IoTSec Taxonomy Proposal

IoTSec

Consortium meeting

11. October 2018

Rune Winther

Multiconsult

rune.winther@multiconsult.no

+47 91665762

Øivind Berg

Senior Researcher Energy Economics

Oivind.berg@smartinnovationnorway.com

+47 995 21 679

Topics

- Background and goal
- Considerations
- Causes vs. consequences
- About the proposal
- Practical issues
- The proposal

Background and goal

- We want to establish a trust case (explicit argument) for security, privacy and dependability in smart grids
  - The starting point is the claim “Smart grid is adequately secure, private and dependable (SPD)”
- A convincing trust case requires a precise understanding of this claim
- Thus, we need a taxonomy for SPD, specifically suitable for building trust cases

Considerations

- No ambition to establish a «globally» accepted taxonomy
  - Focus is on our needs to formulate a *precise claim* in the trust case
- Should, as far as possible, be based on existing taxonomies
  - «Pick and choose»
- The taxonomy must cover all of SPD, but also be usable for each of S, P and D separately
- Essential that the structure directly supports the construction of trust cases

Causes vs consequences

The difference between safety and security can be described as:

- Security: The effect the world has on a system
- Safety: The effect a system has on the world

- From the perspective of the system, this means that:
  - Security is about causes
  - Safety is about consequences

- When establishing the taxonomy we need to be conscious about whether we characterize causes, consequences, or both

Security – Can go both ways…

- Security defined by the CIA triad
  - Loss of confidentiality, integrity and availability can be interpreted as primarily being characterizations of *consequences*
- Security defined as “protection against threats”
  - Focus is primarily on *causes*

- Neither is more correct, but we need to be consistent, and ensure that terms are understood in the same way by all stakeholders

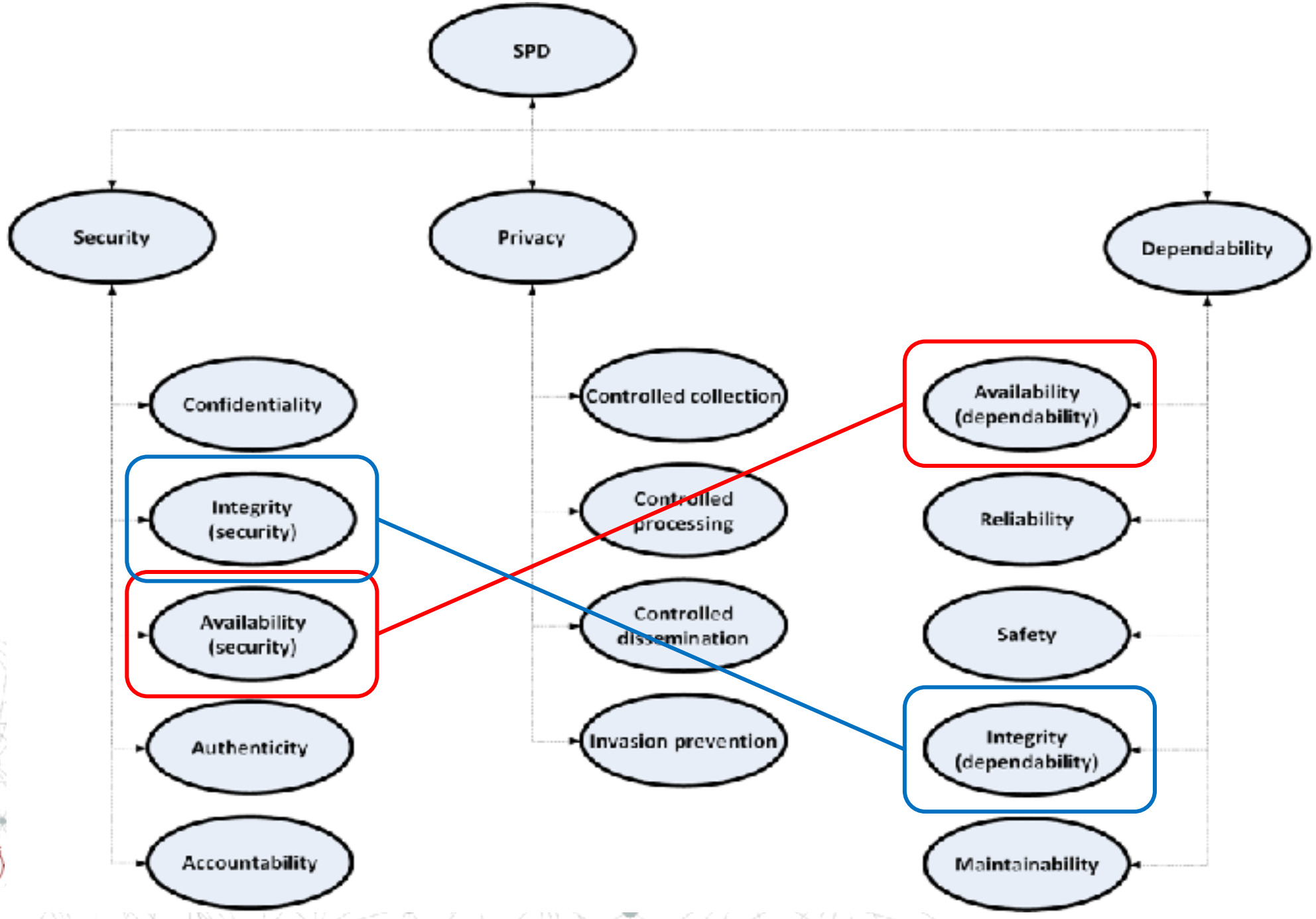
About the taxonomy proposal

- Primarily focused on characterizing *consequences*
  - Sort of…
  - Typically the loss of some characteristic
  - Top-level claim will often be about the *absence of negative effects*
- Primarily based on
  - Laprie et.al, “dependable and secure”
  - PIPS-project
  - Stallings, W. *Cryptography and network security: principles and practice*

Practical issues

- Since the taxonomy is focused on consequences, we need to ensure that all relevant causes are included in the trust cases
  - Whether unwanted events are intentional or unintentional should be explicitly addressed in the trust case
  - Should we extend the taxonomy to address both causes and consequences?

- Confidentiality is in the taxonomy only associated with security, but is usually also part of dependability


SPD
Security
Privacy
Dependability
Confidentiality
Integrity (security)
Availability (security)
Authenticity
Accountability
Controlled collection
Controlled processing
Controlled dissemination
Invasion prevention
Availability (dependability)
Reliability
Safety
Integrity (dependability)
Maintainability

The taxonomy – Definitions - Security

Security	
Confidentiality	The absence of unauthorized disclosure of information.
Integrity (security)	Absence of unauthorized system alterations. Note: Unauthorized system alterations can be internal or external, as well as intentional or unintentional.
Availability (security)	Availability for authorized actions only.
Authenticity	The property of being genuine and being **able to be verified and trusted**; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.
Accountability	The security goal that generates **the requirement for actions of an entity to be traced uniquely to that entity**. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Because truly secure systems are not yet an achievable goal, we must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

The taxonomy – Definitions - Privacy

Privacy	
Controlled collection	The individual has control on what, and how, personal information is collected.
Controlled processing	The individual has control on how, and for what purpose, personal information is used.
Controlled dissemination	The individual has control on what, and how, personal information is disseminated.
Invasion prevention	Protection against disturbance/intrusion of an individual's solitude or seclusion

The taxonomy – Definitions - Dependability

Dependability	
Availability (dependability)	Readiness for correct service.
Reliability	Continuity of correct service.
Safety	Absence of catastrophic consequences on the user(s) and the environment.
Integrity (dependability)	For safety: The probability of a safety-related system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time. General: Absence of improper system alterations.
Maintainability	Ability to undergo modifications and repairs.