UNIK4750 - Measurable Security for the Internet of Things

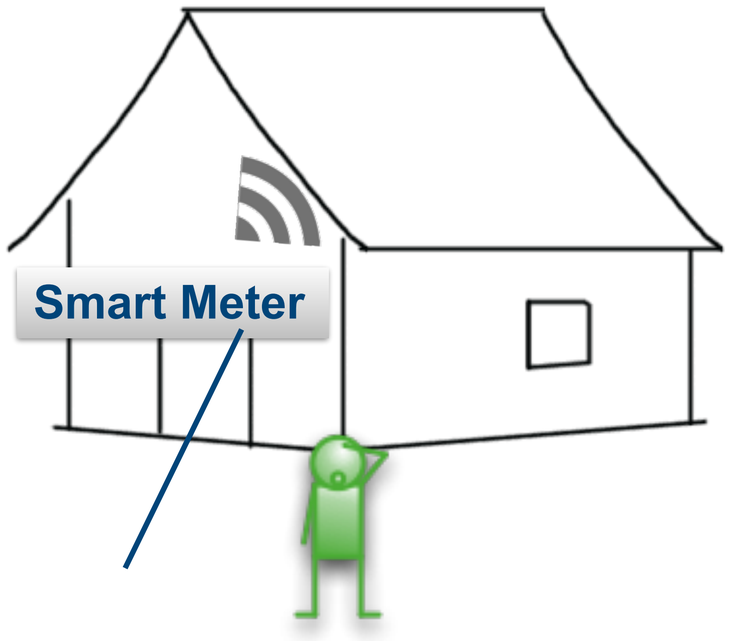
L11 - Multi-Metrics Weighting of an AMR sub-system

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

Josef Noll
UiO/UNIK
josef@unik.no

Overview

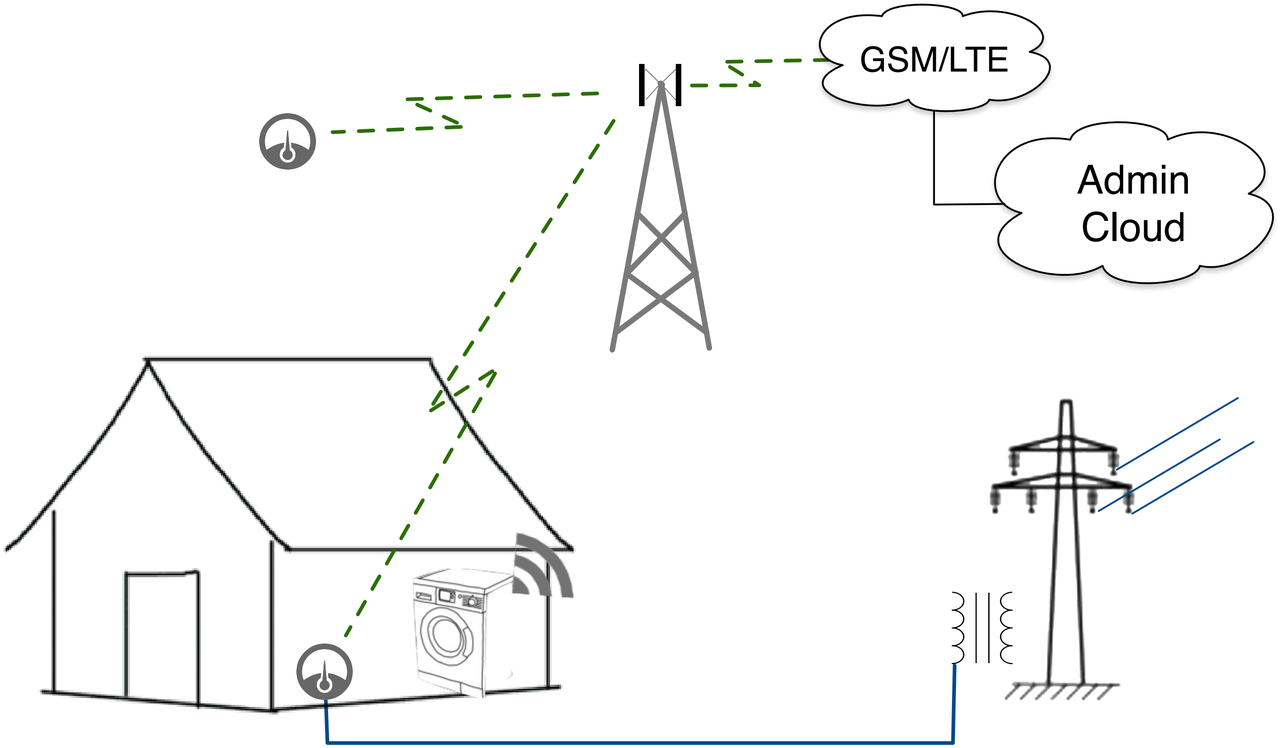
- Learning outcomes L11
- Use case (application) Automatic Meter Reader (AMR)
- Identification of sub-system
- Metrics for the s,p-functionality
- Values for Security, Privacy
- weighting of components
- Multi-Metrics analysis
- Evaluation of results
- Future work



Expected Learning outcomes

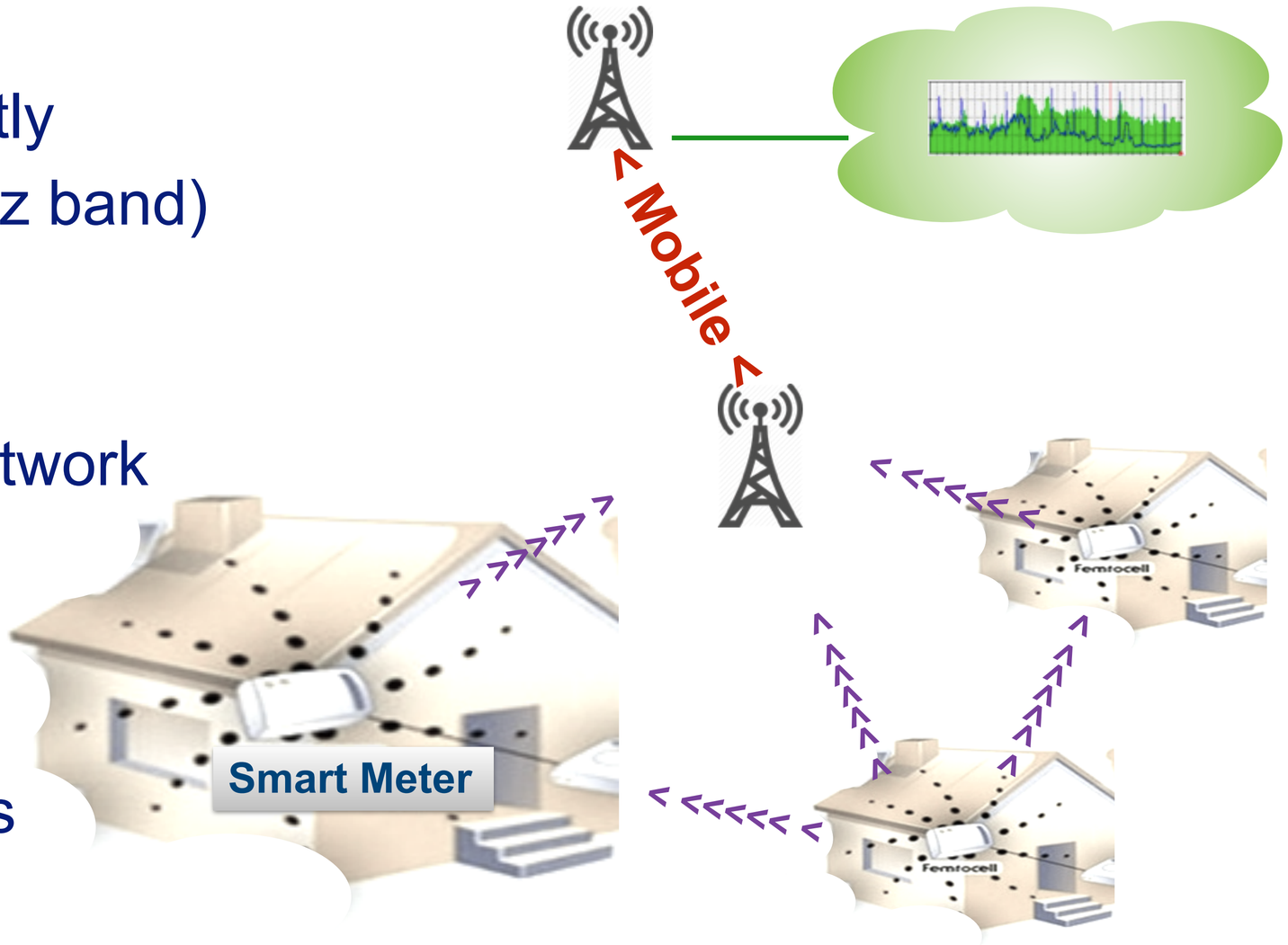
Having followed the lecture, you can

- subdivide a system into sub-systems and components
- identify s,p,d-functionalities
- reason over (discuss) the weighting of components with respect to total security
- apply the Multi-Metrics method
- provide meaning for s,p-results



Current Infrastructure

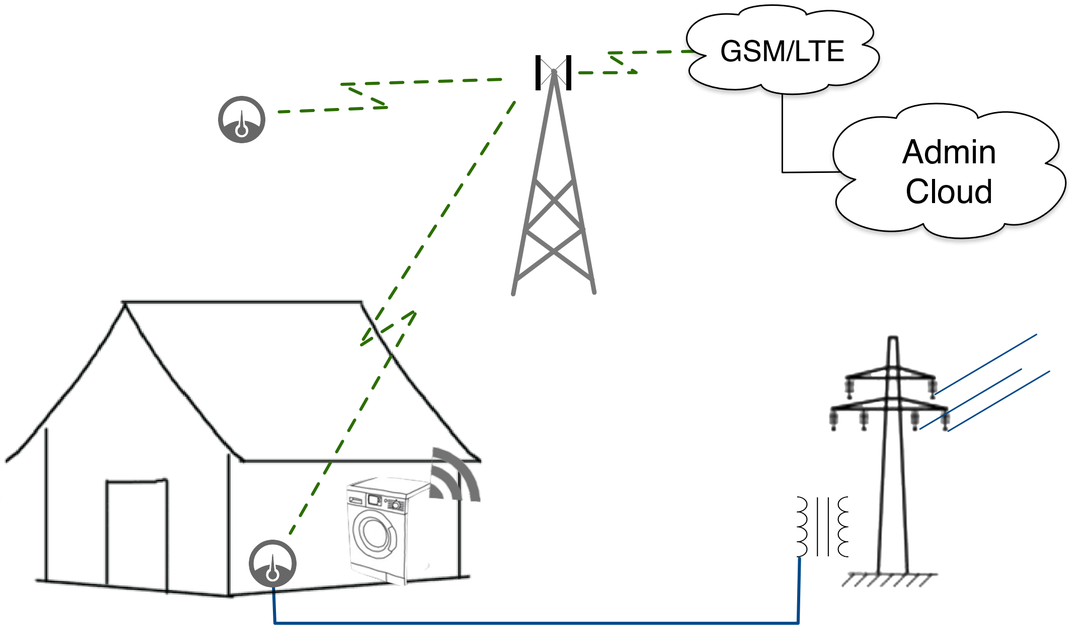
- Smart Meter (customer home)
  - ➡ connected via mesh or directly
  - ➡ proprietary solution (800 MHz band)
- Collector
  - ➡ collects measures
  - ➡ communicates via mobile network
- Mobile Network
  - ➡ as a transmission network
- Cloud (Provider)
  - ➡ entry point for remote access
  - ➡ Application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



[source: seminarsonly.com]

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”

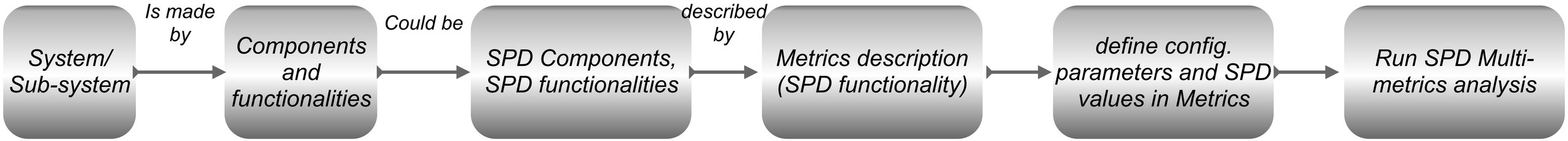


Action:
Establish Application Goals for Security & Privacy

- 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?

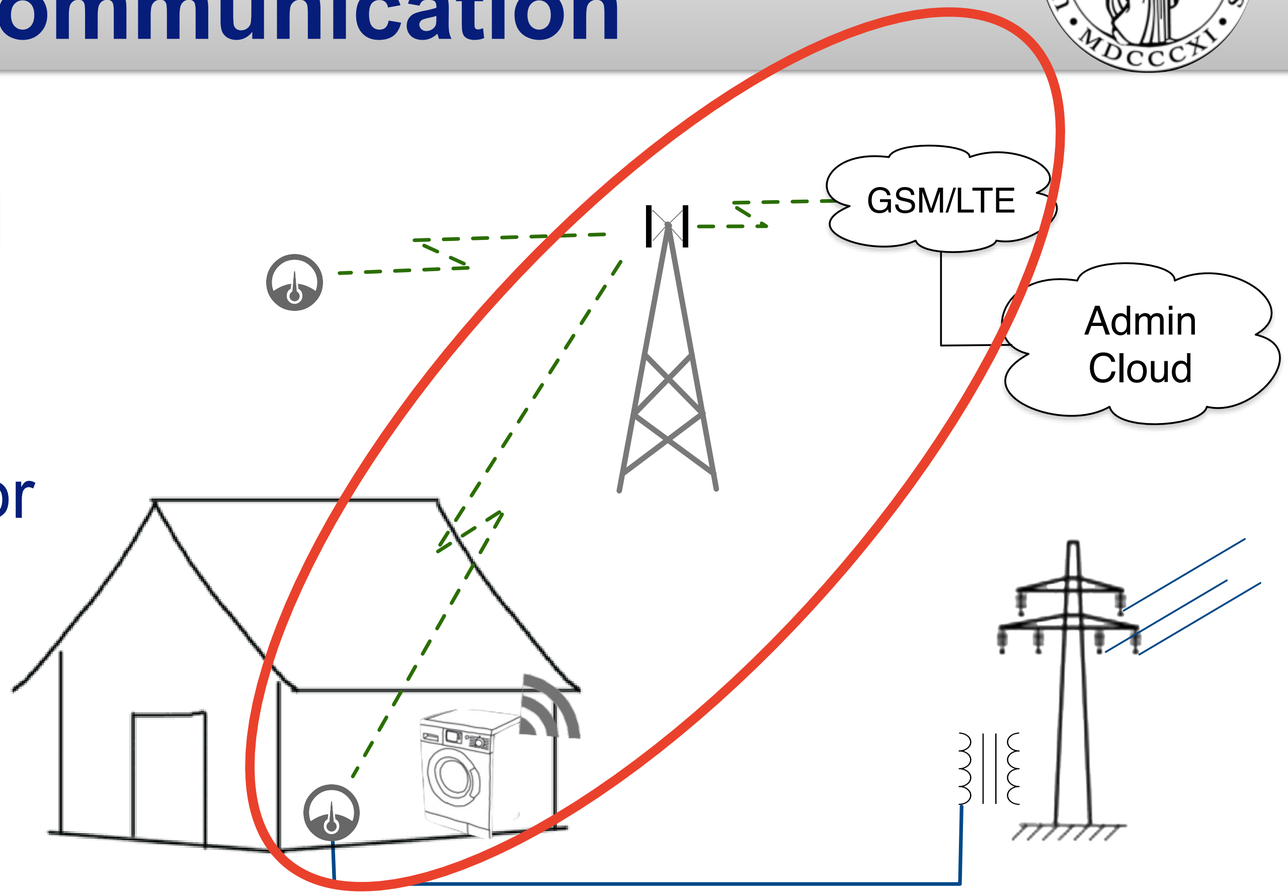
Methodology and AMR system: From System description to SPD level



- 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=?

Sub-system analysis
Here: Smart Meter with Communication

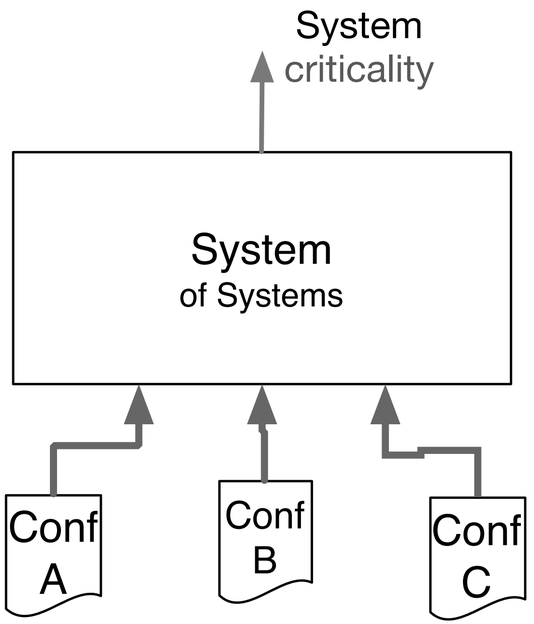
- the Automatic Meter Reader (AMR)
  - AMR to measure, sense and control power consumption
- the Mesh radio link
  - direct communication to concentrator
  - or multi-hop through other AMR
- the Mobile link sub-systems
  - from collector to mobile operator
  - typical 2G/3G/4G data, or SMS

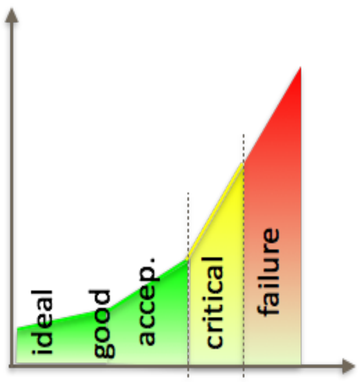


Sub-system analysis
Metrics for AMR

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

- 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)





(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

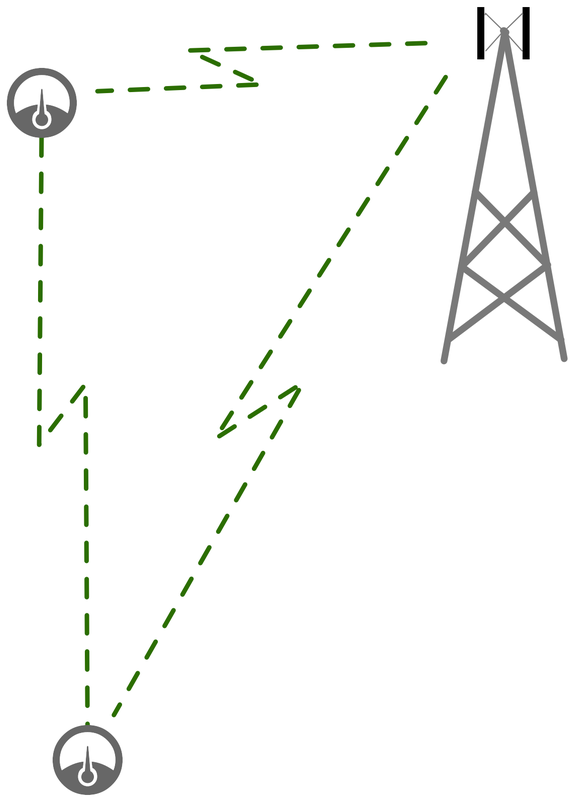
Configuration	Cs	Cp
Encryption ON	10	10
Encryption OFF	80	80

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

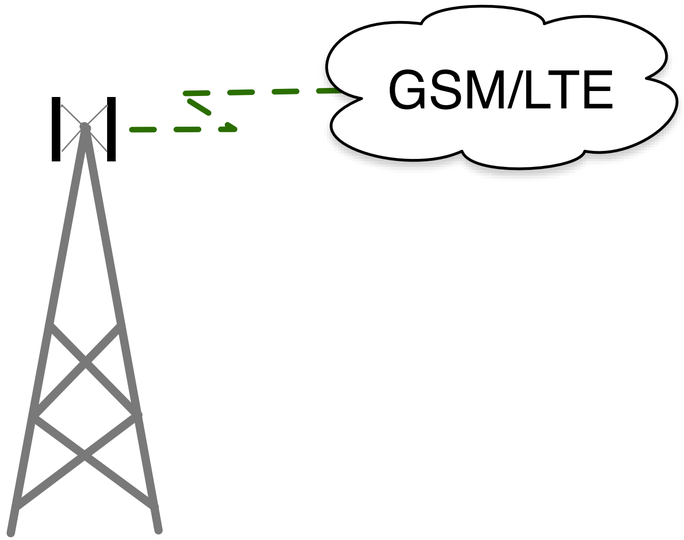
Configuration	Cs	Cp
Encryption ON	10	10
Encryption OFF	80	80

(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)

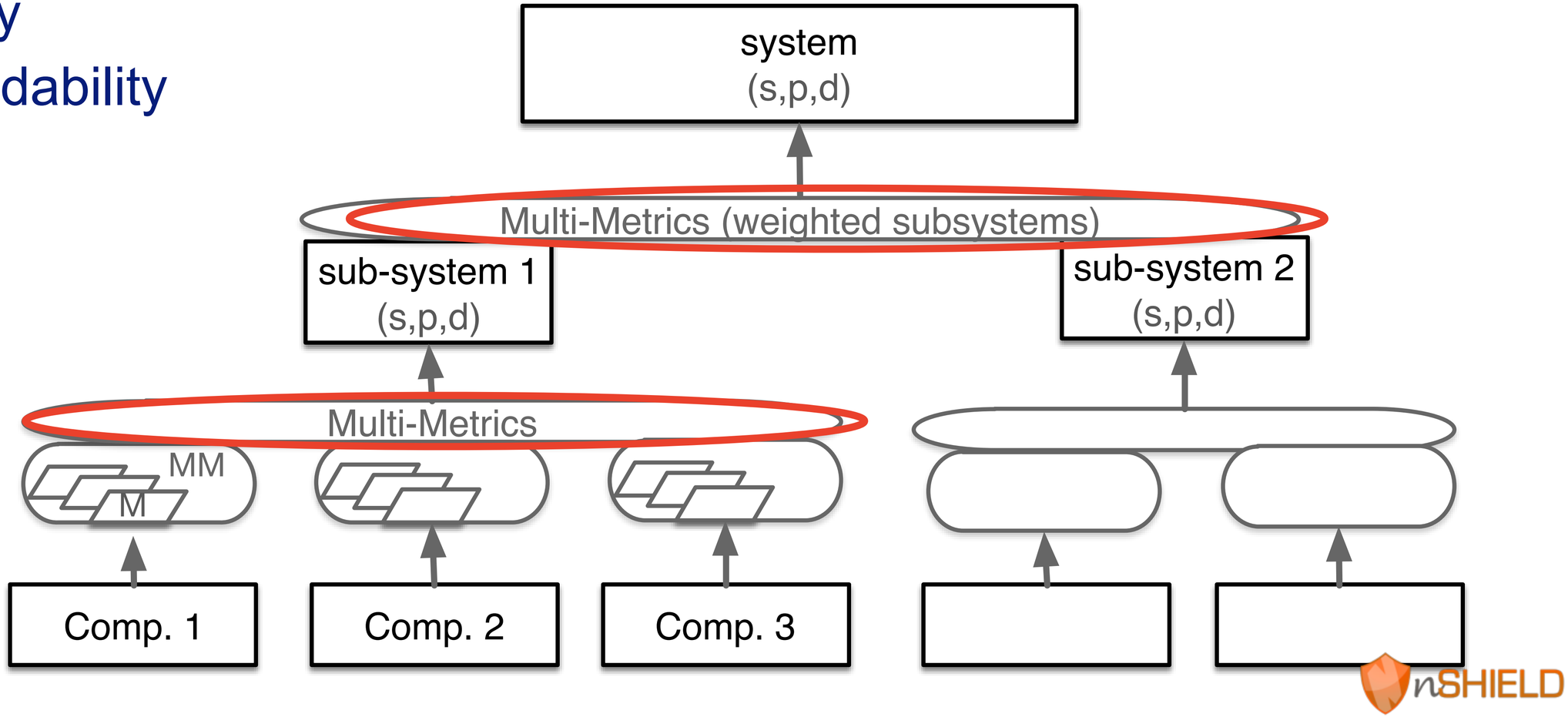
Configuration	Cs	Cp
1 hour	20	20
20 min	25	30
1 min	40	50
5 sec	50	70

(6)

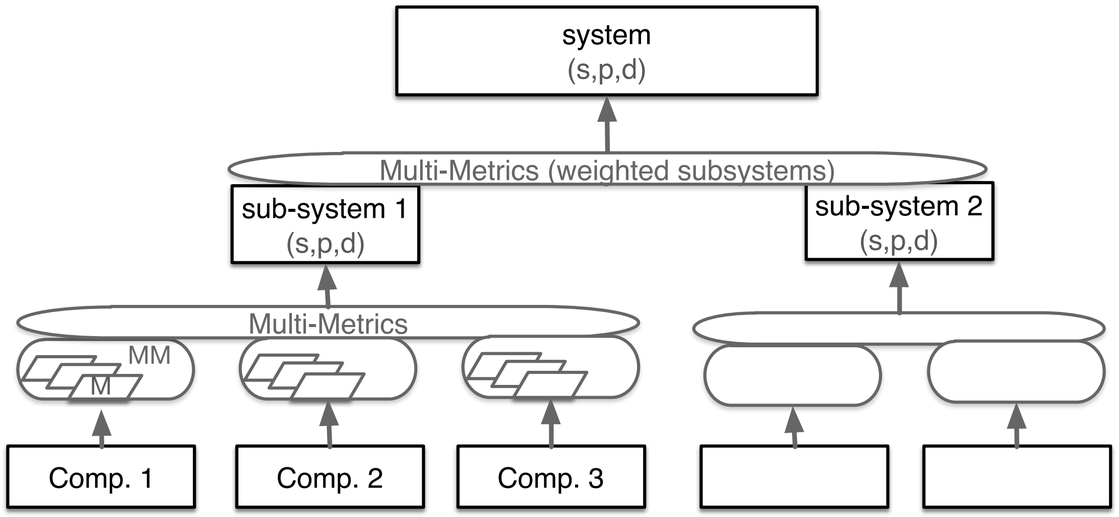
Configuration	Cs	Cp
GPRS	60	70
SMS	40	50

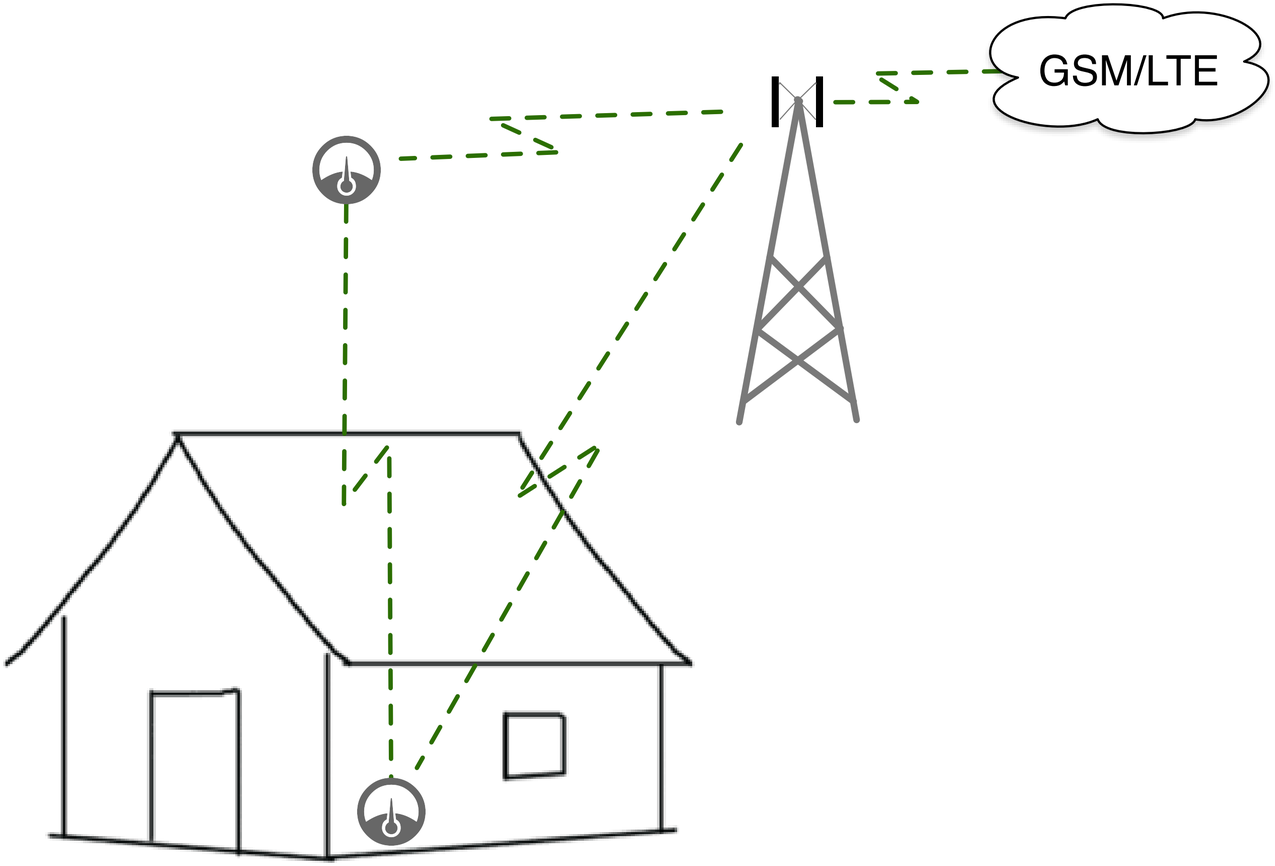
Multi-Metrics$_{v2}$ - system composition

- 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

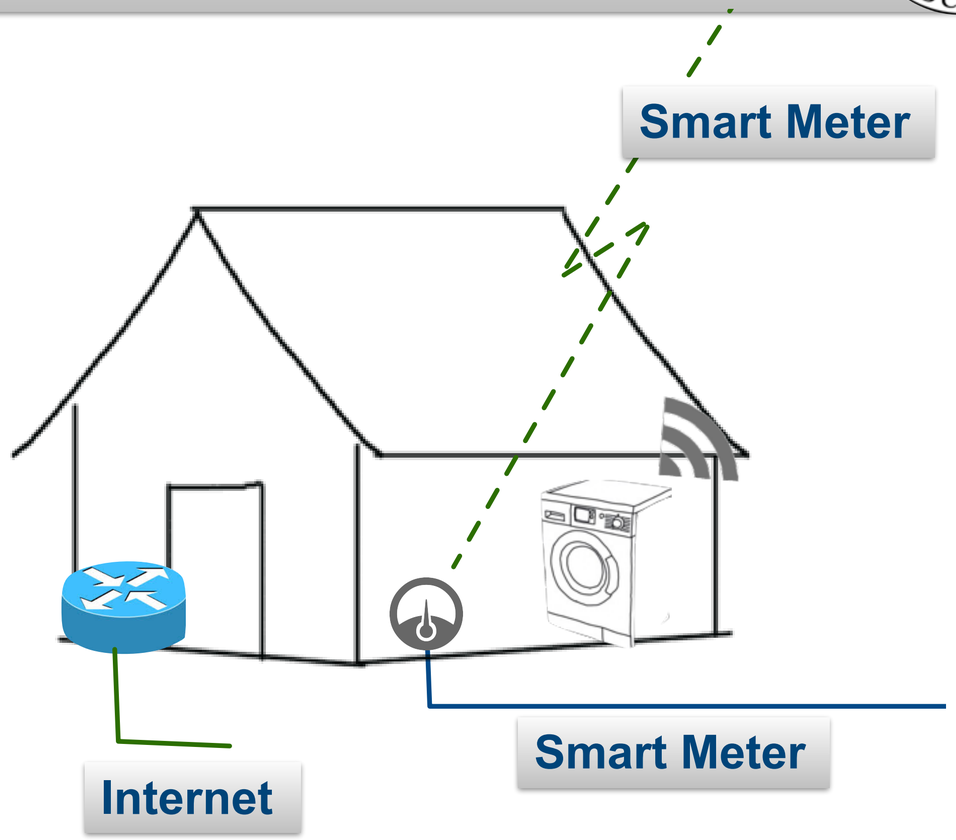
Use Case	Security	Privacy
Billing	90	80
Home Control	90	80
Alarm	60	40

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)	(🔴,🟡,🟡)

Upcoming Infrastructure

- Smart Meter
  - ➡ read and control
  - ➡ logic?
- Smart Home
  - ➡ intelligent devices
  - ➡ on-demand regulation
- Challenges
  - ➡ Logic: Centralised <—-> Fog
  - ➡ Smart Meter: Information <—> Control
  - ➡ Smart Grid Information <—> Internet Info



[source: seminarsonly.com]

Conclusions

- Security and Privacy methodology applied for Smart Grid
- Sub-system Meter Reader, Mesh communication, Mobile Communication assessed
- Weighting, see example

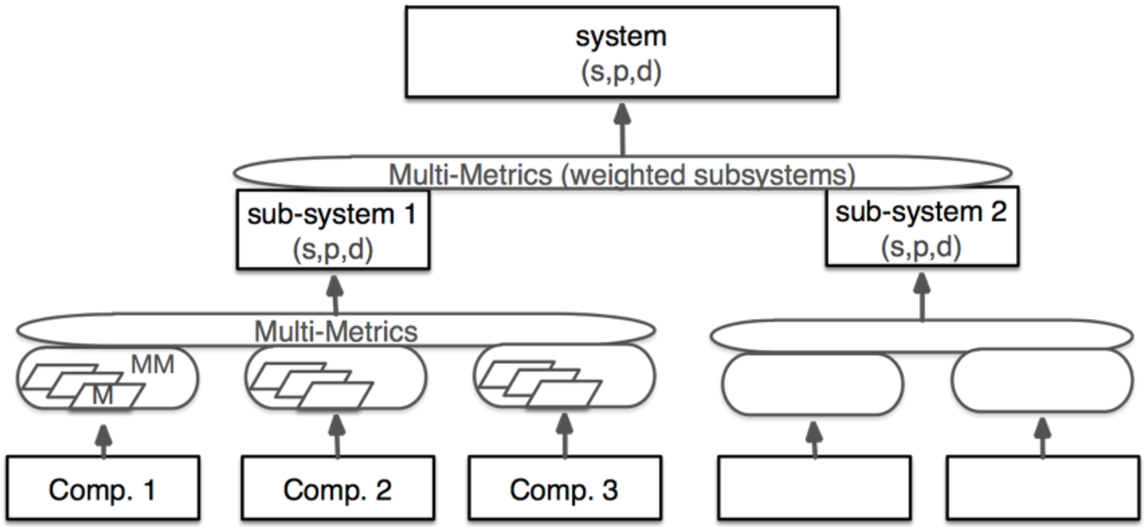
Table 8 Sub-systems and components weights

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

- 11 configurations assessed, best result providing (s,p,d) = (84,77,42)

Upcoming lectures

- L12: System Security and Privacy Analysis

$$|\mathrm{SPD}_{Goal} - \mathrm{SPD\ level}| = \leq 10, \text{ green}.$$
$$|\mathrm{SPD}_{Goal} - \mathrm{SPD\ level}| = > 10, \leq 20, \text{ yellow}.$$
$$|\mathrm{SPD}_{Goal} - \mathrm{SPD\ level}| = > 20, \text{ red}.$$

- …. applying Multi-Metrics on your own