IoTSec - WP3 work meeting, Kjeller

Multi-Metrics Analysis for Measurable Security

György Kálmán,
Mnemonic/CCIS/UNIK
gyorgy@unik.no

Seraj Fayyad
Movation/UNIK
seraj@unik.no

Josef Noll
UiO/UNIK
josef@unik.no

Overview

- Use case (application) Smart Grid
- Values for Security, Privacy
- Analyse the system of systems
- Identify Security, Privacy attributes and functionality for a sub-system
- Multi-Metrics analysis
- Future work

Multi-Metrics Methodology for Assessment of Security, Privacy, and Dependability (SPD)

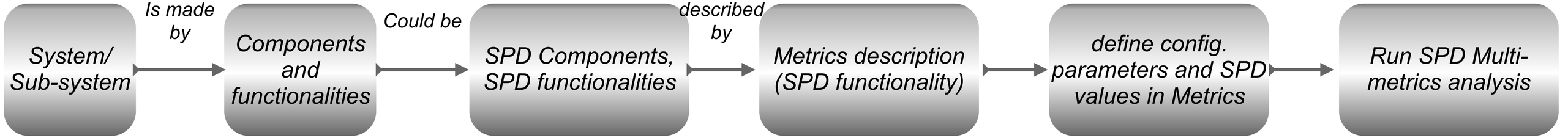
Thanks to our colleagues from SHIELD for the collaboration

» Iñaki Equia, Frode van der Laak, Seraj Fayyad, Cecilia Coveri, Konstantinos Fysarakis, George Hatzivasilis, Balázs Berkes, Josef Noll

Feb2015

ARTEMIS

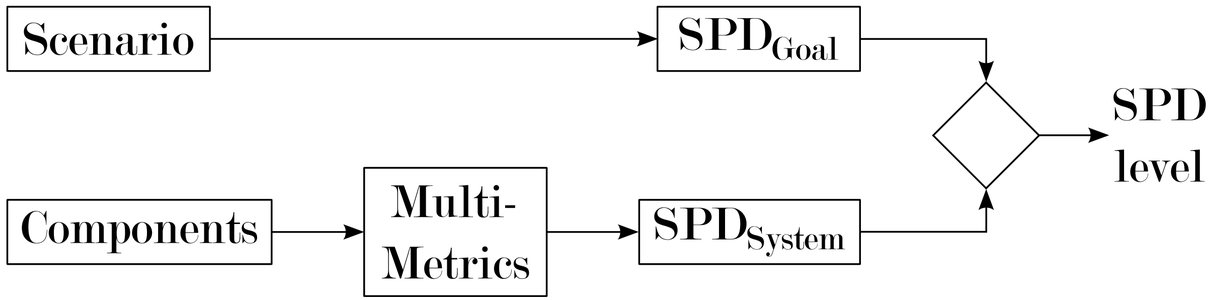
Methodology:
From System description to SPD level



- System: Automatic Meter System (AMS) consists of reader (AMR), aggregator, communications, storage, user access
- Sub-systems: AMR consists of power monitor, processing unit, communication unit
- Component: AMR communication contains of a baseband processing, antenna, wireless link
- Configuration Parameter: Wireless link: f=868 MHz, output power=?, Encryption=?

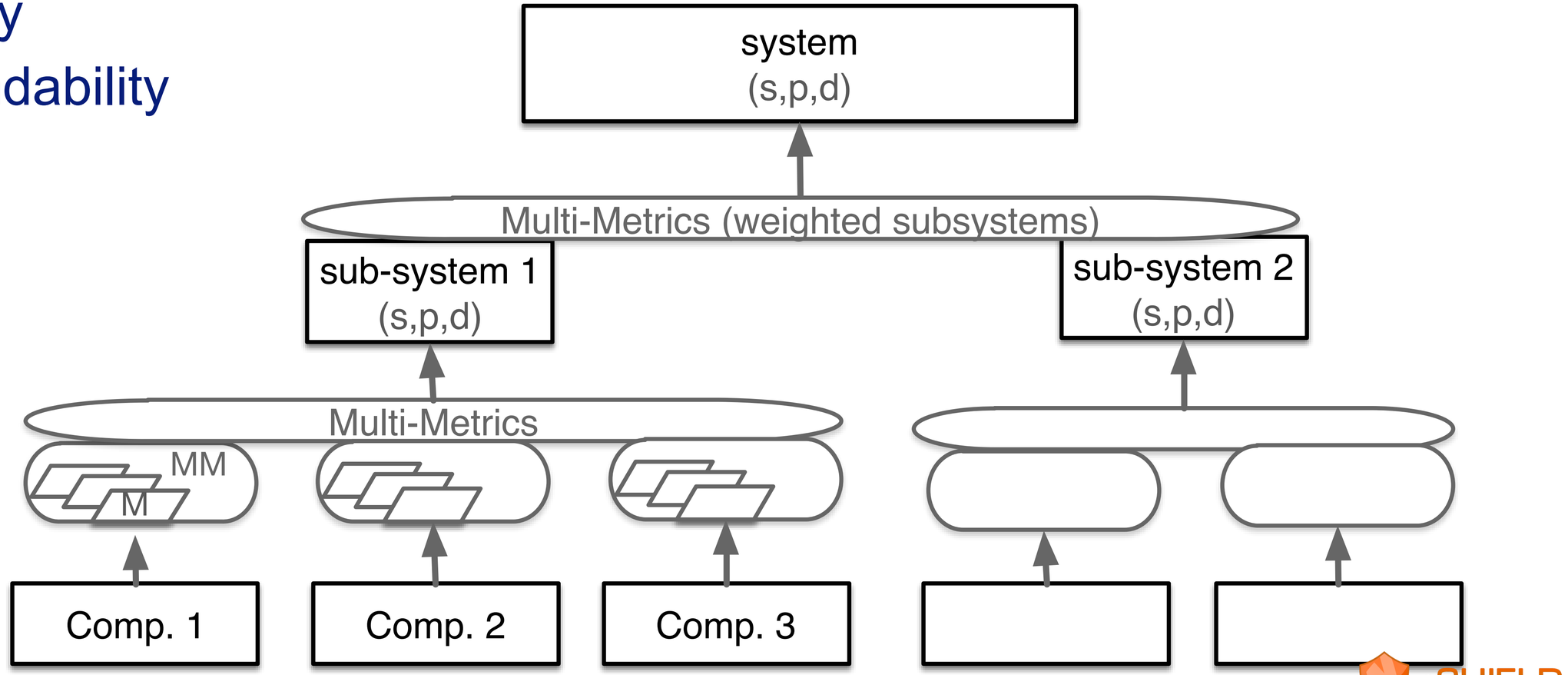
Smart Grid Main Focus

- Focus on «entry the industrial market»
- Identified challenges
  - ➡ industry «needs security» - with entry models
  - ➡ Communication module
  - ➡ Role-based access
  - ➡ Middelware (Multi Metrics v2)
- System Security, Privacy and Dependability is assessed
- $System_{SPD}$ is compared to $Goals_{SPD}$



Multi-Metrics$_{v2}$ - system composition

- System consists of sub-systems consists of components
  - ➡ security
  - ➡ privacy
  - ➡ dependability

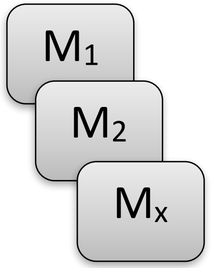


SHIELD Multi Metrics Approach

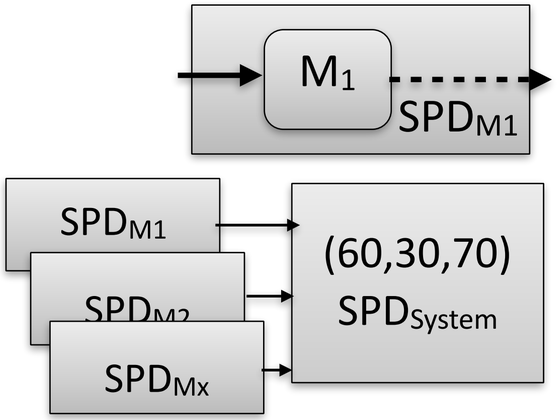
- Security, Privacy and Dependability
  - » Specific application
  - » Social Mobility: privacy scenario

		SPD_{Goal}	SPD level	
Scenario 1	**Conf. A**	(s,80,d)	(s,100,d)	(s,🟡,d)
	Conf. B		(s,80,d)	(s,🟢,d)
	Conf. C		(s,80,d)	(s,🟢,d)

- Multi-Metrics approach to assess the SPD of a system
  - » Provides a snapshot of the current state of the system
  - » Metrics for SPD parameters of sensors, network, service access
  - » Metrics M_1 … M_x, e.g. Network latency, Protection level



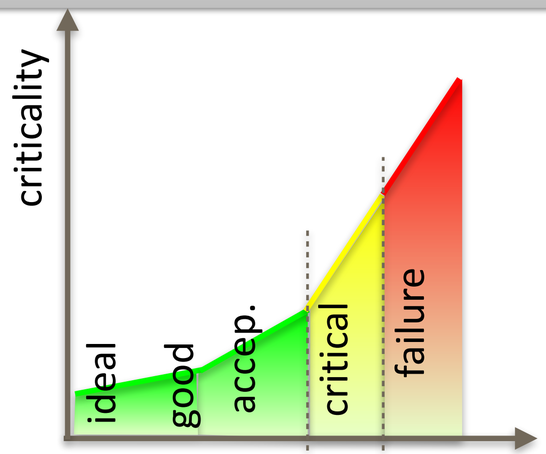
- Individual Metrics scaling $SPD_{M1}(20,5,10)$
  - » Parametrisation of assessment, e.g. latency = 50 ms -> S:acceptable
  - » Subjective translation into SPD severity
    - » Operational ranges defined as ideal, good, acceptable, critical, failure
    - » Max influence on the S,P,D value (estimate)

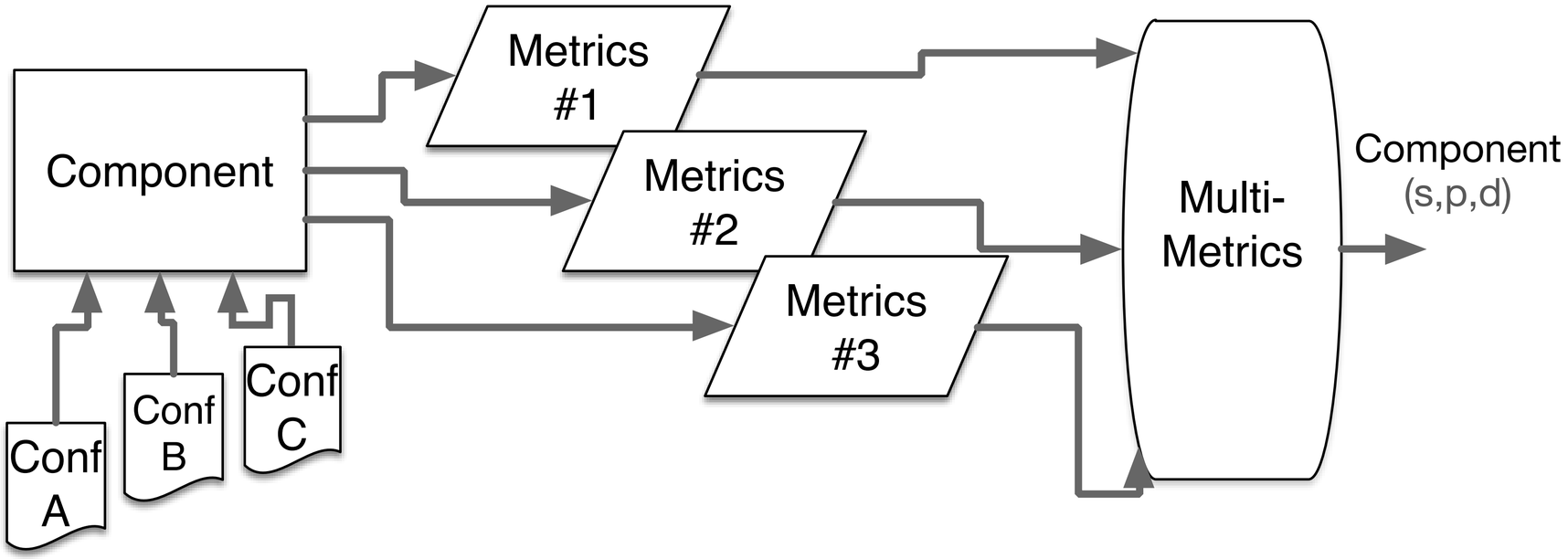


- Metrics combination to provide an SPD tripple: (60, 30, 70)

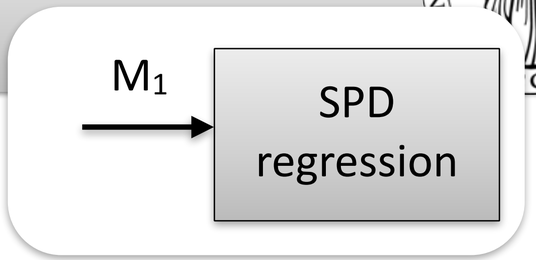
Multi-Metrics components

- Components have a security, privacy and dependability factor.
- Metrics assess the components

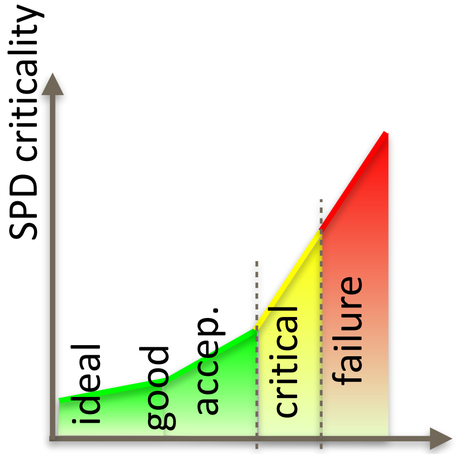




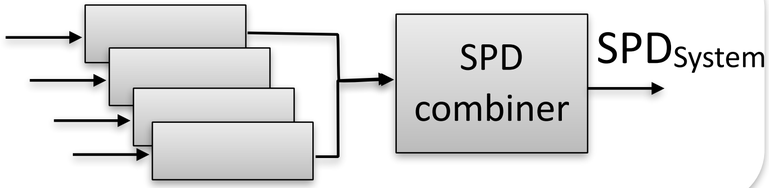
SHIELD Multi Metrics$_{v2}$



- Metrics to SPD conversion
  - » Parametrisation of system parameters, e.g. latency -> [ms]
  - » SPD regression: «SPD value and importance for the system»
    - » parameter into S,P,D value range, e.g. latency=50ms :=> (ideal, good, acceptable, critical, failure)
    - » Scaling according to System Importance, e.g. latency :=> S_{max}=30, P_{max}=10, D_{max}=20
    - » Assignment of SPD values, e.g. latency=50 ms

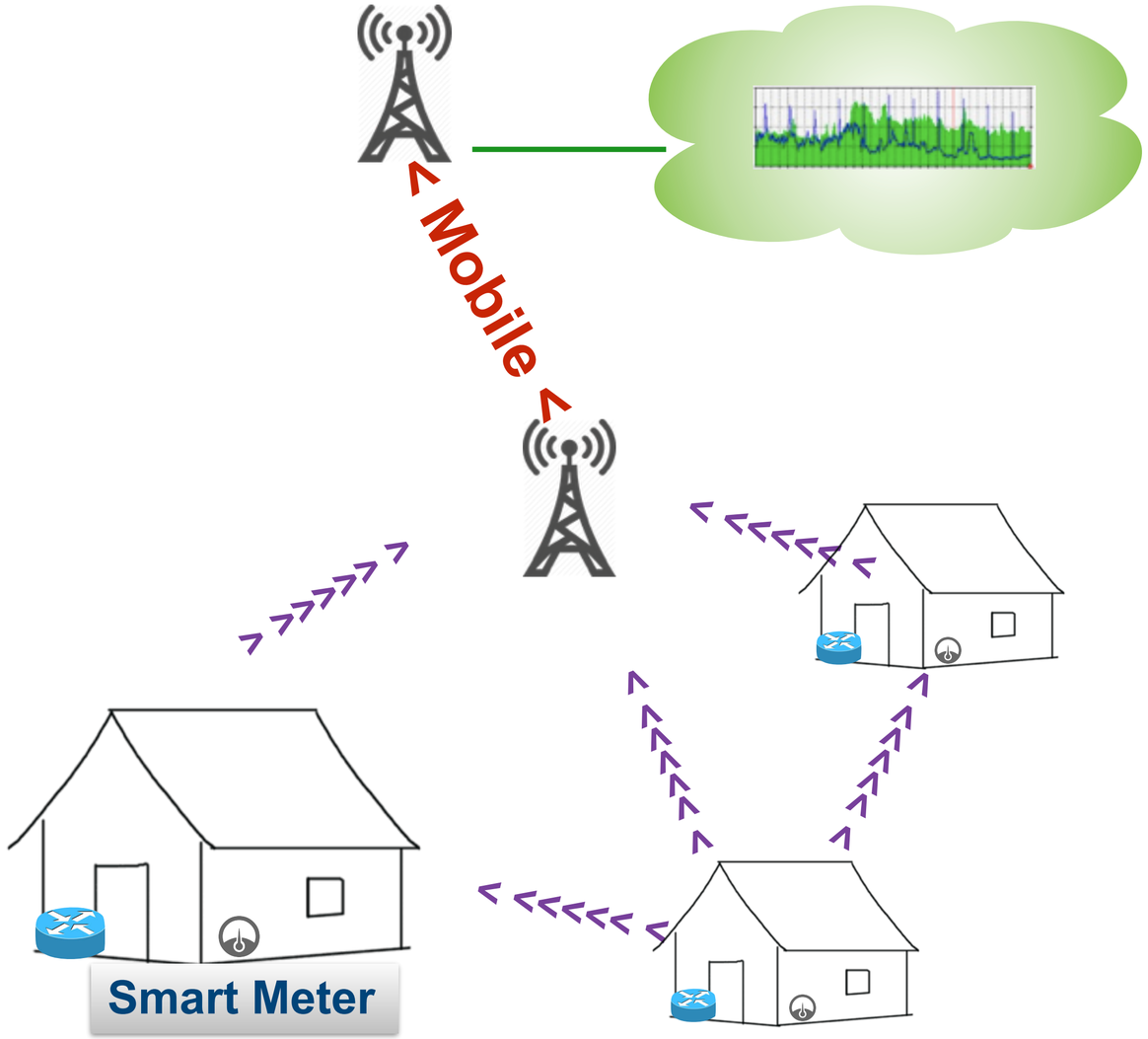


- Metrics combination to provide SPD$_{System}$: (60, 30, 70)
  - » Mathematical combination, e.g. S_{System}=100 - SQRT(S_1^2+S_2^2+…S_x^2)



Current Infrastructure

- Smart Meter (customer home)
  - ➡ connected via mesh or directly
  - ➡ proprietary solution (433, 800 MHz band, power line)
- Collector
  - ➡ collects measures
  - ➡ communicates via mobile network
- Mobile Network
  - ➡ as a transmission network
- Cloud (Provider)
  - ➡ entry point for remote access
  - ➡ Application platform



Future Smart Grid operation, § 4-2 functional requirements

"Forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv."

1. Store measured values, registration frequency max 60 min, can configure to min 15 min.
2. Standardised interface (API) for communication with external equipment using open standards
3. Can connect to and communicate with other type of measurement units
4. Ensures that stored data are not lost in case of power failure
5. Can stop and reduce power consumption in every measurement point (exception transformator)
6. Can send and receive information on electricity prices and tariffs. Can transmit steering information and ground faults
7. Can provide security against miss-use of data and non-wished access to control-functions
8. Register flow of active and re-active power flow in both directions

§ 4-2. *Funksjonskrav*

AMS skal:

a) lagre måleverdier med en registreringsfrekvens på maksimalt 60 minutter, og kunne stilles om til en registreringsfrekvens på minimum 15 minutter,

b) ha et standardisert grensesnitt som legger til rette for kommunikasjon med eksternt utstyr basert på åpne standarder,

c) kunne tilknyttes og kommunisere med andre typer målere,

d) sikre at lagrede data ikke går tapt ved spenningsavbrudd,

e) kunne bryte og begrense effektuttaket i det enkelte målepunkt, unntatt trafomålte anlegg,

f) kunne sende og motta informasjon om kraftpriser og tariffer samt kunne overføre styrings- og jordfeilsignal,

g) gi sikkerhet mot misbruk av data og uønsket tilgang til styrefunksjoner og

h) registrere flyt av aktiv og reaktiv effekt i begge retninger.

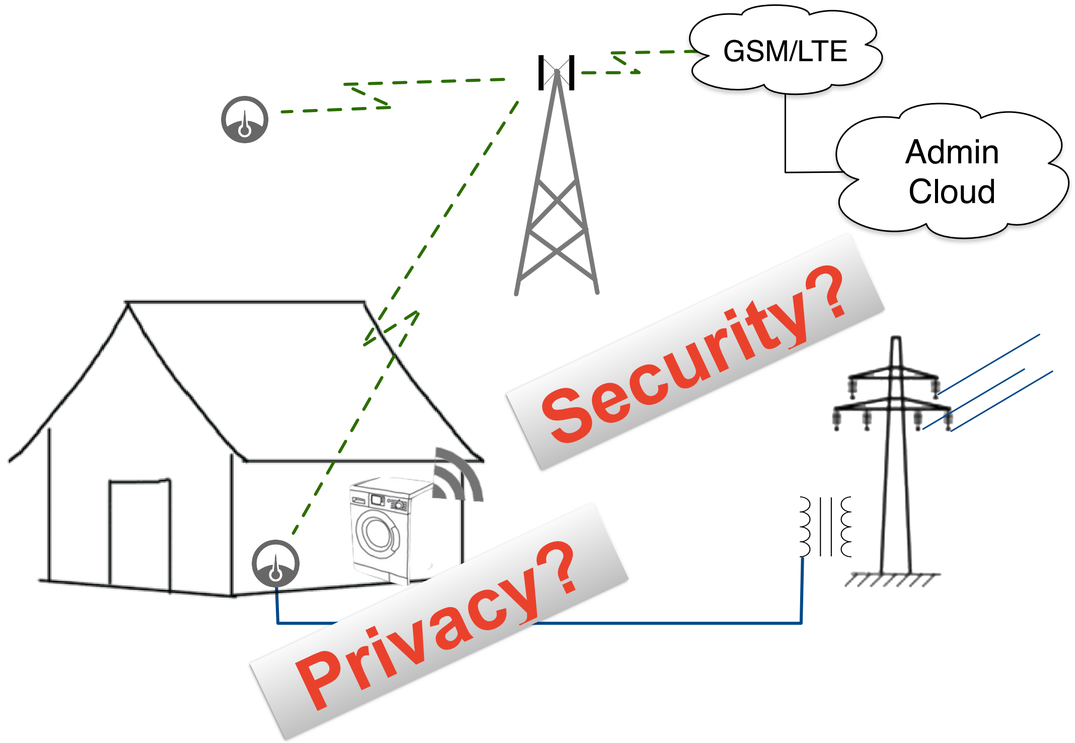
Norges vassdrags- og energidirektorat kan etter søknad i særlige tilfeller gi dispensasjon fra enkelte funksjonskrav.

0 Tilføyd ved forskrift 16 jan 2012 nr. 75 (i kraft 20 jan 2012).

https://lovdata.no/dokument/SF/forskrift/1999-03-11-301

Ecosystem - Application Scenarios for Smart Meters

- Monitoring the grid to achieve a grid stability of at least 99,96%,
- Alarm functionality, addressing
  - ➡ failure of components in the grid,
  - ➡ alarms related to the Smart Home, e.g. burglary, fire, or water leakage,
- Intrusion detection, monitoring both hacking attempts to the home as well as the control center and any entity in between,
- Billing functionality, providing at least the total consumption every hour, or even providing information such as max usage,
- Remote home control, interacting with e.g. the heating system
- Fault tolerance and failure recovery, providing a quick recovery from a failure.
  - Future services
  - ➡ Monitoring of activity at home, e.g. “virtual fall sensor”



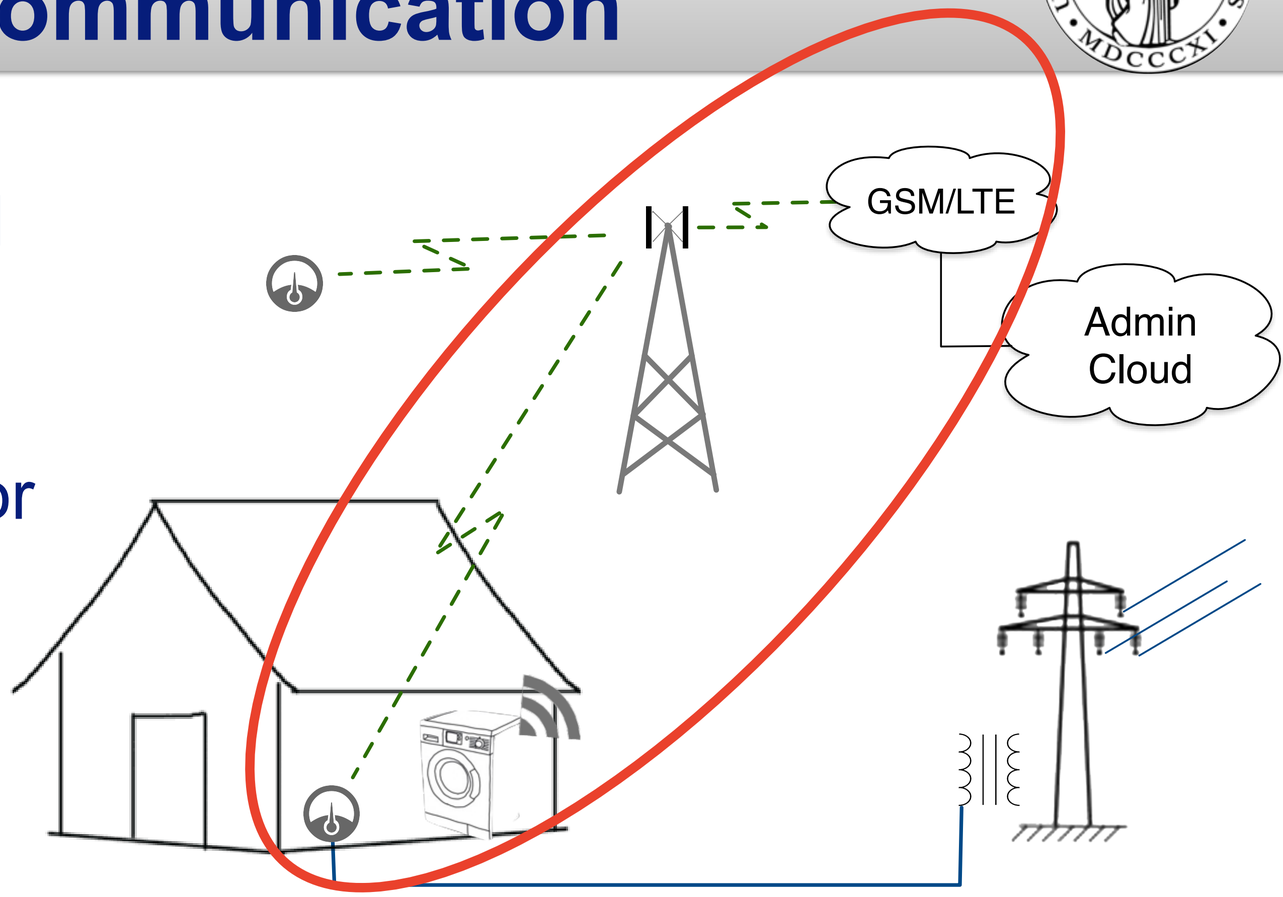
Action:
Establish Application Goals for Security & Privacy

- Discuss with your neighbours the security and privacy goal for :
- Billing (1/hour)
  - ➡ Security, Privacy Goal: (s,p) - Range [0…100]
- Fire alarm
  - ➡ Security, Privacy Goal: (s,p) - Range [0…100]
- Home Control (1/hour)
  - ➡ Security, Privacy Goal: (s,p) - Range [0…100]

Goal:
"basis of discussion"
- why?

Sub-system analysis
Here: Smart Meter with Communication

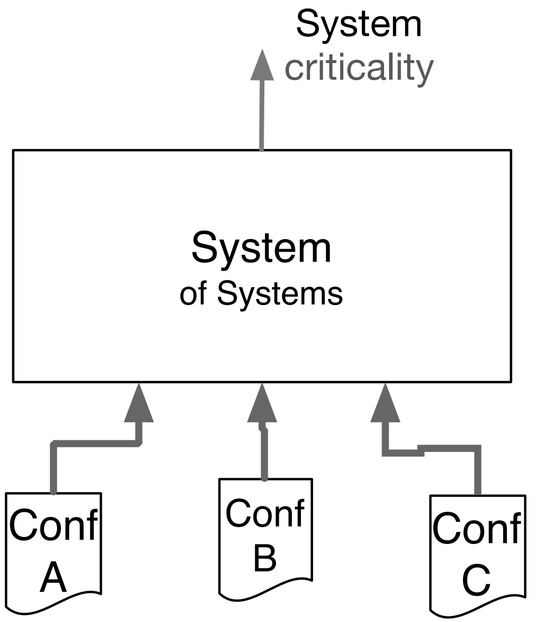
- the Automatic Meter Reader (AMR)
  - AMR to measure, sense and control power consumption
- the Mesh radio link
  - direct communication to concentrator
  - or multi-hop through other AMR
- the Mobile link sub-systems
  - from collector to mobile operator
  - typical 2G/3G/4G data, or SMS

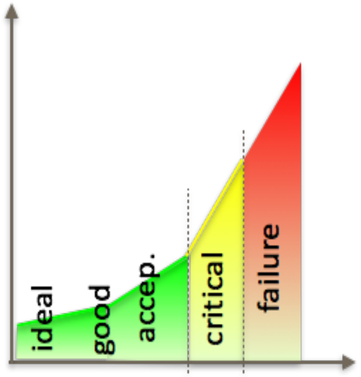


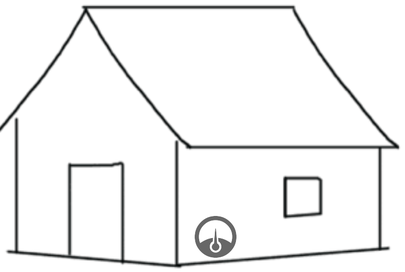
Sub-system analysis
Metrics for AMR

- the Automatic Meter Reader (AMR)
  - (1) remote access metric - (yes/no)
    - reading, or just controlling
  - (2) authentication metric
    - everyone, or authenticated user
  - (3) encryption metric (on, off)

$$(Cs, Cp, Cd) = (100, 100, 100) - (s, p, d).$$







(1) remote access

Configuration	Cs	Cp
Remote Access ON	60	60
Remote Access OFF	10	20

(2) authentication

Configuration	Cs	Cp
Authentication ON	10	30
Authentication OFF	80	70

(3) encryption

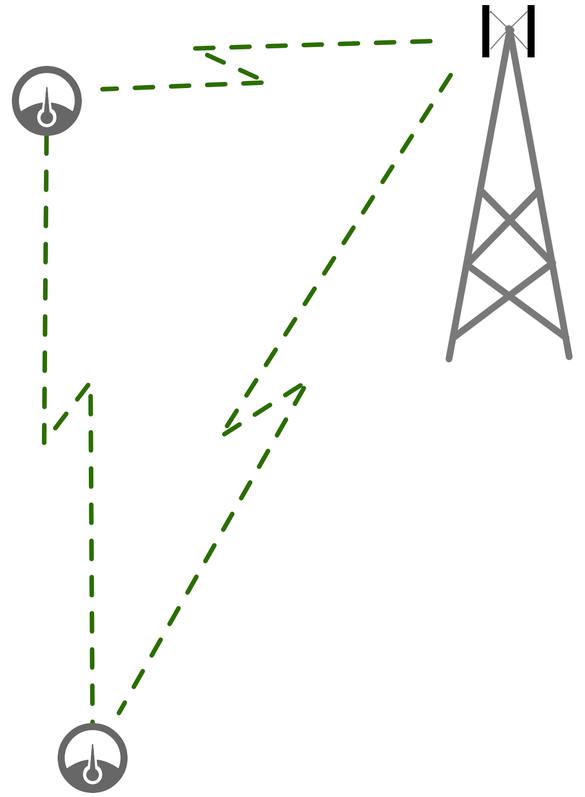
Configuration	Cs	Cp
Encryption ON	10	10
Encryption OFF	80	80

Sub-system analysis
Metrics for Mesh Radio

- the Mesh radio link
  - (4) mesh
  - (5) message rate
  - (3) encryption

(4) mesh

Configuration	Cs	Cp
Multi-path routing	60	60
Single-path routing	30	30



(3) encryption

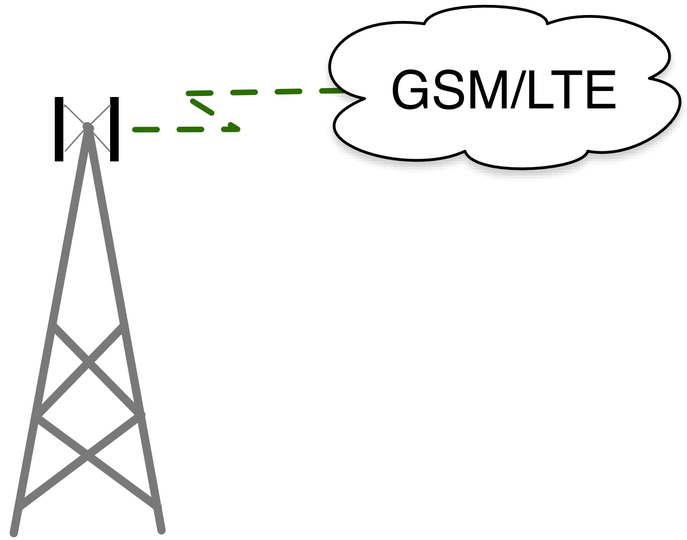
Configuration	Cs	Cp
Encryption ON	10	10
Encryption OFF	80	80

(5) message rate

Configuration	Cs	Cp
1 hour	20	20
20 min	25	30
1 min	40	50
5 sec	50	70

Sub-system analysis
Metrics for mobile link sub-system

- the Mobile link sub-systems
  - (6) mobile channel (2G or SMS)
  - (6+) 3G/4G, IP, powerline
  - (3) encryption



(3) encryption

Configuration	Cs	Cp
Encryption ON	10	10
Encryption OFF	80	80

(6) mobile channel

Configuration	Cs	Cp
GPRS	60	70
SMS	40	50

AMR sub-system analysis
Summary of Metrics for functionality

- the Automatic Meter Reader (AMR)
  - (1) remote access metric
  - (2) authentication metric
  - (3) encryption metric
- the Mesh radio link
  - (4) mesh
  - (5) message rate
  - (3) encryption
- the Mobile link sub-systems
  - (6) mobile channel (2G or SMS)
  - (3) encryption

(1)

Configuration	Cs	Cp
Remote Access ON	60	60
Remote Access OFF	10	20

(3)

Configuration	Cs	Cp
Encryption ON	10	10
Encryption OFF	80	80

(2)

Configuration	Cs	Cp
Authentication ON	10	30
Authentication OFF	80	70

(4)

Configuration	Cs	Cp
Multi-path routing	60	60
Single-path routing	30	30

(5)

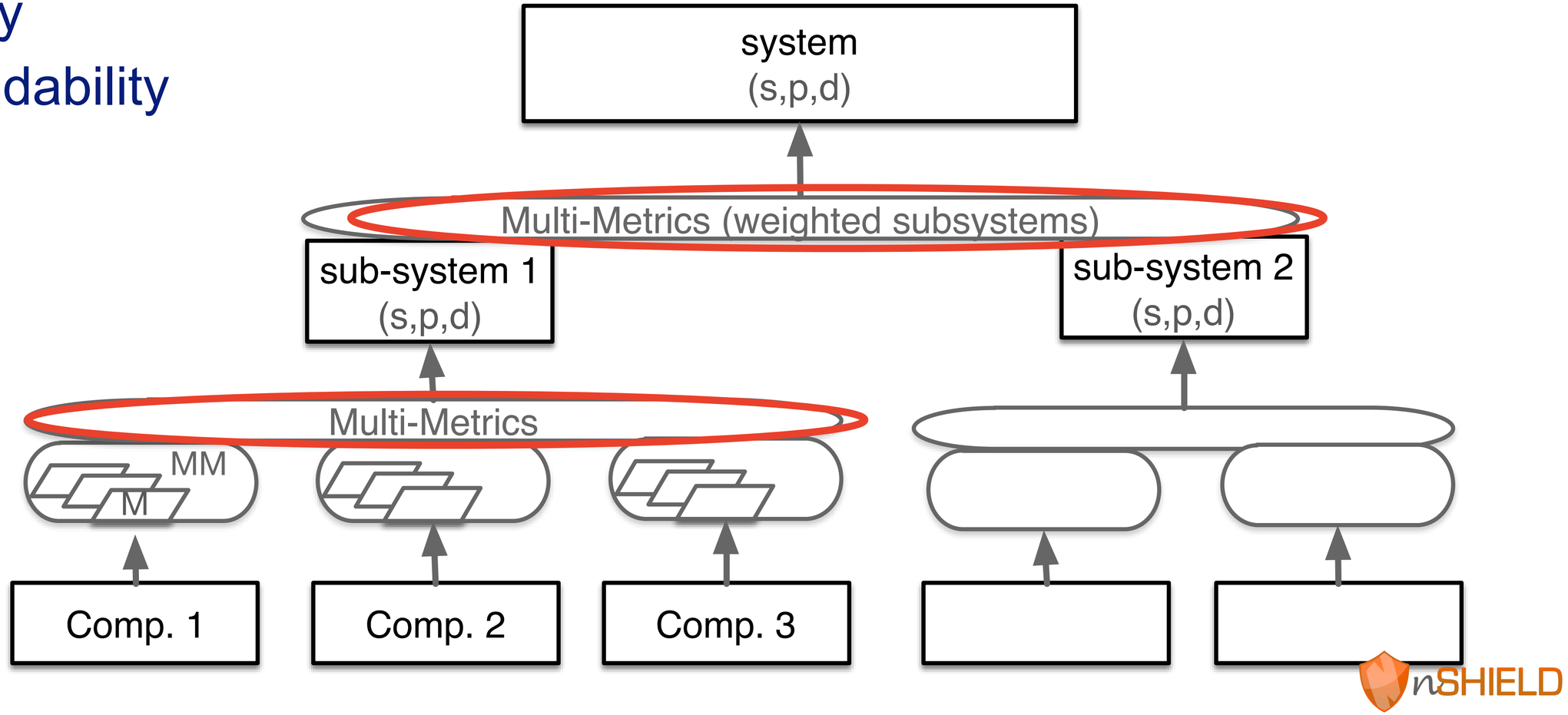
Configuration	Cs	Cp
1 hour	20	20
20 min	25	30
1 min	40	50
5 sec	50	70

(6)

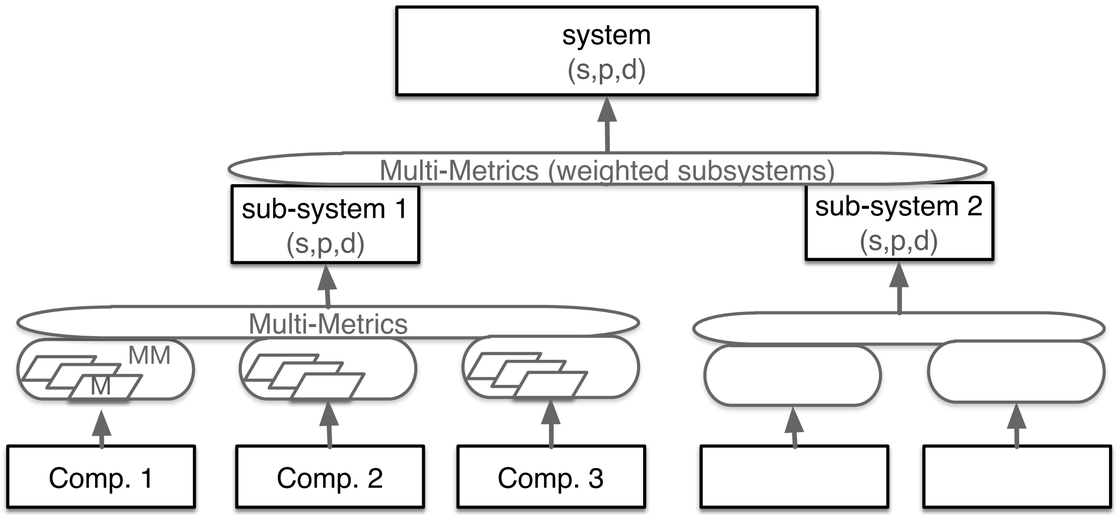
Configuration	Cs	Cp
GPRS	60	70
SMS	40	50

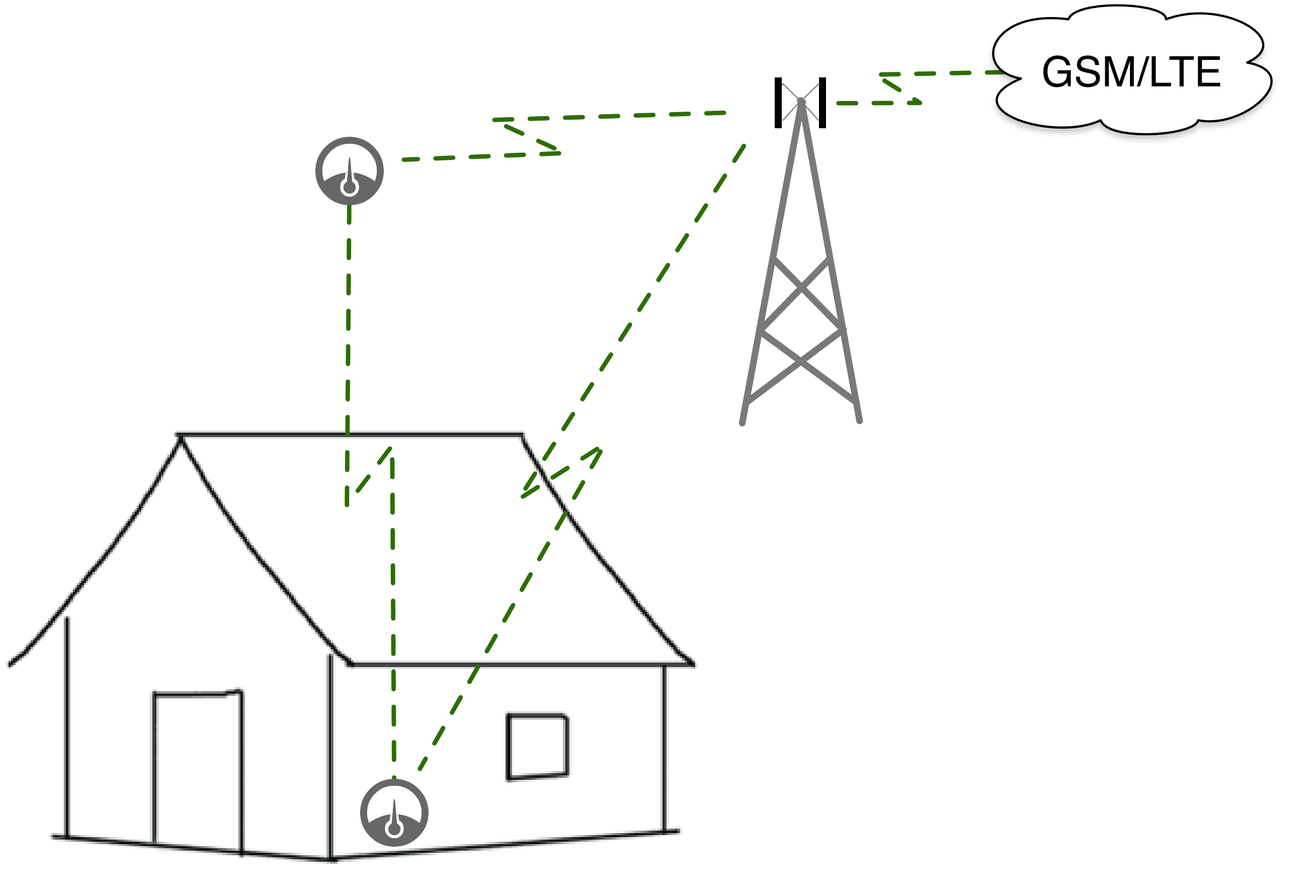
Multi-Metrics$_{v2}$ - system composition

- System consists of sub-systems consists of components
  - ➡ security
  - ➡ privacy
  - ➡ dependability



Why weighting of sub-systems?





Sub-system weighting

- Component criticality from metrics
- sub-system criticality from evaluation of components
- system criticality from evaluation of sub-systems
- Criticality *C* through root mean square weight
- Actual criticality x_i for component or (sub-)system
- Weight w_i for each metric,
- Result will maximise the impact of high criticalities

$$C = \sqrt{\sum_i \left(\frac{x_i^2 W_i}{\sum_i^n W_i} \right)} \qquad W_i = \left(\frac{w_i}{100} \right)^2$$

Table 8 Sub-systems and components weights

Sub-system	Sub-sys. Weight	Component	Comp. Weight
AMS	80	Remote Access	70
		Authentication	80
		Encryption	80
Radio link	50	Mesh	60
		Message Rate	80
		Encryption	40
Mobile link	20	Mobile link	70
		Encryption	40

s,p-goal versus system-s,p

- 11 possible configurations
  - selected as combinations of “states”
- highest SPD element dominates the outcome of the metrics
  - Billing & Home Control: security
  - Alarm: dependability
- Sensitivity Analysis:
  - max security: s=84
  - same config: p=77
  - satisfies billing (🟢,🟢,🟢)
  - satisfies home control (🟢,🟢,🟡)

Table 1 SPD_{Goal} of ea

Use Case	Security	Privacy
Billing	90	80
Home Control	90	80
Alarm	60	40

Table 9 Selected configuration SPD level for each use case

Use case	SPD_{Goal}	Configuration	SPD level	SPD vs SPD_{Goal}
Billing	(90,80,40)	10	(67,61,47)	(🔴,🟡,🟢)
Home Control	(90,80,60)	10	(67,61,47)	(🔴,🟡,🟡)
Alarm	(60,40,80)	6	(31,33,63)	(🔴,🟡,🟡)

Conclusions

- Security and Privacy methodology applied for Smart Grid
- Sub-system Meter Reader, Mesh communication, Mobile Communication assessed
- Weighting, see example
- 11 configurations assessed, best result providing (s,p,d) = (84,77,42)
- Challenges
  - ➡ Logic: Centralised <—-> Fog
  - ➡ Smart Meter: Information <—> Control
  - ➡ Smart Grid Information <—> Internet Info

Table 8 Sub-systems and components weights

Sub-system	Sub-sys. Weight	Component	Comp. Weight
AMS	80	Remote Access	70
		Authentication	80
		Encryption	80
Radio link	50	Mesh	60
		Message Rate	80
		Encryption	40
Mobile link	20	Mobile link	70
		Encryption	40