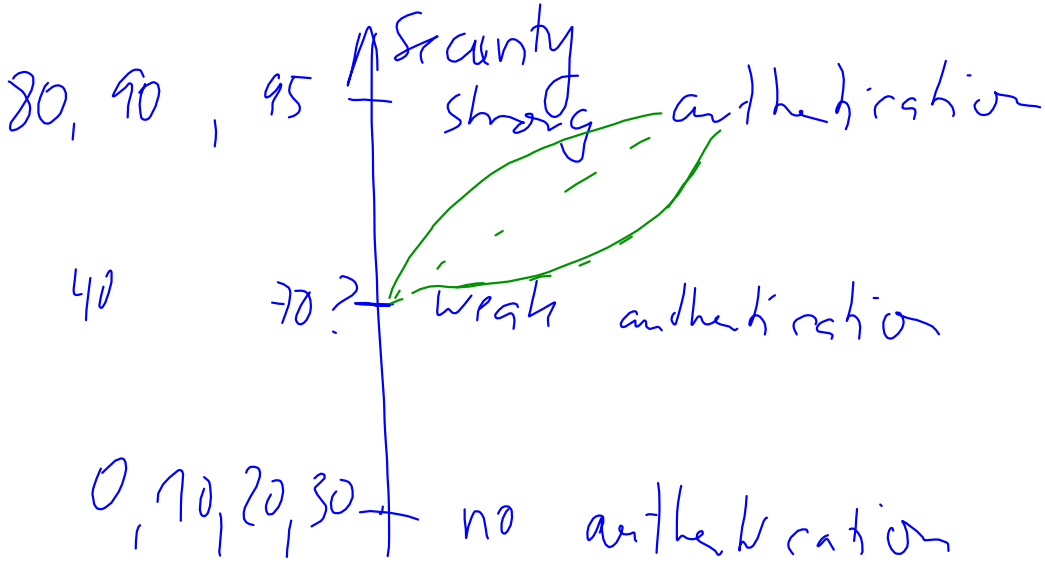
Your take

	S_1	S_2	S_3	P_1	P_2	P_3
• Billing (1/hour) ➡ Security, Privacy Goal: (s,p) - Range [0...100]	80	80	85	80	70	30
• Fire alarm ➡ Security, Privacy Goal: (s,p) - Range [0...100]	95	95	92	5	30	0
• Home Control (1/hour) ➡ Security, Privacy Goal: (s,p) - Range [0...100]	70	90	85	70	85	90

*1 kind of reaction — light
alarm → bubble
acoustical alarm

Define a scale for security & privacy

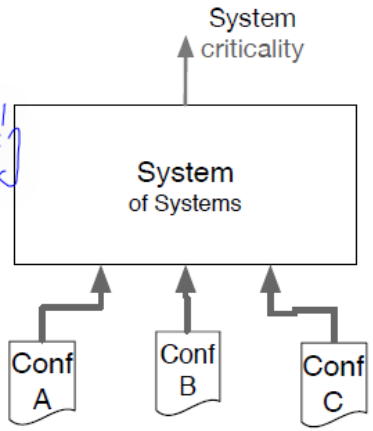
Example Authentication

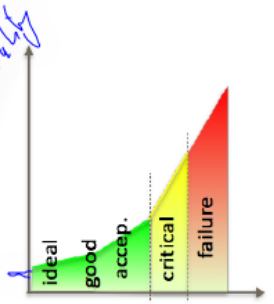


Sub-system analysis
Metrics for AMR

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

- 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

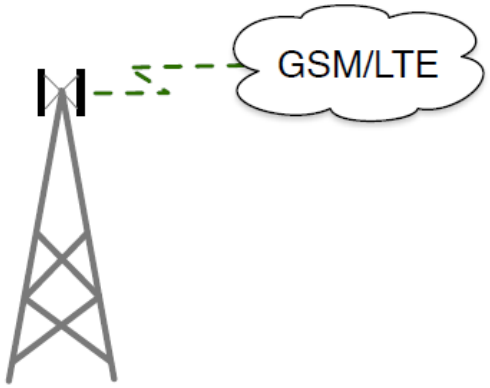
(2) authentication

Configuration	Cs	Cp
Authentication ON	10	30
Authentication OFF	80	70

(3) encryption

Configuration	Cs	Cp
Encryption ON	10	10
Encryption OFF	80	80

- 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

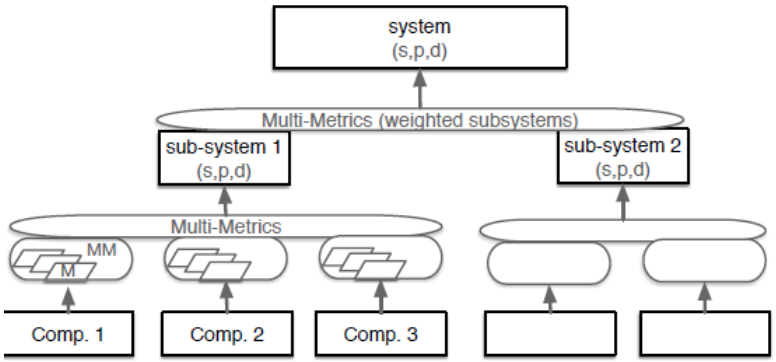
(5)

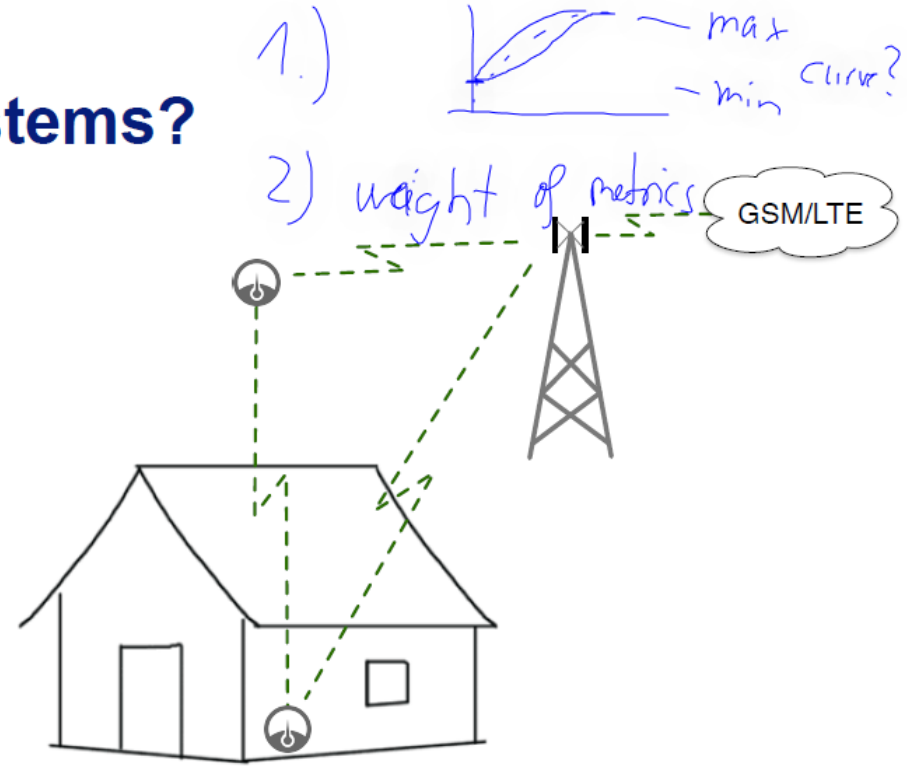
Configuration	Cs	Cp
1 hour	20	20
20 min	25	30
1 min	40	50
5 sec	50	70

(6)

Configuration	Cs	Cp
GPRS	60	70
SMS	40	50

Why weighting of sub-systems?



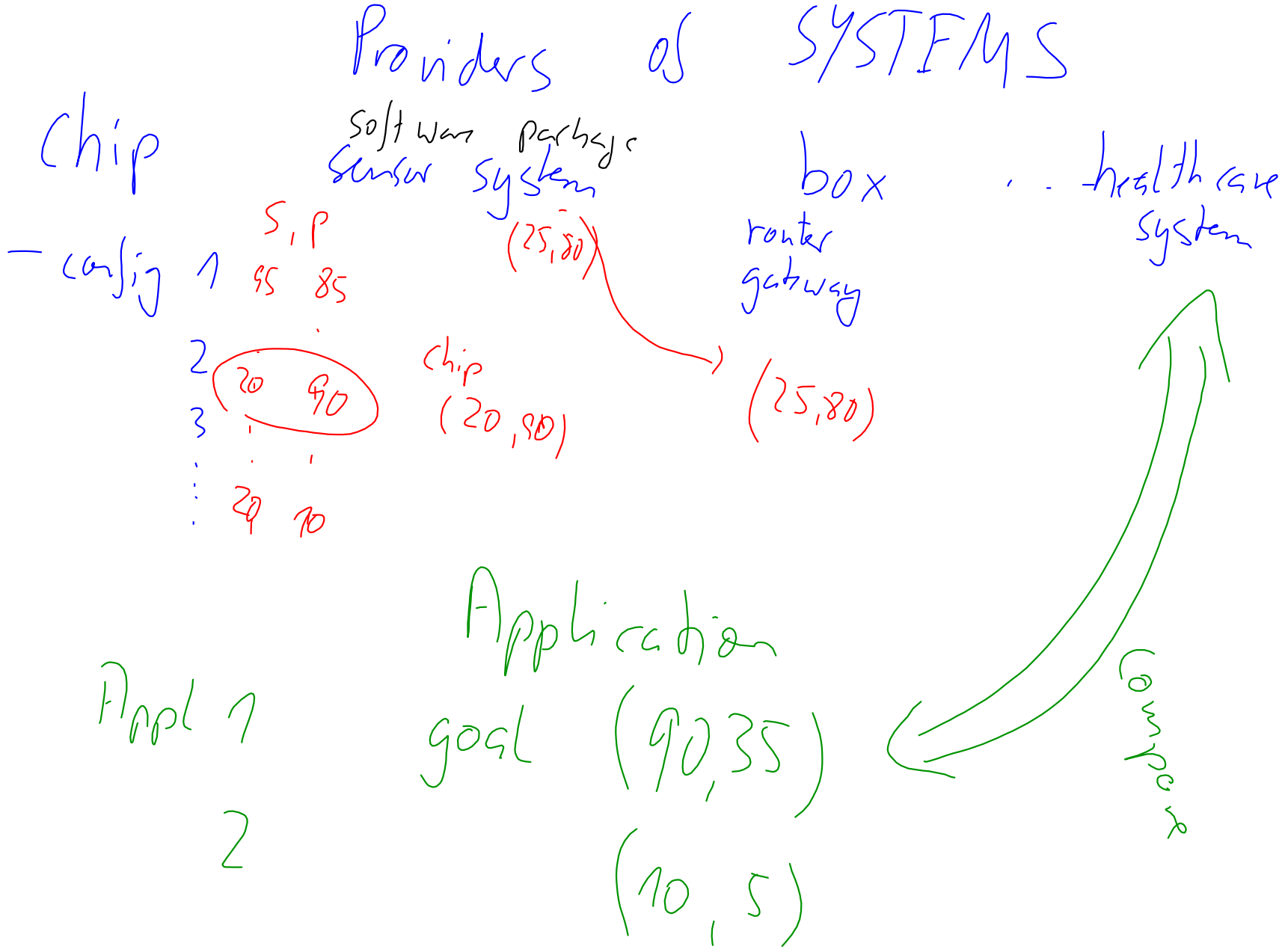


- Component criticality from metrics
- sub-system criticality from evaluation of components
- system criticality from evaluation of sub-systems
- Criticality *C* through root mean square weight
- Actual criticality x_i for component or (sub-)system
- Weight w_i for each metric,
- Result will maximise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


Providers of SYSTEMS
chip
Software package
sensor system
box
. . health care system
router gateway
S, P
config 1 95 85
2 20 90
3
29 10
(25,80)
chip (20,90)
(25,80)
Application
goal (90,35)
(10,5)
Compare
Appl 1
2

- 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 (🟢,🟢,🟡)

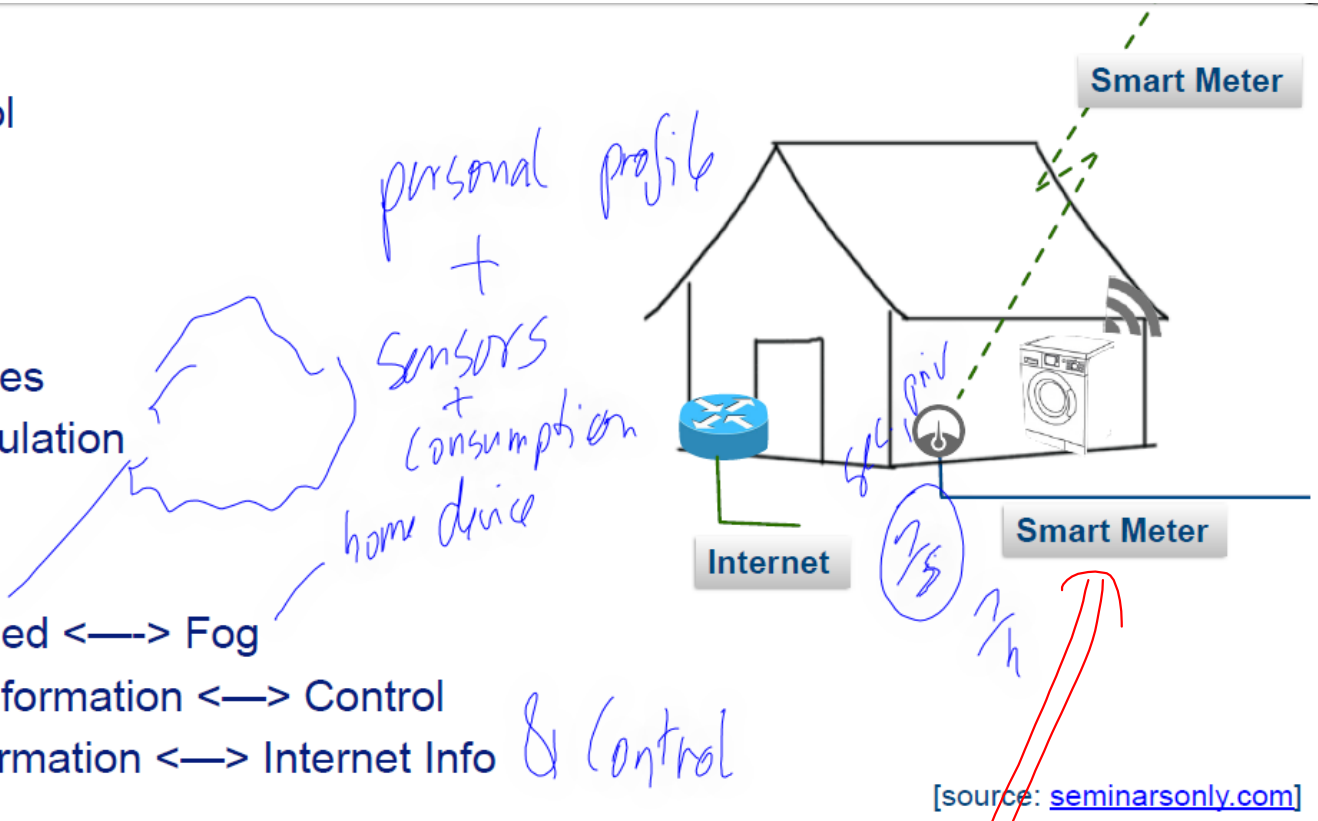
Table 1 SPD_{Goal} of ea

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)	(🔴,🟡,🟡)

- 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]

Starting from the identified menaces and attacks, a set of SPD Functionalities is identified that are able to prevent or mitigate them. The functionalities are the ones that we have to represent in our SPD relevant ontology. An example is provided in Fig. 6. Of course, the node model has relation with the functional ontology.

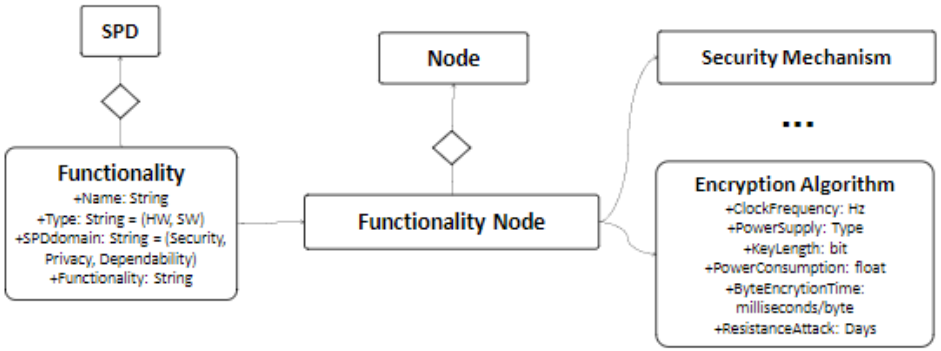


Fig. 6. Functional Ontology

3.2 SPD Ontology

The last model is given by the SPD attributes that allow the link between the structural word and the functional word. This is the most simple and, at the same time, significant ontology. For the purpose of our work we have choose to describe all Dependability, Security (and Privacy) issues by means of six attributes: *availability, reliability, safety, confidentiality, integrity, maintainability* (see Fig. 7).