Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Institute of Metrology METAS

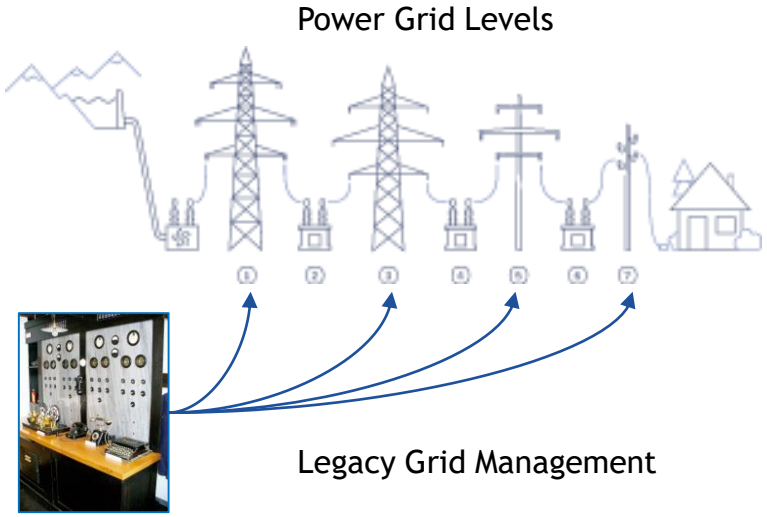
Data Security Evaluation for intelligent Measurement Systems in Switzerland

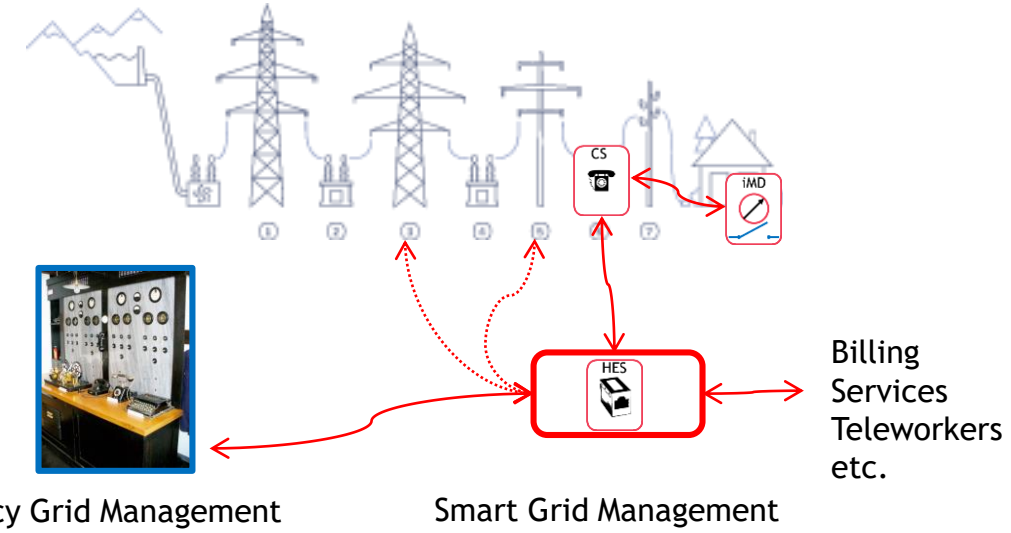
Dr. Volker Zeuner, August 2021

Contents

- Smarting-up the Power Grid
- Overview
- Derivation for the intelligent Measurement Device
- Data Security Testing Scheme (on the edge of a nutshell)
- Fusion of Assets, Protection and Specification
- Outlook

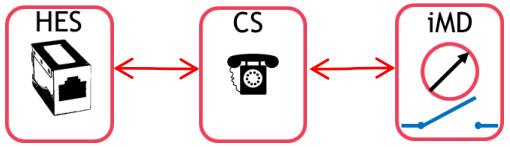
Smarting-up the Power Grid





iMS: intelligent Measurement System

HES: Head End System
CS: Communication System
iMD: intelligent Measurement Device



- RED means bi-directional ICT
- CS and iMD in unsupervised locations
- HES assumed to be physically safe, but

- Data Security Requirements for Communication
- Data Security Requirements for Resilience
- Data Security Requirements for Connectivity

Overview

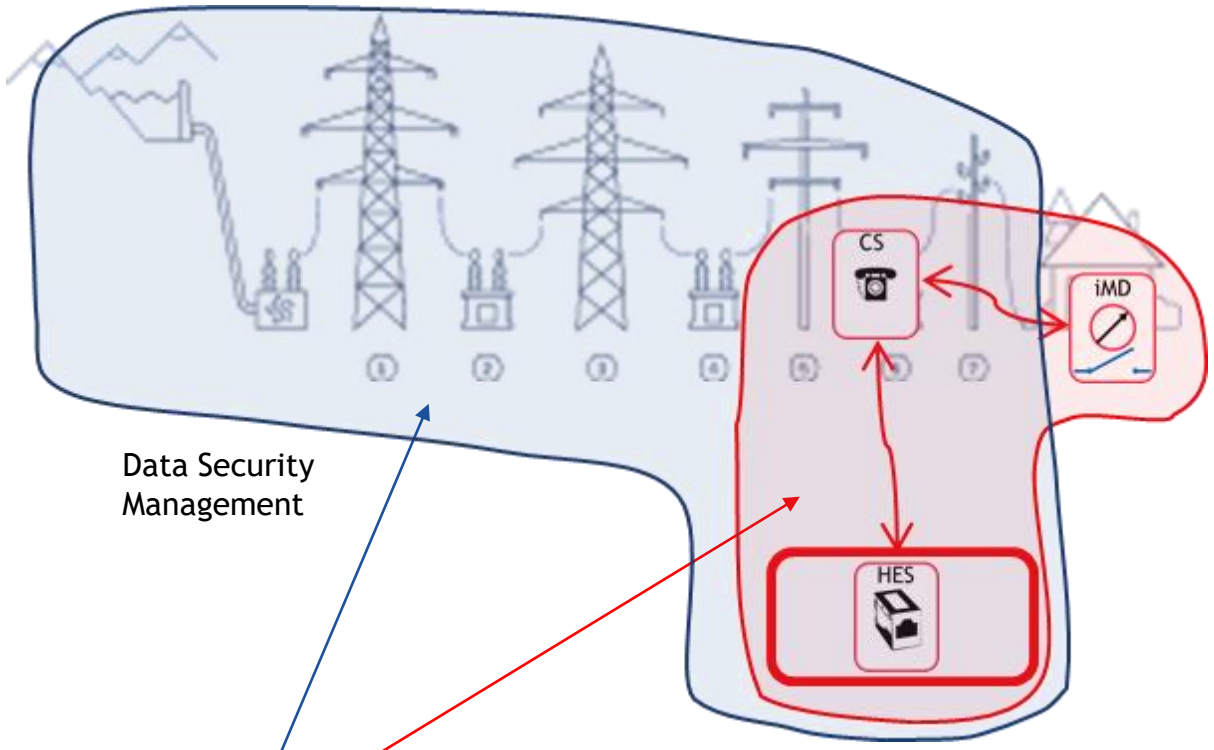
We don‘t want: 

We do want: Trustworthy Data Security

- Certified Components
- Data Security management for DSO

Switzerland:

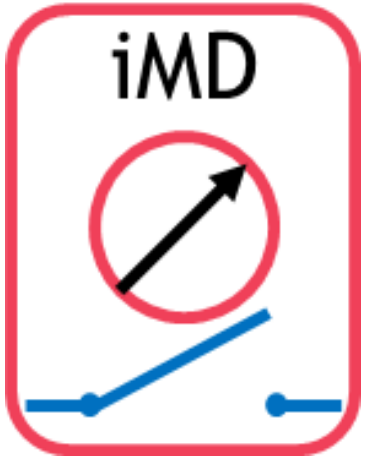
- Agency for Energy **BfE/FOE**
  - Security Requirements Analysis (SBA)
  - legislative ordinance (StromVV)
- Operators’ association **VSE**
  - requirements and guidelines (Editor)
- Manufacturers’ association **Swissmig**
  - input to VSE requirements
  - Testing Methodology (Editor)
- **METAS**
  - Data Security Certification Body
- **Test Labs**
  - Data Security Evaluation Labs



* «slightly» means that the iMD is a publicly accessible entry point into a Critical Infrastructure

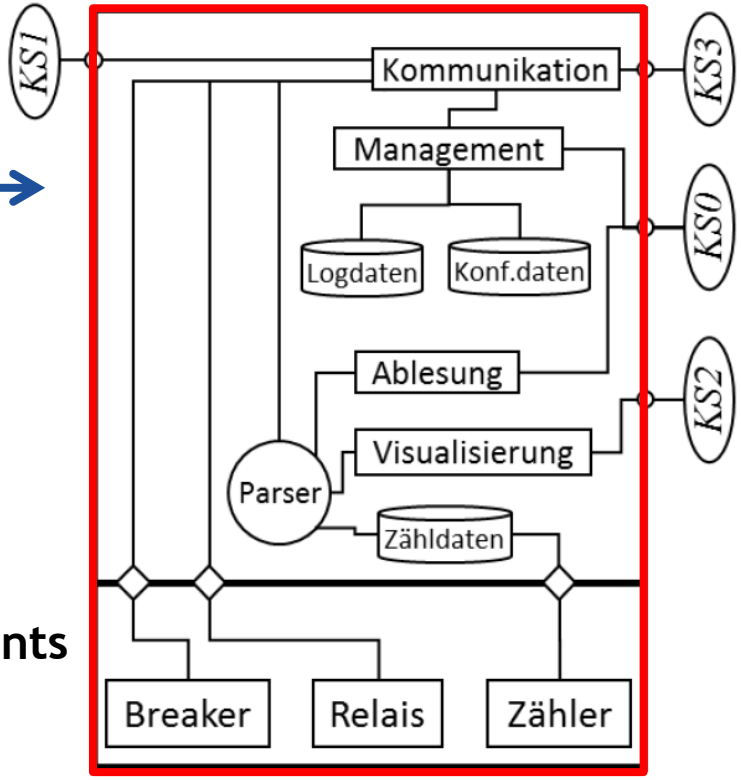
Derivation for the intelligent Measurement Device

(accordingly for DC and HES)



Definition of a Generic Model for iMD that:

- fits to all products
- no-one built like this before
- no-one will build alike in the future
- serves to derive **real Data Security Requirements**
- specifies **Assets** (i.e. Objects to-be-protected)
- serves to define **Threats** (i.e. Feared Events)



Swiss Data Security Certification Scheme

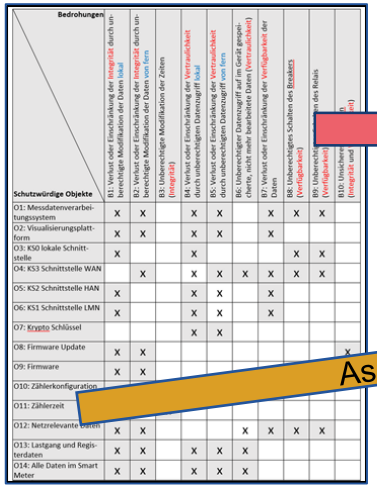
(on the edge of a nutshell)

1. There are Legal Requirements: Definition of **roles and rules**
2. There is a Swiss Protection Requirement Analysis yielding:
   - **risk scenarios** for processes
     and with some effort
   - a generic **Matrix of Objects and Threats** for components
3. A list of **real** Data Security Requirements derived from a **generic** Model.

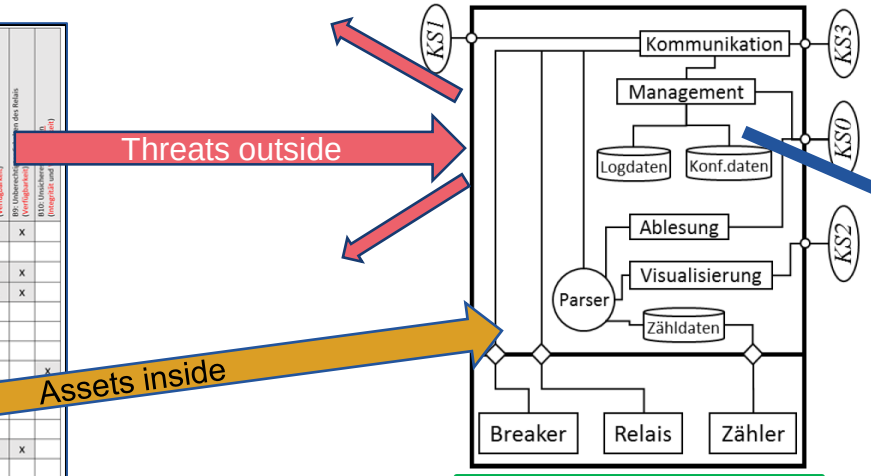
4. A **device-specific** Object-Threat-Matrix:
   - Data Security Fingerprint of a device
   - yielding Data Security Objectives for protective functionalities
5. A **device-specific** Test List:
   - The filled-in information explains, which functionality serves which requirement.

6. The **Test Lab** evaluates, whether the device fulfills the requirements correctly and effectively.
7. The **Certification Body** assesses the correctness of the Testing and certifies the devices.

Fusion of Assets, Protection and Specification



The OT Matrix is the Data Security Fingerprint of a Device



GENERIC IT Architecture of a Device (iMD)

The device is a "resilient" Data Security Domain
- Assets are stored and processed inside.
- Functional or Architectural Modules render security relevant functionalities.
- Assets are transmitted via secure interfaces.
- All external interfaces
  - do also render security relevant functionalities.
  - are "well defined" and hardened against unauthorised access.

GENERIC Requirements
- WHAT is required

Anforderung	Beschreibung der Umsetzung durch Hersteller		Prüfergebnis	
WAS (zu erfüllen)	WIE (funktional/prozedural)	WO (architektonisch)	Anforderung erfüllt j/n	Bemerkung
5.1.2 Zugriffskontrolle				
a) An denjenigen Schnittstellen der Hauptkomponenten mit Benutzerzugriff, sind bezüglich der schützenswerten Objekte die jeweiligen Zugriffsrechte für alle Rollen definiert.				
b) Das anzuwendende Rollenmodell ist vom Hersteller zu definieren.				
c) Das Rollenmodell ist durch autorisierte Benutzer erweiterbar.				

SPECIFIC Implementation
- functional (HOW)
- architectural (WHERE)

This table is only an example for a Test List Module!

Outlook

1. Risk Assessment for Components

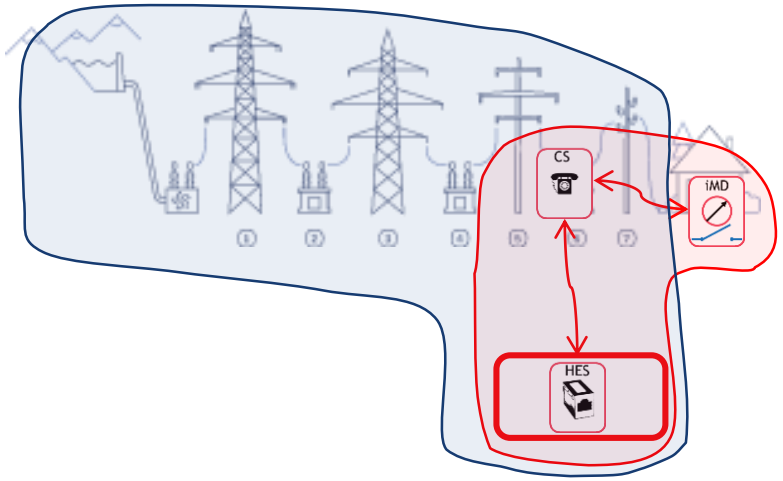
   How should a risk resulting from a component be assessed, if there is no baseline data security scenario?

2. Component Resilience

   With a metrics for resilience based on generic requirements, the entry probability of risk drops considerably.

3. Generic Requirements for real components

   It seems to be «an issue» to abstract from standardised functionalties to standardised requirements.


CS
iMD
HES


HES
CS
iMD