

(Semantics)

Open



Closed

World Approach

Camp everywhere,  
except close to houses...

Blacklist

Camp, if it is allowed

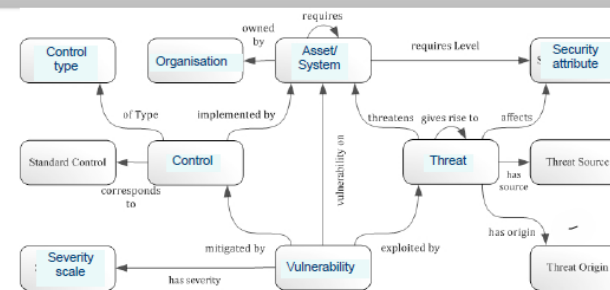
Whitelist

## Limitations of the traditional approach



- Scalability
  - ➔ Threats
  - ➔ System
  - ➔ Vulnerability
- System of Systems
  - ➔ sensors
  - ➔ gateway
  - ➔ middleware
  - ➔ business processes

// applications



### Recommendation:

One ontology per aspect:

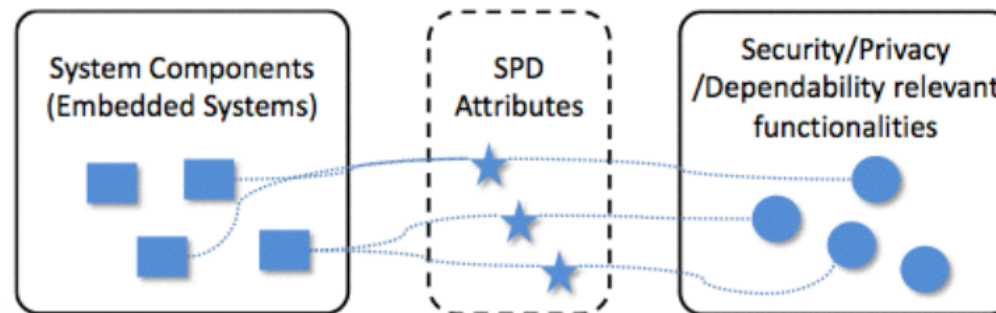
- security
- system
- threats

...



# Security description

- Ontologies for system, security attributes, security functionality



1. describe ontologies

2. rules describing relations

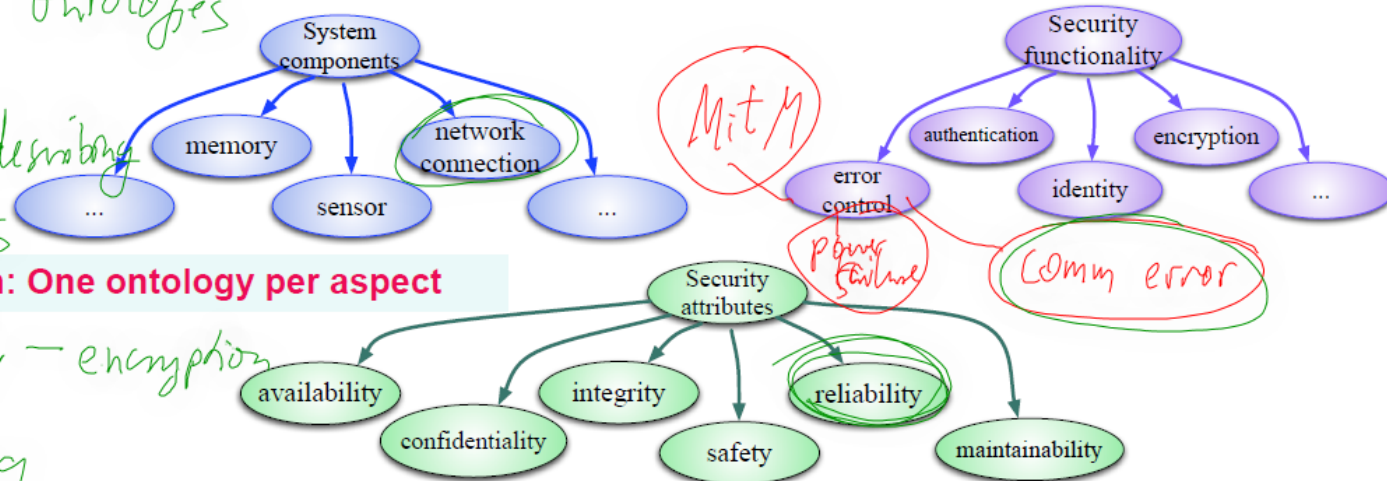
**Recommendation: One ontology per aspect**

3. Reasoning



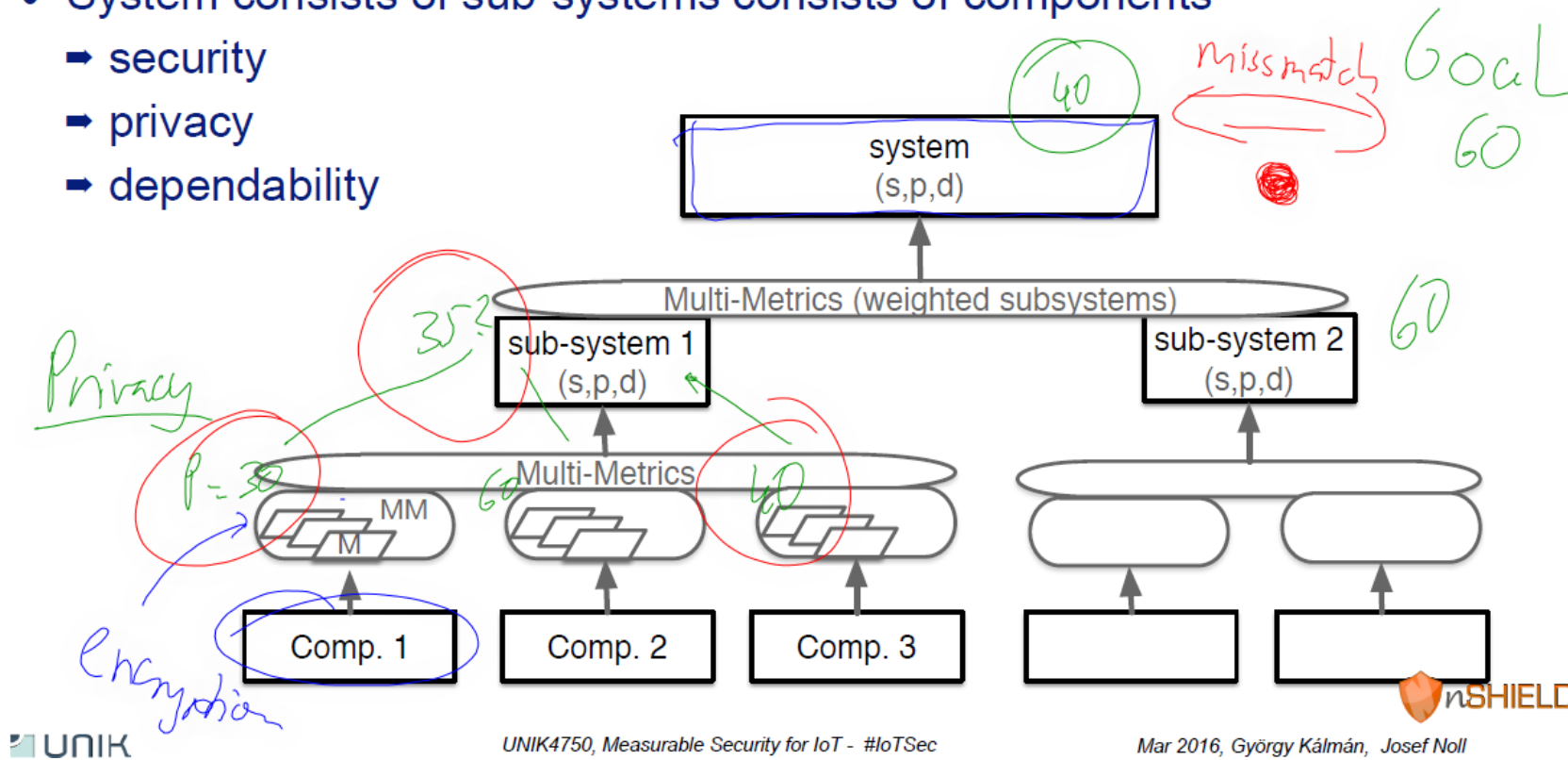
UNIK4750, Measurable Security for IoT - #IoTSec

Mar 2016, György Kálmán, Josef Noll



- System consists of sub-systems consists of components

- ➔ security
- ➔ privacy
- ➔ dependability



UNIK4750, Measurable Security for IoT - #IoTSec

Mar 2016, György Kálmán, Josef Noll

7

→ 1)  $SP \times \text{appl goal} \Rightarrow SP \times \text{goal}$

2) Components: here Comp 1

# SHIELD Multi Metrics Approach



- Security, Privacy and Dependability

- » Specific application
- » Social Mobility: privacy scenario

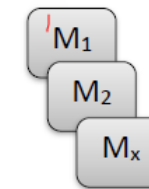
70

| Scenario 1 |         | SPD <sub>Goal</sub> | SPD level   |           |
|------------|---------|---------------------|-------------|-----------|
|            | Conf. A |                     | (s, 100, d) | (s, ●, d) |
|            | Conf. B | (s, 80, d)          | (s, 80, d)  | (s, ●, d) |
|            | Conf. C |                     | (s, 80, d)  | (s, ●, d) |

mismatch

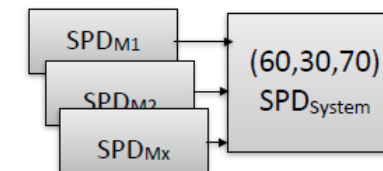
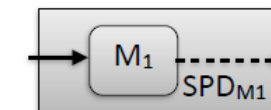
- Multi-Metrics approach to assess the SPD of a system

- » Provides a snapshot of the current state of the system
- » Metrics for SPD parameters of sensors, network, service access
- » Metrics  $M_1 \dots M_x$ , e.g. Network latency, Protection level



- Individual Metrics scaling SPD<sub>M1</sub>(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)

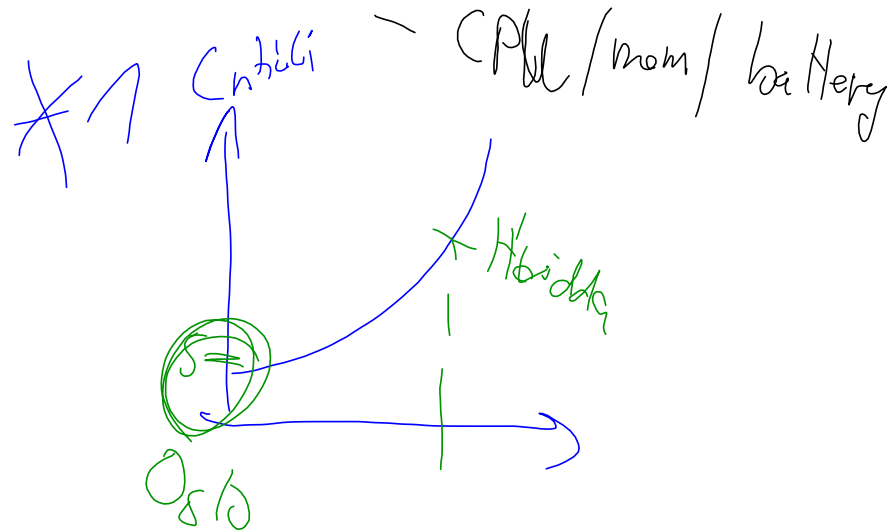


- Metrics combination to provide an SPD tripple: (60, 30, 70)

Drone.  $\rightarrow$  fly over Oslo  $Criticality = 5$  ~~7~~ Rel. = 95  
 fly over H'vikk Rel. = 40

Trade-off in Sec./priv

- usability
- costs

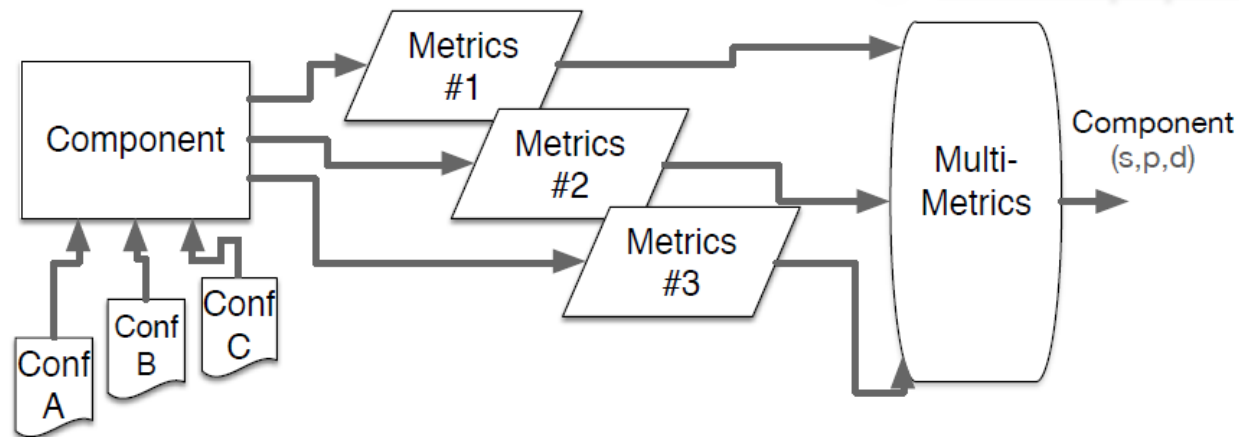
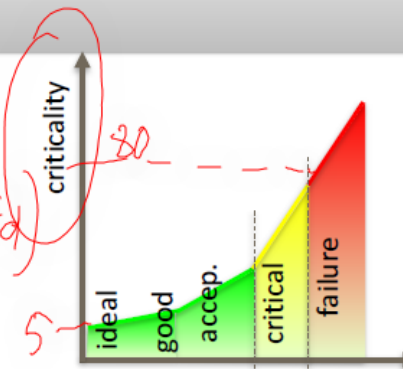


## Multi-Metrics components



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

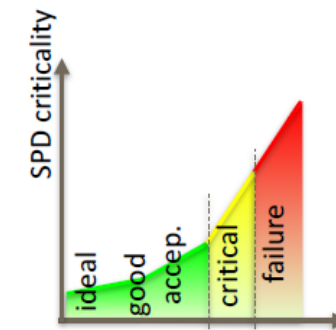
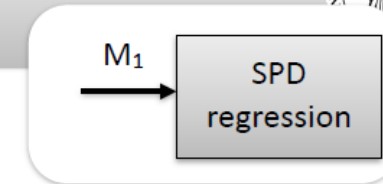
$$(S, P, D) = 100 - (S, P, D)$$



# SHIELD Multi Metrics<sub>v2</sub>

- Metrics to SPD conversion

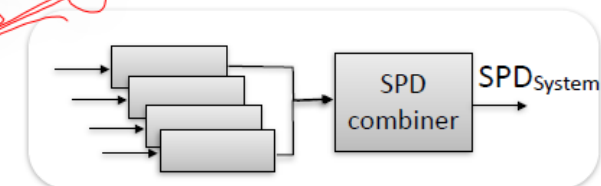
- » Parametrisation of system parameters, e.g. latency -> [ms]
- » SPD regression: «SPD value and importance for the system»
  - » parameter into S,P,D value range, e.g. latency=50ms :=> (ideal, good, acceptable, critical, failure)
  - » Scaling according to System Importance, e.g. latency :=>  $S_{\max}=30$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



- Metrics combination to provide SPD<sub>System</sub>: (60, 30, 70)

- » Mathematical combination, e.g.  $S_{\text{System}} = 100 - \text{SQRT}(S_1^2 + S_2^2 + \dots S_x^2)$

*weighting*

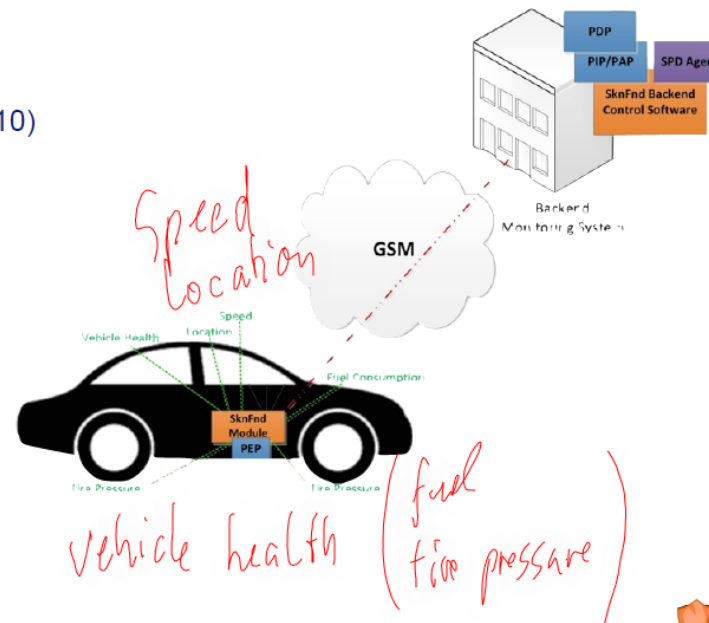


## Social Mobility Components



Applicable nSHIELD Components (Px):

- 1- Lightweight Cyphering (P1)
- 2- Key exchange (P2)
- 3- Anonymity & Location Privacy (P10)
- 4- Automatic Access Control (P11)
- 5- Recognizing DoS Attack (P13)
- 6- Intrusion Detection System (P15)
- 7- Attack surface metrics (P28)
- 8- Embedded SIM, sensor (P38)
- 9- Multimetrics (P27)

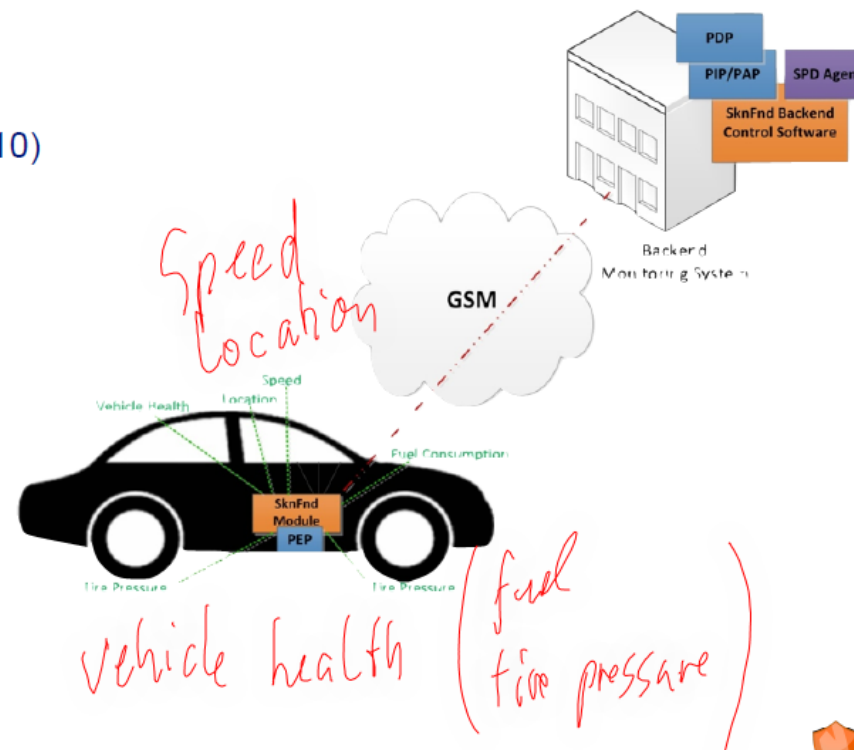


# Social Mobility Components



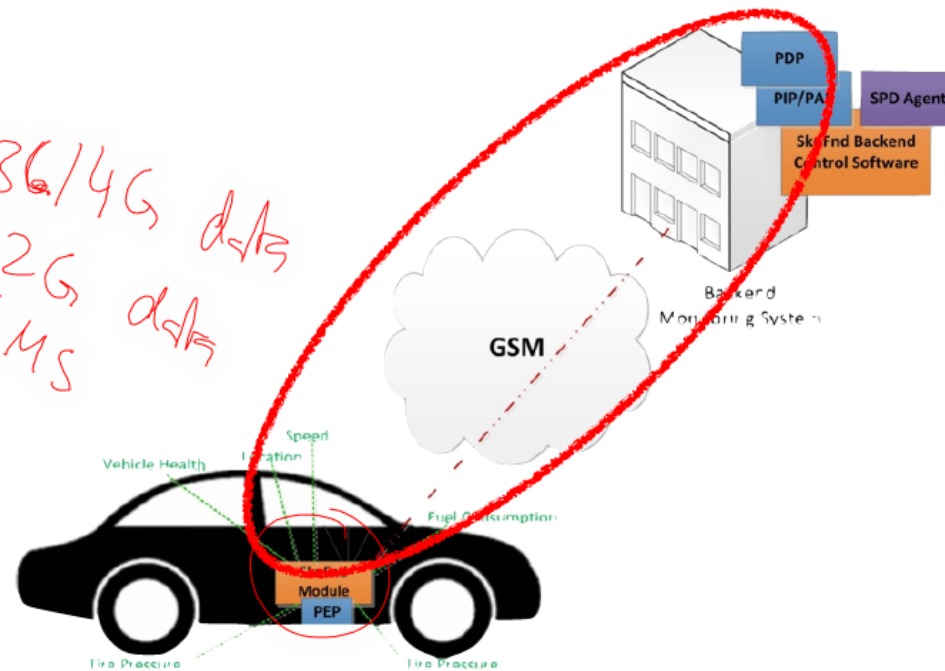
Applicable nSHIELD Components (Px):

- 1- Lightweight Cyphering (P1)
- 2- Key exchange (P2)
- 3- Anonymity & Location Privacy (P10)
- 4- Automatic Access Control (P11)
- 5- Recognizing DoS Attack (P13)
- 6- Intrusion Detection System (P15)
- 7- Attack surface metrics (P28)
- 8- Embedded SIM, sensor (P38)
- 9- Multimetrics (P27)



## (SPD) Metrics

- ➔ Port metric
- ➔ Communication channel
- ➔ GPRS message rate
- ➔ SMS rate
- ➔ Encryption



# Social Mobility - Examples of Metrics



GPRS message rate metric

| Parameter(sec) | 0.5 | 1  | 2  | 5  | 10 | 20 | 60 | 120 | $\infty$ |
|----------------|-----|----|----|----|----|----|----|-----|----------|
| Cp             | 80  | 60 | 45 | 30 | 20 | 15 | 10 | 5   | 0        |

$$P = 100 - C_p \quad 20$$

700

Encryption metric

| Parameter | No encryption | Key 64 bits | Key 128 bits | Not applicable |
|-----------|---------------|-------------|--------------|----------------|
| Cp        | 88            | 10          | 5            | 0              |

10

12

Metrics weighting

95

100

Port (M1),  $w = 100$

Communication channel (M2),  $w = 100$

GPRS message rate (M3),  $w = 80$

SMS message rate (M4),  $w = 20$

Encryption (M5),  $w = 100$



# Multi-Metrics subsystem evaluation



5 metrics

|                        | Criticality |    |               |    |                     | SPD <sub>P</sub> |          |          |          |
|------------------------|-------------|----|---------------|----|---------------------|------------------|----------|----------|----------|
|                        | C1          | C2 | C3            | C4 | Sub-Sys.            |                  | Scen. 1  | Scen. 2  | Scen. 3  |
| SPD <sub>Goal</sub>    |             |    |               |    |                     |                  | (s,80,d) | (s,50,d) | (s,5,d)  |
| Multi-Metrics Elements | M1          | M2 | M3<br>∩<br>M4 | M5 | C1...<br>∩<br>...C4 |                  | Privacy  | Speeding | Accident |
| Conf. A                | 30          | 20 | 0             | 5  | 17                  | 83               | ●        | ●        | ●        |
| Conf. B                | 61          | 20 | 4             | 5  | 32                  | 68               | ●        | ●        | ●        |
| Conf. C                | 41          | 20 | 9             | 5  | 23                  | 77               | ●        | ●        | ●        |
| Conf. D                | 82          | 41 | 2             | 10 | 45                  | 55               | ●        | ●        | ●        |
| Conf. E                | 82          | 41 | 18            | 10 | 45                  | 55               | ●        | ●        | ●        |
| Conf. F                | 83          | 41 | 27            | 10 | 47                  | 53               | ●        | ●        | ●        |
| Conf. G                | 82          | 42 | 4             | 88 | 70                  | 30               | ●        | ●        | ●        |
| Conf. H                | 82          | 42 | 40            | 88 | 73                  | 27               | ●        | ●        | ●        |
| Conf. I                | 83          | 42 | 72            | 88 | Alarm               | 21               | ●        | ●        | ●        |

17

Conf.

●  $\Rightarrow \Delta < 10$

● yellow  $\Rightarrow \Delta < 20$

●  $\Delta > 20$

nSHIELD

f Noll

16

# Metrics & weight (only privacy)



1) Port metric, weight  $w_p=40$

|                               | $C_p$ | $SPD_p$ |
|-------------------------------|-------|---------|
| SNMP (UDP) 161 in the ES      | 40    | 60      |
| SNMP trap (UDP) 162 in the BE | 60    | 40      |
| SSH (TCP) 23 in the ES        | 30    | 70      |
| SMS                           | 80    | 20      |

*Embedded System = sensor*

2) Communication channel metric, weight  $w_p=20$

|                        | $C_p$ | $SPD_p$ |
|------------------------|-------|---------|
| GPRS with GEA/3        | 20    | 80      |
| SMS over GSM with A5/1 | 40    | 60      |

4) SMS message rate metric  $w_p=20$   
0,1, or 2 messages  $SPD_p=90-100$

5) Encryption metric  $w_p=60$

|                | $C_p$ | $SPD_p$ |
|----------------|-------|---------|
| No encryption  | 88    | 12      |
| Key 64 bits    | 10    | 90      |
| Key 128 bits   | 5     | 95      |
| Not applicable | 0     | 100     |

*Back End*

3) GPRS message rate metric  $w_p=80$

| message delay | $C_p$ | $SPD_p$ |
|---------------|-------|---------|
| 0.5 sec       | 80    | 20      |
| 1 sec         | 60    | 40      |
| 2 sec         | 45    | 65      |
| 5 sec         | 30    | 70      |
| 10 sec        | 20    | 80      |
| 20 sec        | 15    | 85      |
| 60 sec        | 10    | 90      |
| 120 sec       | 5     | 95      |
| No messages   | 0     | 100     |