Updated October 2nd, 2018
By Rune Winther

Proposal: Defining the core attributes of the SPD trust case

Introduction

When building an argumentation that a Smart Grid is “good enough”, we need to be precise about what is meant by “good enough”. In the IoTSec project so far, the terms security, privacy and dependability have been used as core attributes. However, I have problems finding definitions in the IoTSec (and Scott) project that are adequately precise *for use in the SPD trust case*.

I have therefore written this proposal for defining the core attributes relevant to the SPD trust case. It is based on the terms dependability & security, as defined in [1] and [2], but with the addition of privacy. The definition of privacy is based/influenced by the trust case developed as part of the PIPS-project [3], as well as [4].

Attributes of SPD

J.C. Laprie defined dependability & security as shown in Figure 1.

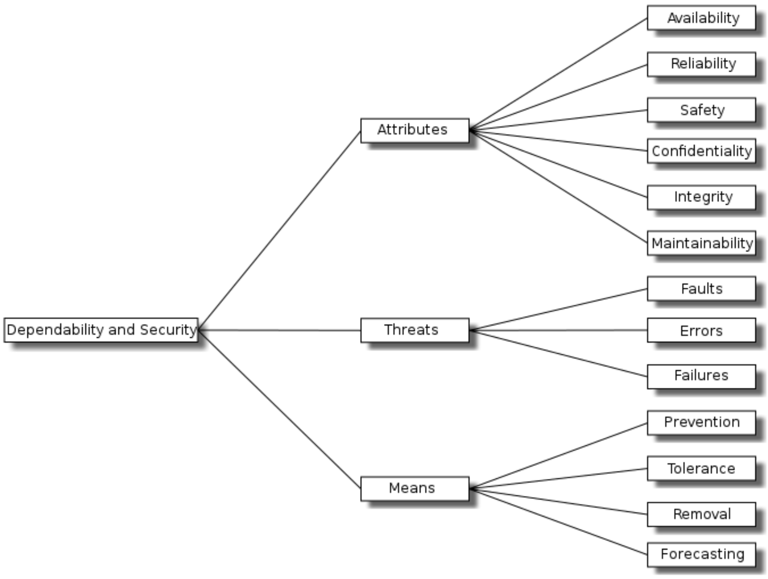

Figure 1: Taxonomy of dependability & security.

For the formulation of the top-level claim in the trust case, the attributes in Figure 1 are of primary interest. In this taxonomy, the terms dependability and security are to some extent overlapping:

- Dependability consists of: Availability, reliability, safety, integrity and maintainability
- Security includes: Confidentiality, integrity and availability (the CIA triad)

It should be noted, however, that the meaning of the overlapping terms (i.e. integrity and availability) might be interpreted differently for dependability and security. In a security context, integrity is primarily thought of as “ability to prevent unauthorized access”, while integrity in e.g. a safety context is related to probability of failure of a safety function.

As suggested by Elahe Fazeldehkordi, the definition of security has been extended to also include authenticity and accountability.

The term privacy is naturally related to GDPR and personal data:

- Personal data is any information that relates to an identified or identifiable living individual.

Privacy can then be defined as "the ability to have control over one's own personal data". Although written for a slightly different context, the taxonomy of privacy suggested in [4] provides a possible detailing of privacy. This taxonomy identifies four categories:

1. Information collection
2. Information processing
3. Information dissemination
4. Invasion

Figure 2 summarizes the above, in the form of a proposed taxonomy for the SPD trust case.

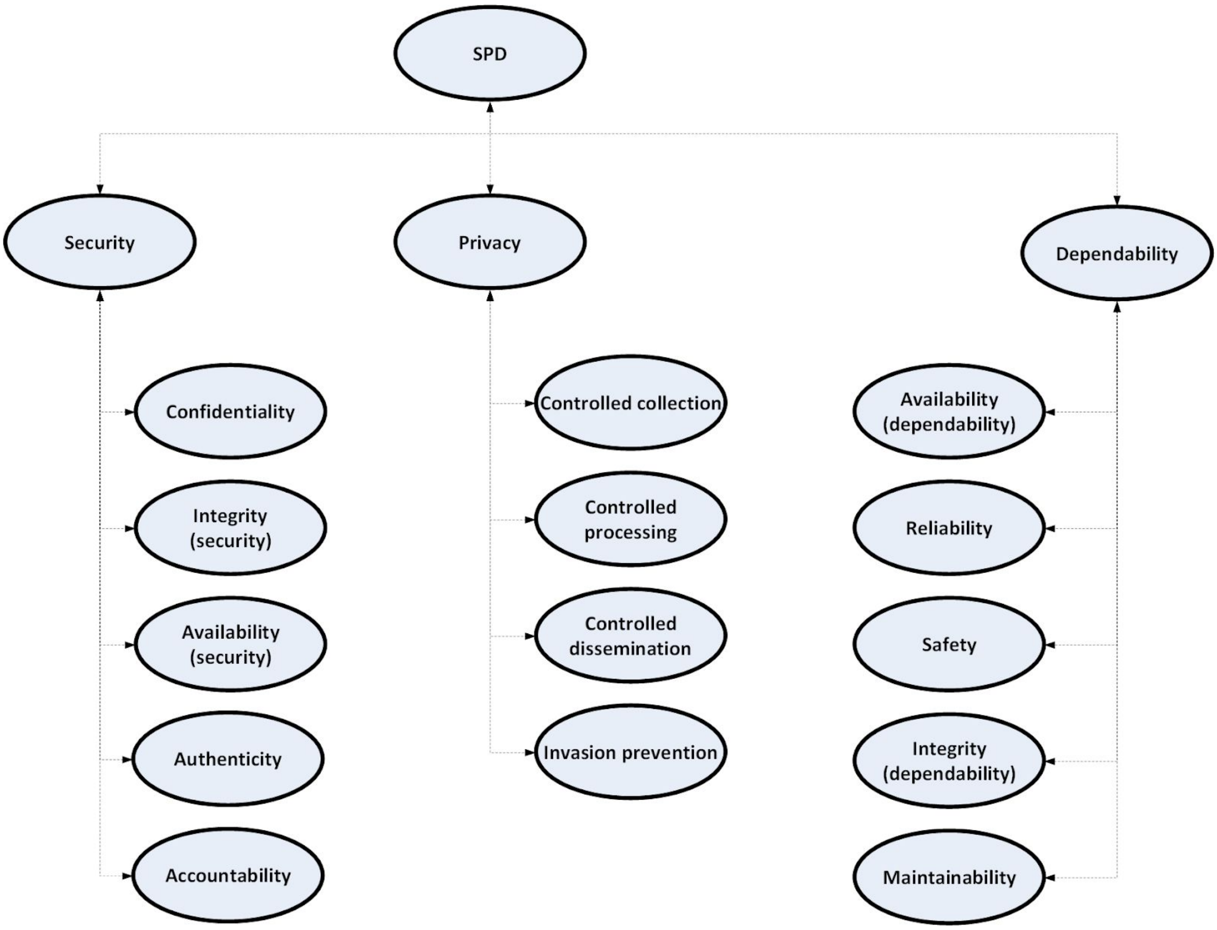

Figure 2: A proposed taxonomy for SPD.

The following definitions are based on [1], [2], [3], [4] and [5], with some adjustments and adaptations:

Term	Definition
	Security
Confidentiality	The absence of unauthorized disclosure of information.
Integrity (security)	Absence of unauthorized system alterations. **<u>Note:</u>** 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.
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
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.

Causes vs consequences

The proposed taxonomy focuses on system attributes, which in fact are primarily characterizations of the outcome of unwanted events. Since risk is typically defined as the “combination of the consequence and the probability of unwanted events”, it makes sense to define the taxonomy this way. However, an issue that is usually attributed to security, and which might not be 100% clear from the above proposal, is the need to address intentional actions, as well as unintentional events. It should, therefore, be noted that when addressing SPD we must include both intentional and unintentional issues when considering possible causes to loss of SPD. In practice, this could be ensured by making separate statements in the trust case regarding “intentional” and “unintentional” events.

References

[1] J.C. Laprie. *Dependable Computing and Fault Tolerance: Concepts and terminology*, in Proc. 15th IEEE Int. Symp. on Fault-Tolerant Computing, 1985

[2] A. Avizienis, J.C. Laprie, B. Randell and C- Landwehr. *Basic Concepts and Taxonomy of Dependable and Secure Computing*, IEEE Transactions on Dependable and Secure Computing, vol. 1, No. 1, January-March 2004

[3] https://cordis.europa.eu/project/rcn/71245_en.html

[4] https://wiki.openrightsgroup.org/wiki/A_Taxonomy_of_Privacy#Introduction

[5] Stallings, W. *Cryptography and network security: principles and practice* SIXTH EDITION (chapter 1, p 29-34).