the IoT

Do you need updates to your business models?

1. Business model for IoT?	Document the business models of the intended IoT use cases
2. Dependencies of IoT?	Identify all internal & external dependencies that the intended IoT use cases will bring in
3. Does IoT affect changes or expansions to other systems?	Identify the needed changes and expansions to the current systems and services, especially the effects to the stored or processed data
4. Finalized business models	Finalize your business models, including the impacts of IoT use cases

Assess the risks through impacts

Step 1:

1.Define the accepted IoT use cases, risks and potential threats
while considering the goals, actors, activities and results of the IoT

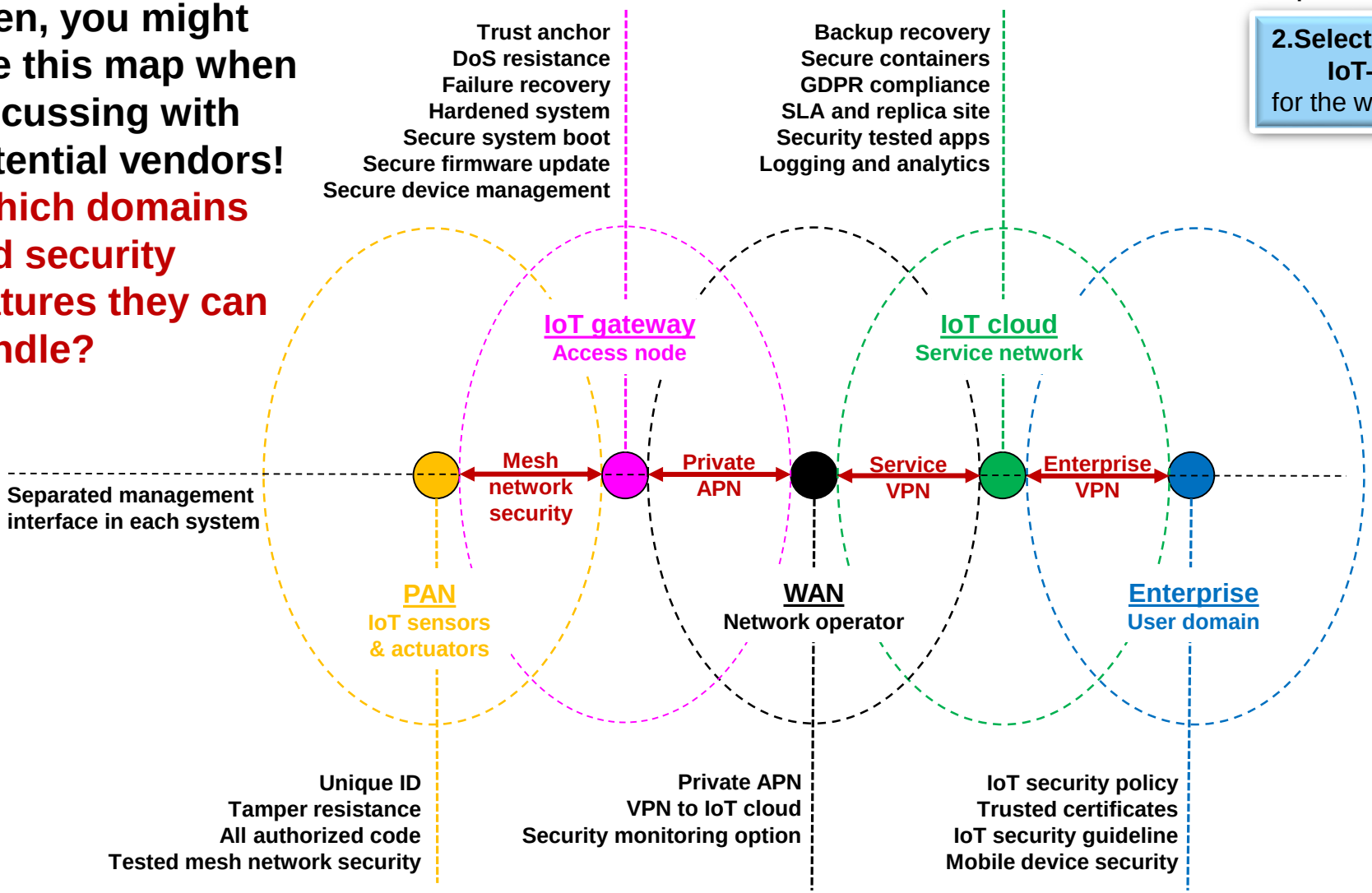
Carry out the risk assessment of your IoT use case.
Estimate risks via negative impacts, e.g.:

- If the IoT use case may only impact **your own work**, then you may accept **more** uncertainty…
- If the IoT use case may impact **your own colleague's work**, then you may accept **some** uncertainty …
- If the IoT use case may impact **your own department's outcome**, then you may accept **less** uncertainty …
- If the IoT use case may impact **your own company's outcome**, then you may accept **even less** uncertainty …
- If the IoT use case may impact **outside your company**, then you may accept **very little** uncertainty …

Then, you might use this map when discussing with potential vendors!
-Which domains and security features they can handle?

Step 2:

2.Select your trusted IoT-vendors
for the whole life-cycle



Step 2:

2.Select your trusted IoT-vendors
for the whole life-cycle

Discuss with vendors, about security!

Security by design
How security is taken care in the whole life cycle?
How changing security policies are taken in?
How human safety is supported?
How security is taken care in power conservation?
How elements are encapsulated to compartments?
How the products are security tested?
How software code reviews are done?

Privacy by design
How privacy enforcement is implemented?
How privacy of applications are assessed?

Asset Management
How asset and configuration management is supported?

Risk and Threat Identification and Assessment
How significant risks are identified?
How the intended use and usage environment is identified?

MORE EVIDENCE GIVEN?
➔ MORE POINTS!

Security policies!

Hint: Ask some evidence from your candidate vendors:
- About their *security by desing* -policy?
- What kind of risks they have already identified and how they are prepared?

Step 2:

2.Select your trusted IoT-vendors
for the whole life-cycle

4.2.1 End-of-life support
How products end-of-life is taken care of?
How long the patching and end-of-life security are supported?
How long the product performance and patch status are monitored?

4.2.2 Proven solutions
What proven solutions are used? What is proprietary?

4.2.3 Management of security vulnerabilities and/or incidents
Procedure for analysis and handling of security incidents?
How you manage vulnerabilities?
How you detect and report vulnerabilities?
Do you utilize Bug Bounty programs or similar?

4.2.4 Human Resources Security Training and Awareness
How do you train your personnel on security and privacy?
How do you follow up your trainings?
Would you like to open up the roles and responsibilities of cyber security in your organisation?

4.2.5 Third-Party relationships
How do you control 3rd party data processing?
How do you ensure that consumer's personal data is not illegally shared without their permission?
How do you ensure that cyber security is handled properly by all HW manufacturers and software developers?

Discuss with vendors, about security!

MORE EVIDENCE GIVEN?
➔ MORE POINTS!

Organization, people & processes!

Ask also some technical issues – select your priorities?

Hardware security
Do you implement root of trust in HW?
Do you utilize hardware security features? Which ones?

Trust and Integrity Management
Do you have trusted secure boot?
Do you employ cryptographically signed program code?
Do you employ controlled software installation?
Do the systems return to secure state after a problem?
Do you employ automated trust management?

Strong default security and privacy
Do you employ secure settings by default?
Do you employ individual device passwords?

Data protection and compliance
How do you ensure that the everybody can control his/her own personal data?
How do you enforce that only lawful personal data is used?
Do you minimize the collected personal data?
Do you employ GDPR requlation for personal data?
How do you ensure that everybody can control the processing of his/her own personal data?

System safety and reliability
How the system prevents unacceptable injuries and physical damages?
Do you employ self-repair/healing from failures?
Do you employ standalone operation?

Secure Software / Firmware updates
How do you employ the security of Over-The-Air (OTA) device updates?
Do you employ automatic firmware update mechanism?
How the backwards compatibility of firmware updates is ensured?

Authentication
How device specific authentication and authorization is employed?
How do you ensure that default passwords and usernames are changed?
How do you support strong authentication mechanisms?
How passwords are secured within the system?
How 'brute force' login attempts are blocked by the system?
How password and key recovery procedures are secured?

Authorization
How applications are enforced to operate with least privileges?
Is privileged program code isolated in device firmware?

Access Control - Physical and Environmental security
How device's integrity and confidentiality is protected by access controls?
Can you employ different security levels depending on context?
How do you employ tamper protection and detection?
How the device is protected against disassembly?
How do you support the disabling of physical external ports?

Cryptography
What cryptographic algorithms and key lengths are supported and how these are maintained and updated?
How the cryptographic keys are managed?
What lightweight security techniques are supported?
How scalable is the supported key management scheme?

Secure and trusted communications
How the security of data transmission and storage is ensured?
What standardized communication security protocols are available?
How passwords and other credentials are protected in data networks?
How data authenticity is ensured?
How all received data, connections and peer devices are authenticated?
Are your IoT devices permissive by default rather than restrictive?
How unauthorized connections are prevented?
How specific ports and connections can be disabled?
How the data traffic rates can be limited?

Secure Interfaces and network services
How the network elements support the isolation of subnetworks?
Do the device communication protocols protect against attacks?
Do you provision a single secret key?
Do you harden your system before commissioning?
Can the system resist against message storms?
How the web interfaces are protected against attacks?
How security is considered in error messages?

Secure input and output handling
How is input validated before processing and output filtered?

Logging
What events can be captured and stored by the logging systems?

Monitoring and Auditing
What kind of regular security monitoring you support?
What kind of security audits and tests are employed and when?

Step 2:

2.Select your trusted IoT-vendors
for the whole life-cycle

Discuss with vendors, about security!

MORE EVIDENCE GIVEN?
➔ MORE POINTS!

Understand IoT threats and agree everybody's role in security

The FINAL MESSAGE for IoT procurements:

- ➔ **Select your IoT partners carefully!**
- ➔ **Agree everybody's security role and tasks for the whole life cycle!**