UiO : Department of Technology Systems
University of Oslo

UNIK4750 - Measurable Security for the Internet of Things

L10 – Multi-Metrics Analysis

György Kálmán,
DNB / ITS

Josef Noll
UiO, ITS
josef.noll@its.uio.no

http://IoTSec.no , #IoTSec, #IoTSecNO

Overview

- Your project (how to collaborate?)
  - Google (UNIK4710), Piazza, …
- Recap: Security Ontologies (last 6 slides of L8)
- Learning outcomes L10
- Use case (application) SocialMobility
- Values for Security, Privacy
- Analyse the system of systems
- Identify Security, Privacy attributes and functionality for a sub-system
- Multi-Metrics analysis
- Future work

Expected Learning outcomes

Having followed the lecture, you can

- establish a scenario/use case
- provide application examples
- provide reasons for the choice of s,p,d
- establish a system architecture with sub-systems and components
- explain the Multi-Metrics method
- (prepare for your own work)

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

nSHIELD

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

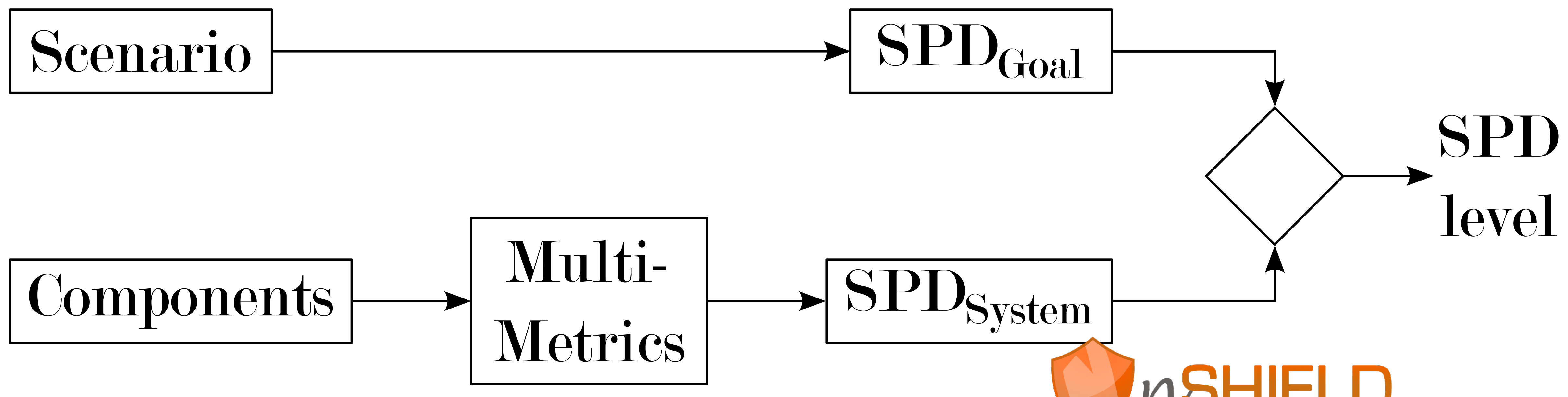
ARTEMIS

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=?

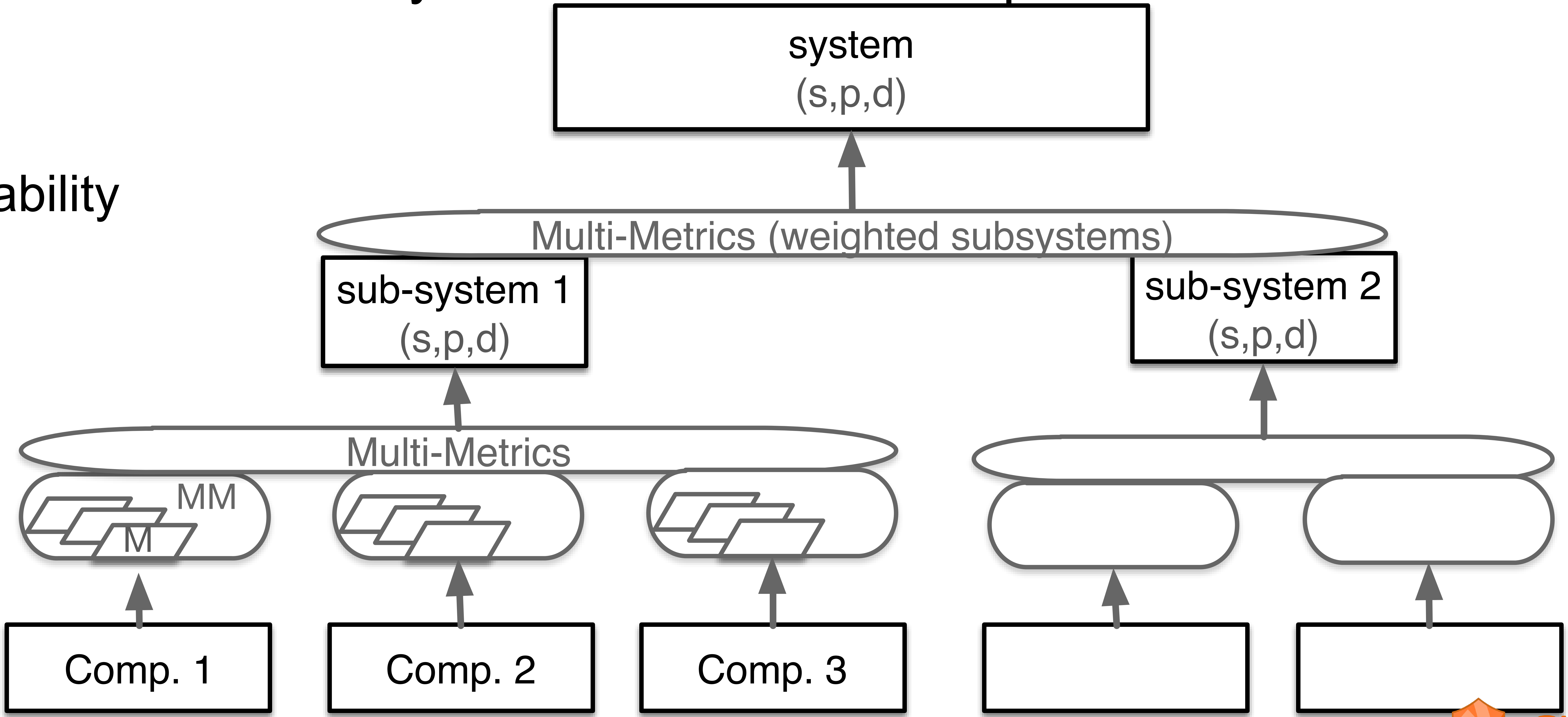
Social Mobility Main Focus

- 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
- SPD_{System} is compared to SPD_{Goal}



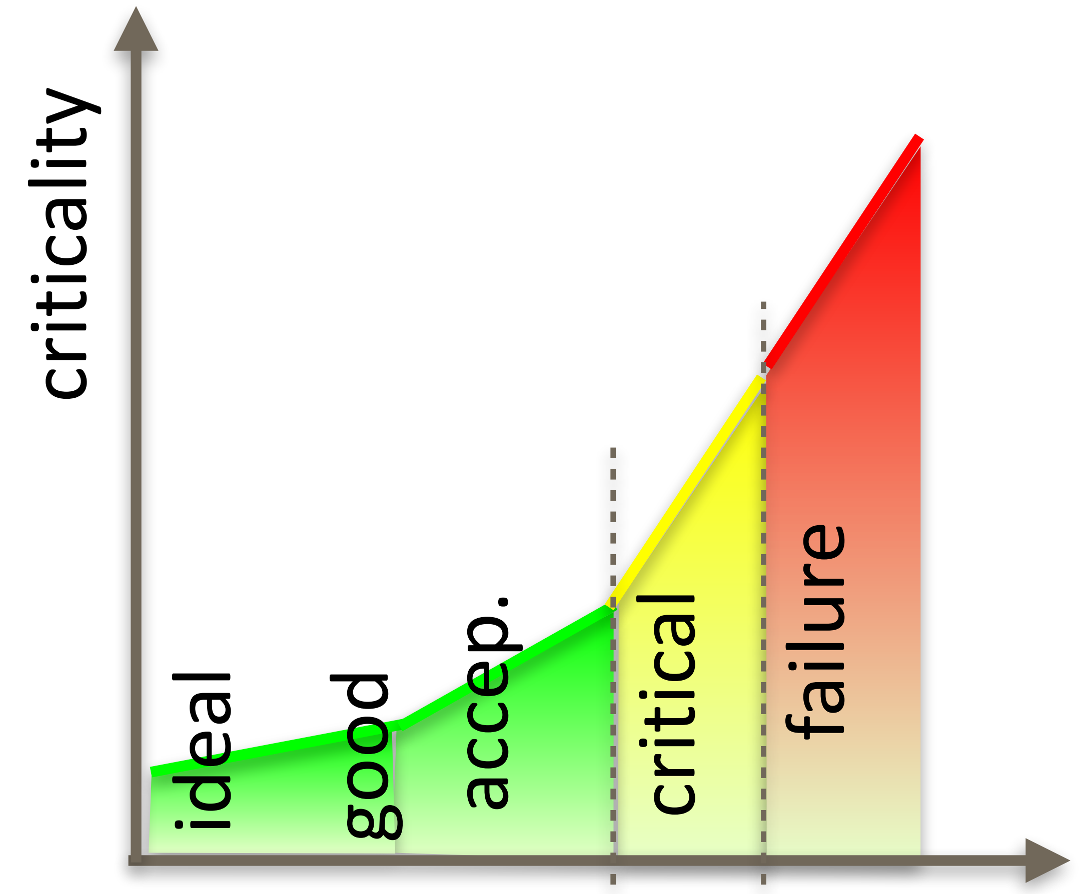
Multi-Metrics$_{v2}$ - system composition

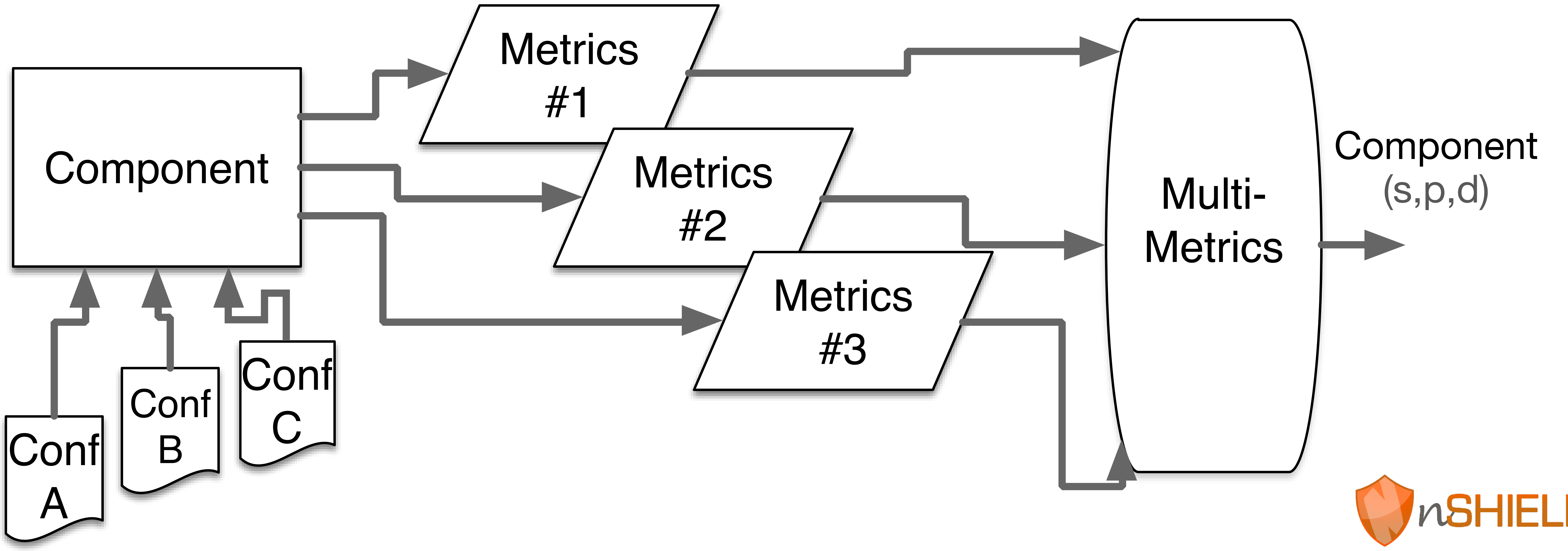
- System consists of sub-systems consists of components
  - security
  - privacy
  - dependability

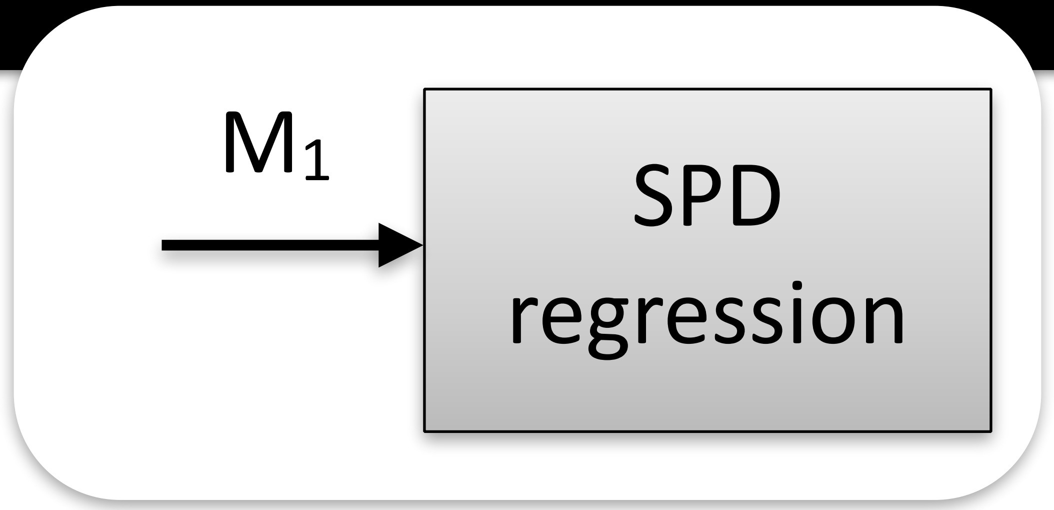


Multi-Metrics components

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

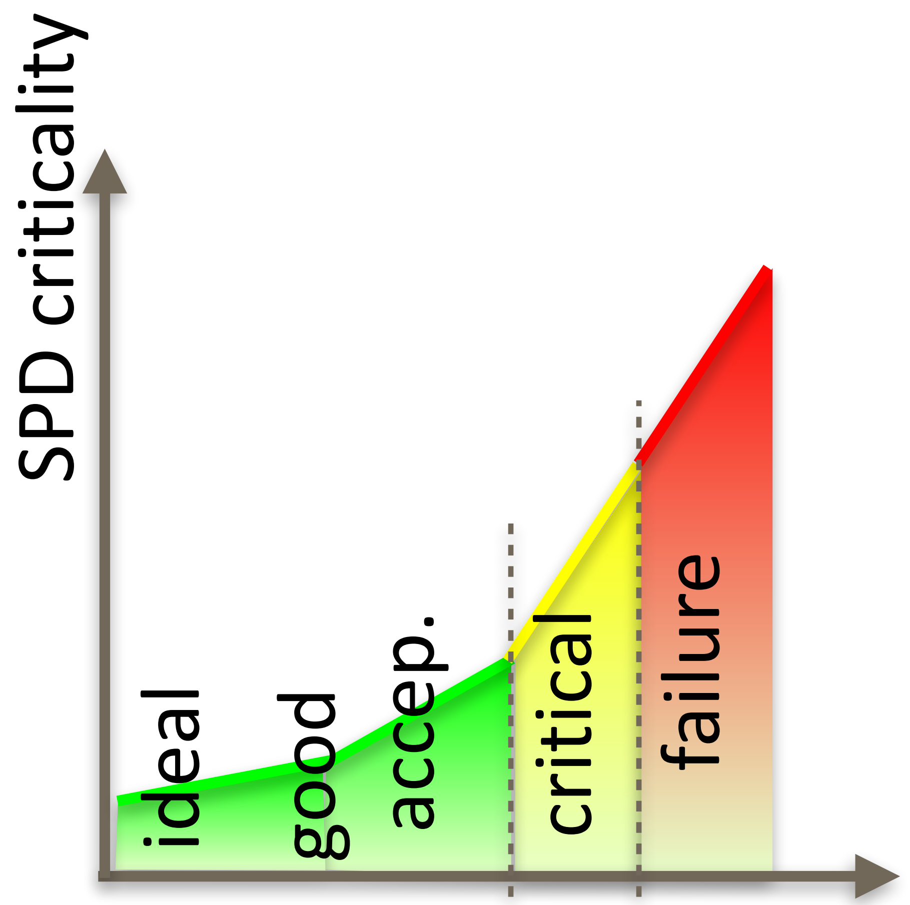




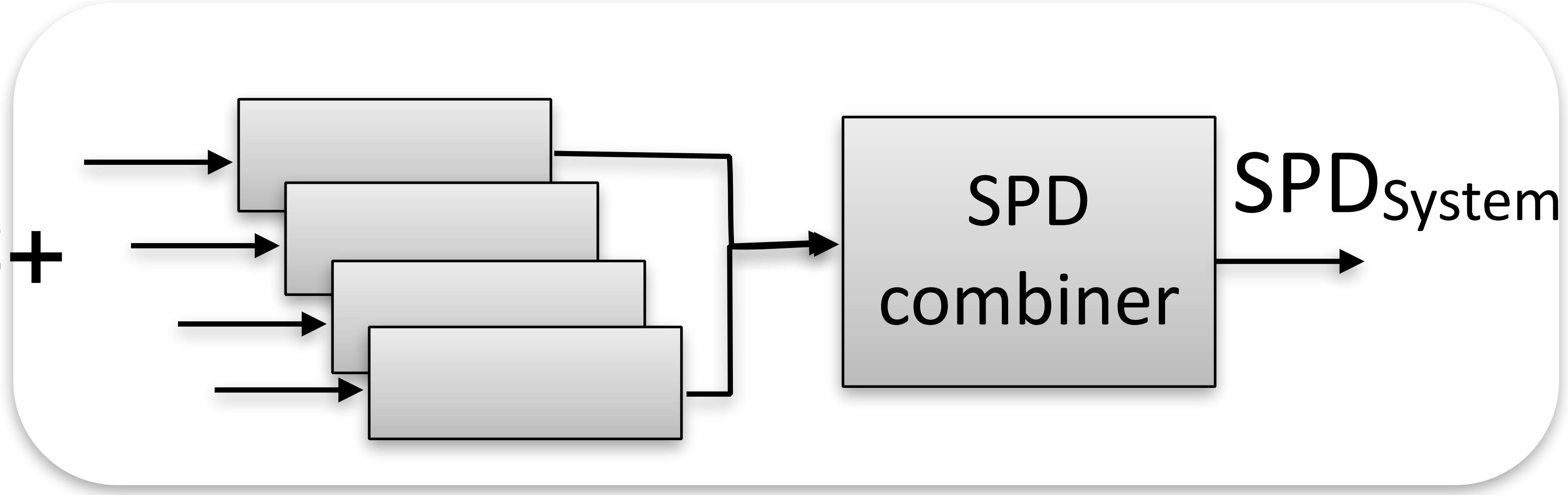


SHIELD Multi Metrics$_{v2}$

- 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

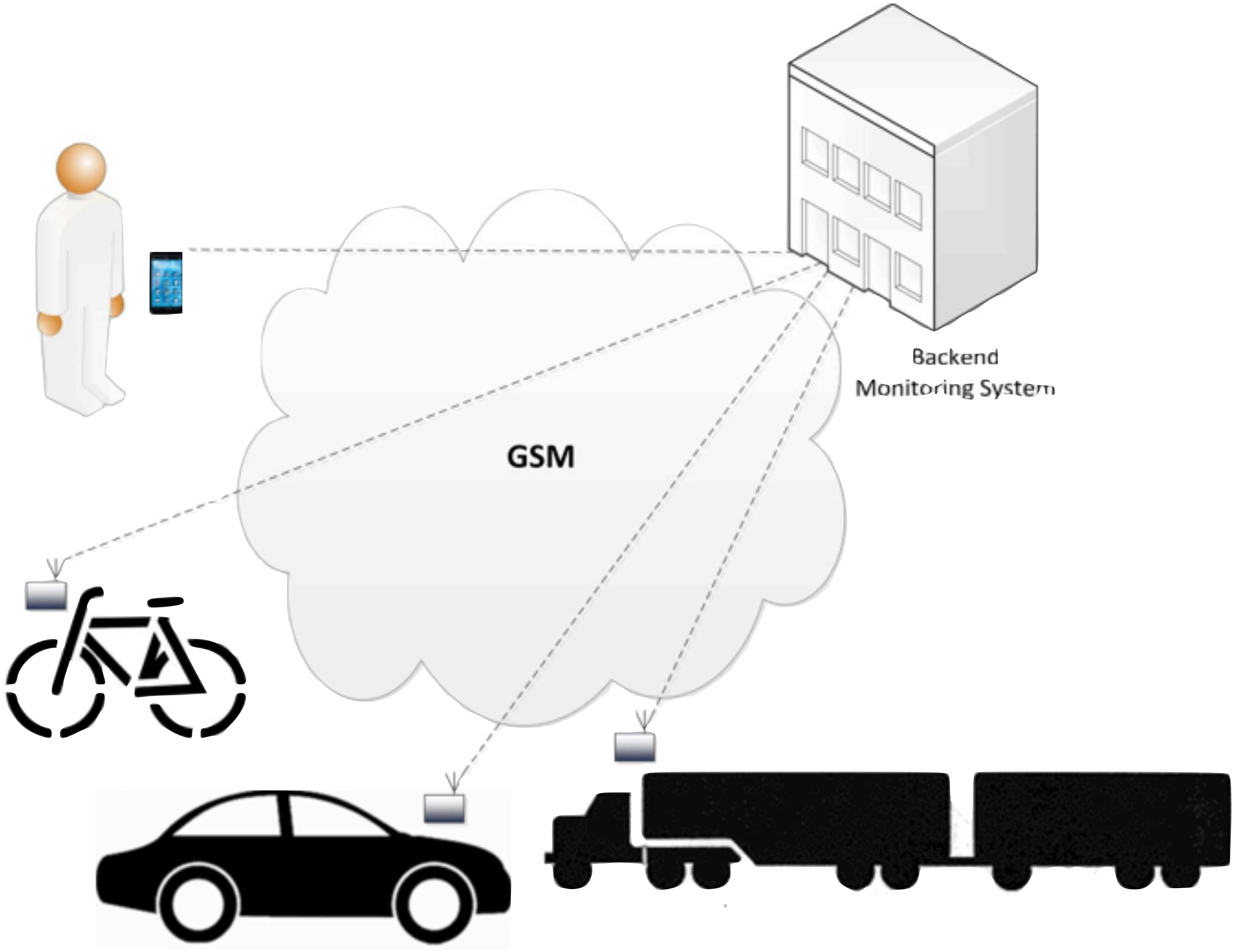


- Metrics combination to provide SPD_{System}: (60, 30, 70)
  - Mathematical combination, e.g. $S_{System}=100 - SQRT(S_1^2+S_2^2+ \ldots S_x^2)$



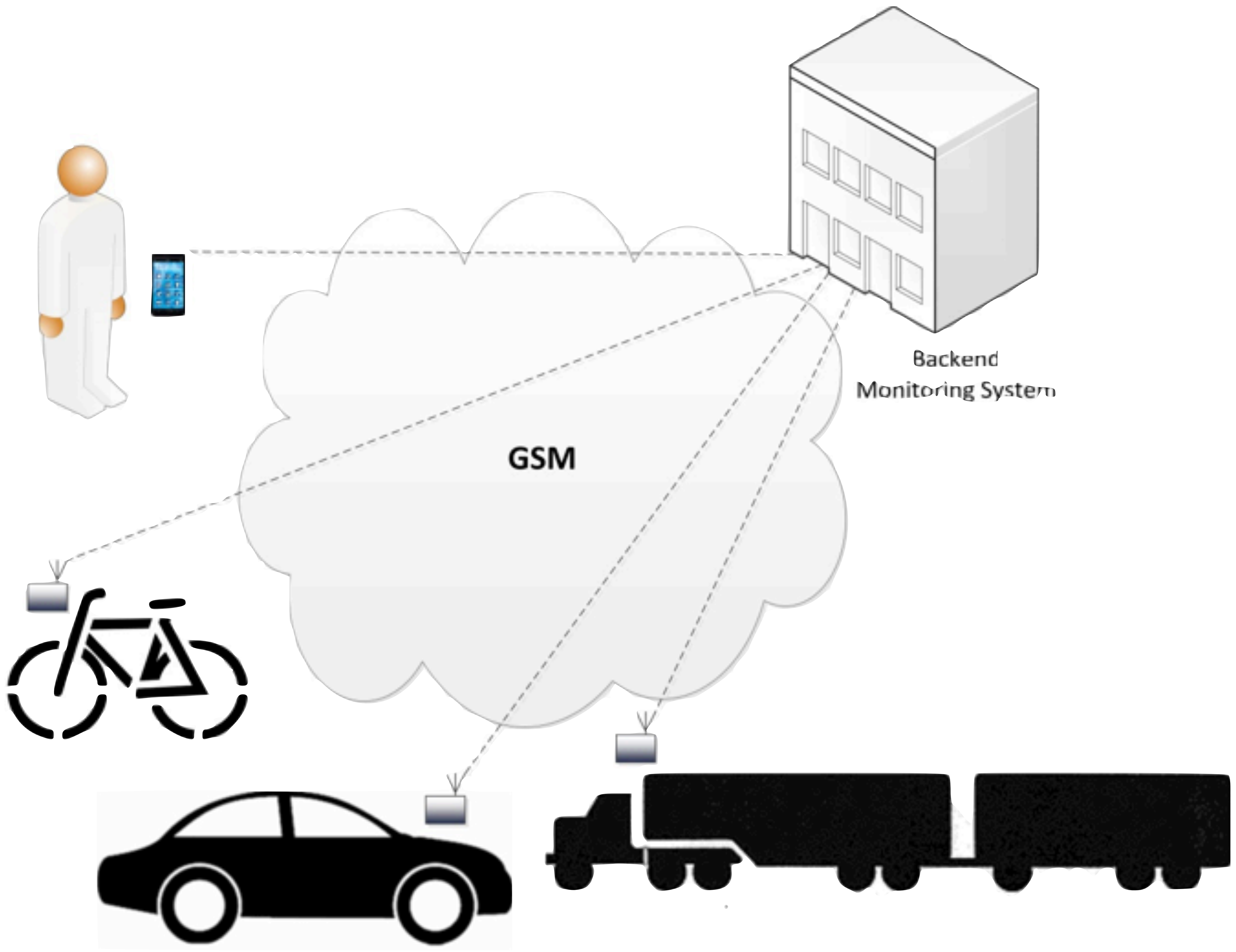
Example:
Privacy in a Social Mobility Use Case

- Social Mobility, including social networks, here: loan of vehicle
- Shall I monitor the user?



Privacy: Loan of vehicle

- Sc1: privacy ensured, «user behaves»
- Sc2: track is visible as user drives too fast
- Sc3: Crash, emergency actions

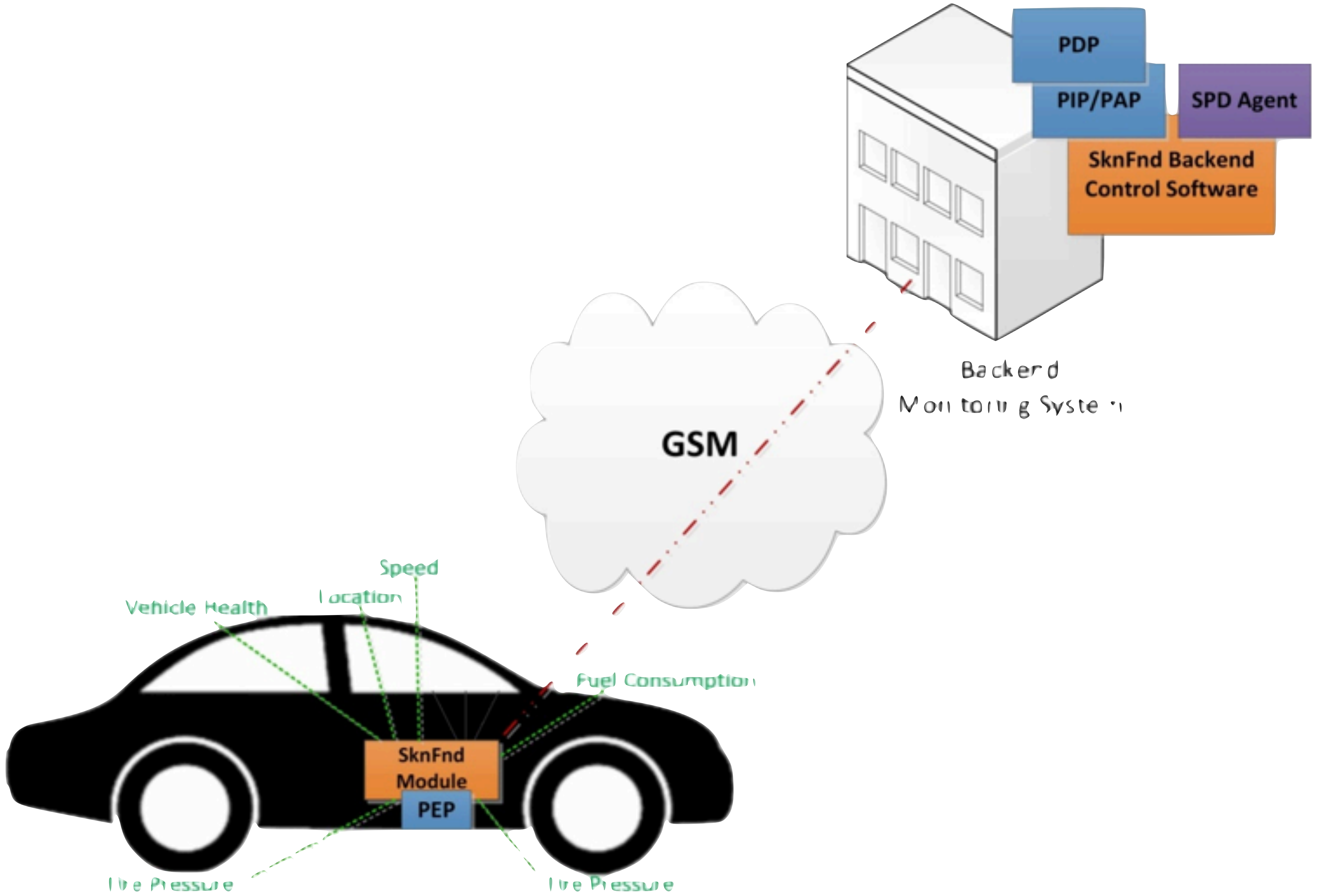


- Industrial applicability: Truck operation (Volvo), Autonomous operations on building places, add sensors (eye control)

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)

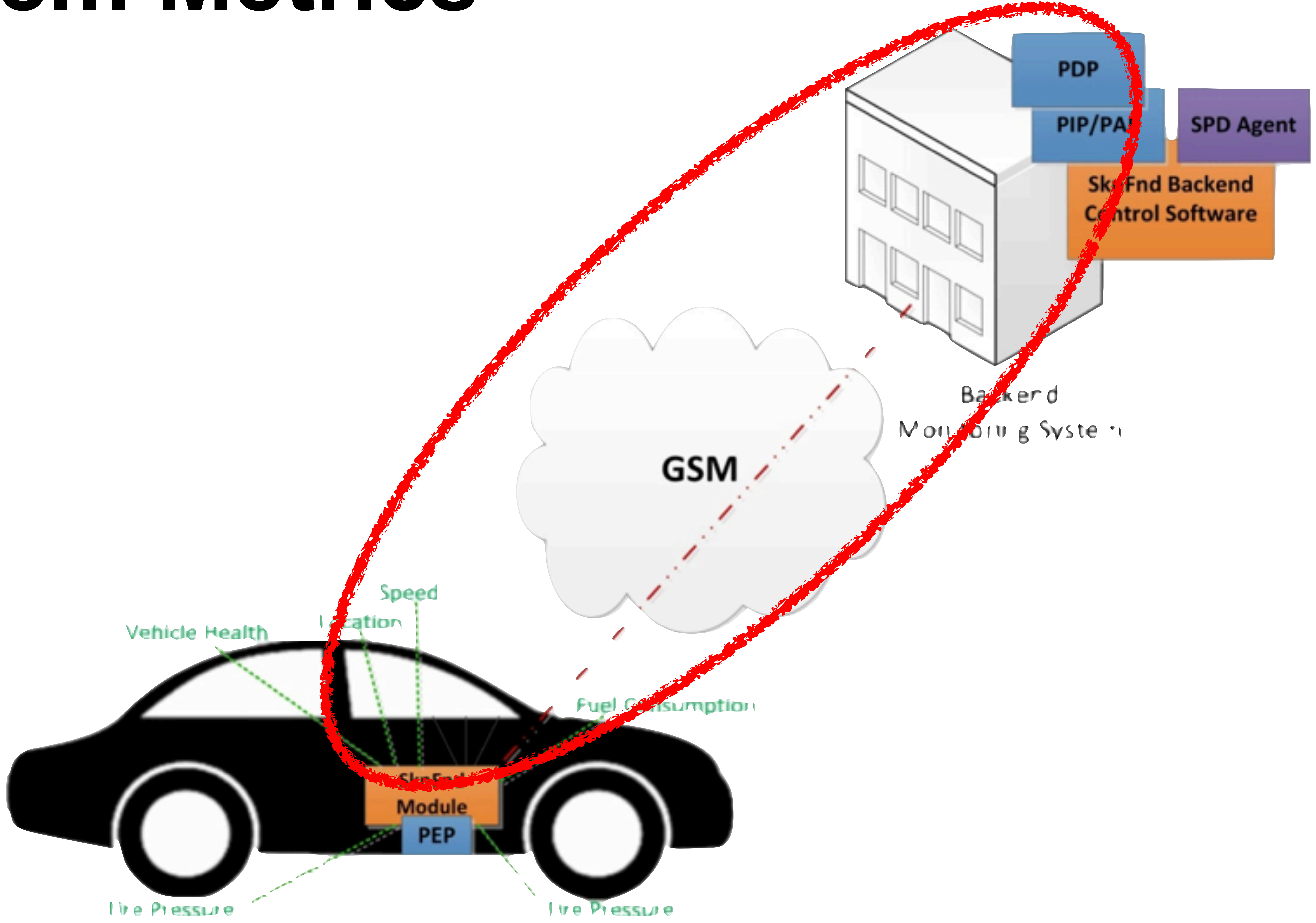


nSHIELD

Communication Subsystem Metrics

(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	∞
Cp	80	60	45	30	20	15	10	5	0

Encryption metric

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

Metrics weighting

Port (M1), $w = 100$
Communication channel (M2), $w = 100$
GPRS message rate (M3), $w = 80$
SMS message rate (M4), $w = 20$
Encryption (M5), $w = 100$

nSHIELD

Multi-Metrics subsystem evaluation

	Criticality					SPD_P			
	C1	C2	C3	C4	Sub-Sys.		Scen. 1	Scen. 2	Scen. 3
SPD_{Goal}							(s,80,d)	(s,50,d)	(s,5,d)
Multi-Metrics Elements	M1	M2	M3 ∩ M4	M5	C1... ∩ ...C4				
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	🔴	🟡	🟡

nSHIELD

Privacy Scenarios - *to trigger your ideas*

- Loan of the car (normal operation, speeding, accident)
- The home medical equipment
  - Transmitting the data
  - Applications storing and handling the data
- Networked cameras and microphones
  - Privacy of persons captured
  - Who can access the data
  - What kind of operations can be performed on the data
- Speaking & listening doll
  - Microphone recording everything in the room (children playing, grown-ups discussing)
- FitBit & Smart Watches
  - sleeping cycle
  - puls, fitness
- *your take….*

thanks to Elahe Fazelkohrdi

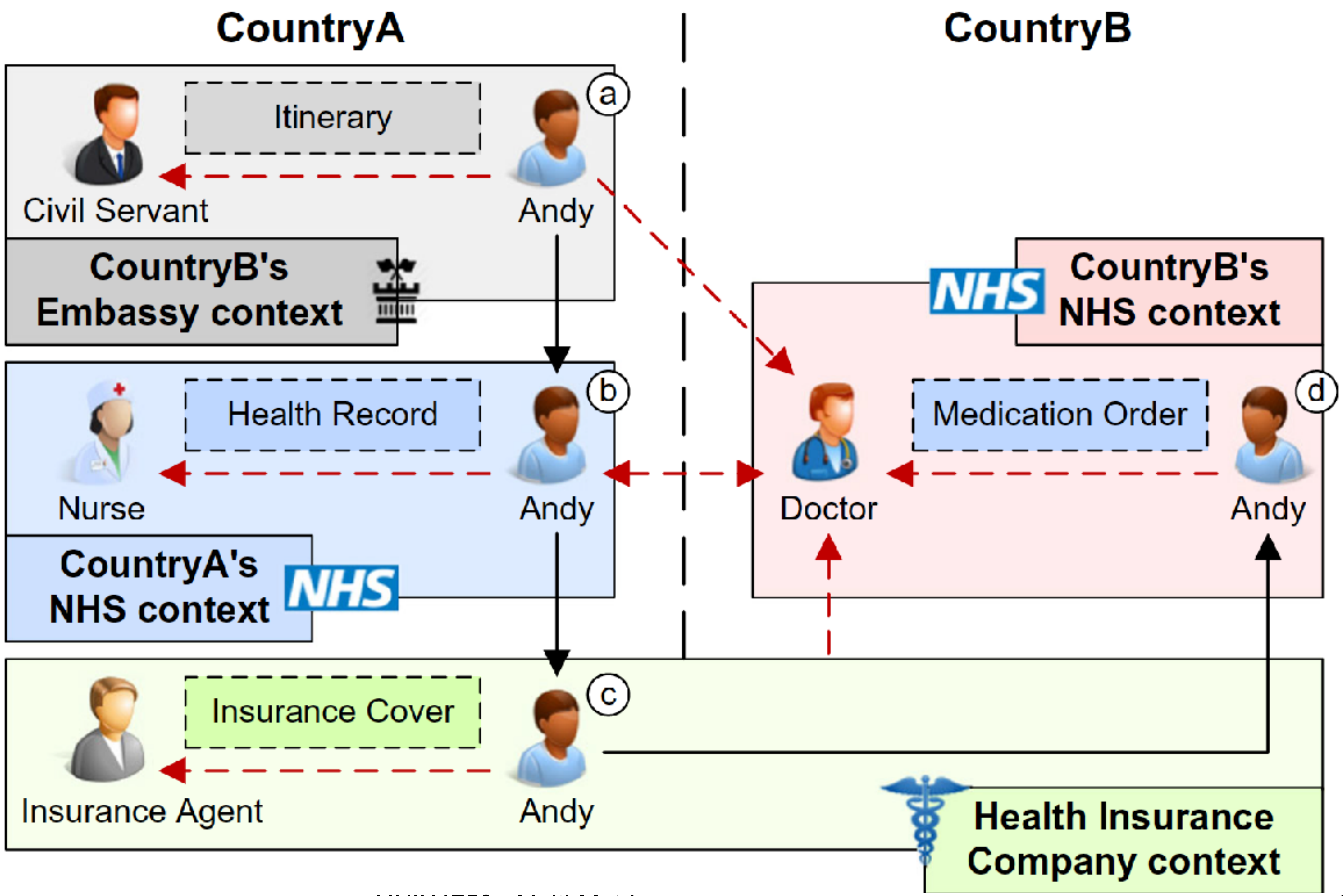
Privacy measuring in Smart Grids and Energy metering

- Advanced Metering Infrastructures (AMI) and Smart Meters are deployed in Norway to automatically and continuously measure energy consumption.
- There are many Privacy Concerns around these:
  - How much Private information can be extracted from this data ?
  - How well is this data anonymized ?
  - How well can we measure the privacy implications of such Smart Systems ?
- Papers to start from (also see who cites these on scholar.google.com):
  - "Smart grid privacy via anonymization of smart metering data." by Costas Efthymiou and Georgios Kalogridis, in IEEE International Conference on Smart Grid Communications (SmartGridComm), 2010.
  - "Influence of data granularity on smart meter privacy." by Günther Eibl and Dominik Engel in IEEE Transactions on Smart Grid 6.2 (2015): 930-939.
  - "Do not snoop my habits: preserving privacy in the smart grid." by Félix Gómez Mármol; Christoph Sorge; Osman Ugus; Gregorio Martínez Pérez in *IEEE Communications Magazine* 50.5 (2012).
  - "Achieving anonymity via clustering." by Aggarwal, et al. in *Proceedings of the twenty-fifth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*. ACM, 2006.
  - "An overview of the use of clustering for data privacy." by Torra, Vicenç, Guillermo Navarro-Arribas, and Klara Stokes in *Unsupervised Learning Algorithms*. Springer, Cham, 2016. 237-251.

Privacy measuring in Smart Buildings for Air Quality

- Multiple sensors are used to monitor air quality in Smart office buildings or industrial facilities. Various privacy sensitive data are being collected and analysed, ranging from office employees to secret industrial processes.
- There are many Privacy Concerns around these:
  - ➡ How much Information should be gathered for the task that is intended ?
  - ➡ Can the indoor location of people and processes be inferred; how precisely ?
  - ➡ If anonymized and minimised, can Machine Learning algorithms still perform well ?
- Papers to start from (also see who cites these on scholar.google.com):
  - ➡ "A terminology for talking about privacy by data minimization." by Pfitzmann, Andreas, and Marit Hansen. (2010).
  - ➡ "Monitoring Data Minimisation." by Pinisetty S, Antignac T, Sands D, Schneider G. (2018)
  - ➡ "A general survey of privacy-preserving data mining models and algorithms." by Charu C. Aggarwal and S. Yu Philip in book *Privacy-preserving data mining*. (2008)
  - ➡ "A survey of computational location privacy." by Krumm, John in *Personal and Ubiquitous Computing* 13.6 (2009): 391-399.
  - ➡ Book 2005: Privacy, security and trust within the context of pervasive computing
  - "Quantifying location privacy." by Shokri, Reza, et al. in *IEEE Symposium on Security and Privacy (2011)*
  - "Geo-indistinguishability: Differential privacy for location-based systems." by Andrés, Miguel E., et al. in *ACM SIGSAC Conference on Computer & Communications Security*. (2013)

Health Scenario, health record exchange



Privacy-specific parameters

- Please discuss with your neighbours
  - a) other scenarios (6 min)
  - b) what are the important privacy parameters (5 min)

- Examples of privacy parameters
  - which data are collected
  - sharing to my phone, my cloud, public cloud,...
  - data communication integrity and storage
  - further distribution of data, ownership of data, further processing

Privacy Labelling

http://PrivacyLabel.IoTSec.no

- “Measure, what you can measure - Make measurable, what you can’t measure” - Galileo
- Privacy today
  - ➡ based on lawyer terminology
  - ➡ 250.000 words on app terms and conditions
- Privacy tomorrow
  - ➡ A++: sharing with no others
  - ➡ A: …
  - ➡ C: sharing with ….
- The Privacy label for apps and devices

Appfail Report – Threats to Consumers in Mobile Apps

The Norwegian Consumer Council analysed the terms of 20 mobile apps. The purpose is to uncover potential threats to consumer protection hidden in the end-user terms and privacy policies of apps.

The economic perspective of Privacy Label

- The big 5 IT companies have a GDP as big as that of France
- Amazon largest sector in terms of revenue is selling of data
  - ➡ 20% of revenue

- How can SMEs compete?
  - ➡ Each service and device gets a privacy label

- Four areas for Privacy Label
  - ➡ which data are collected
  - ➡ sharing to my phone, my cloud, public cloud,...
  - data communication integrity and storage
  - further distribution of data, ownership of data, further processing

Privacy Label (A-F)
- easy visibility
- customer focus
- transparent

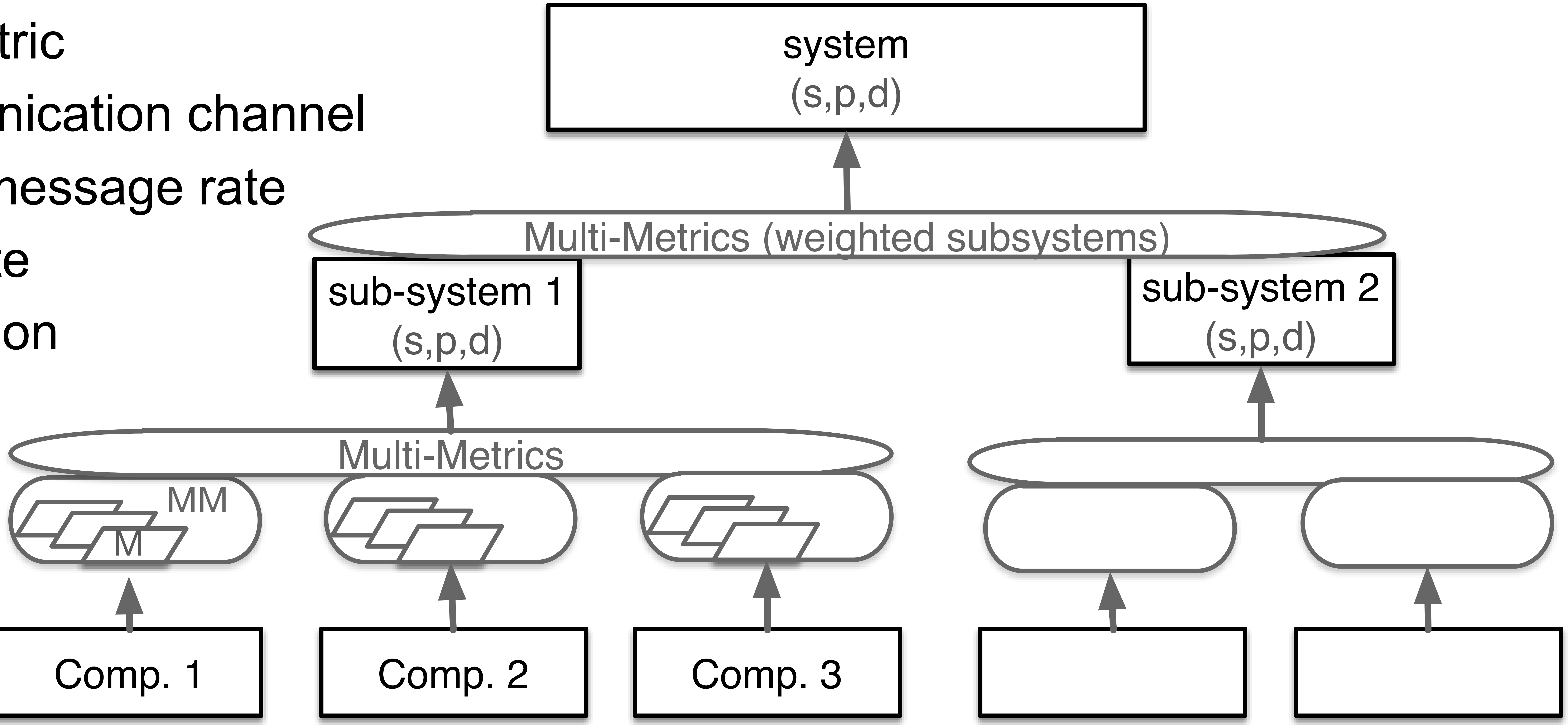
privacylabel.IoTSec.no

Run-Through Example

- Car loan, privacy considerations

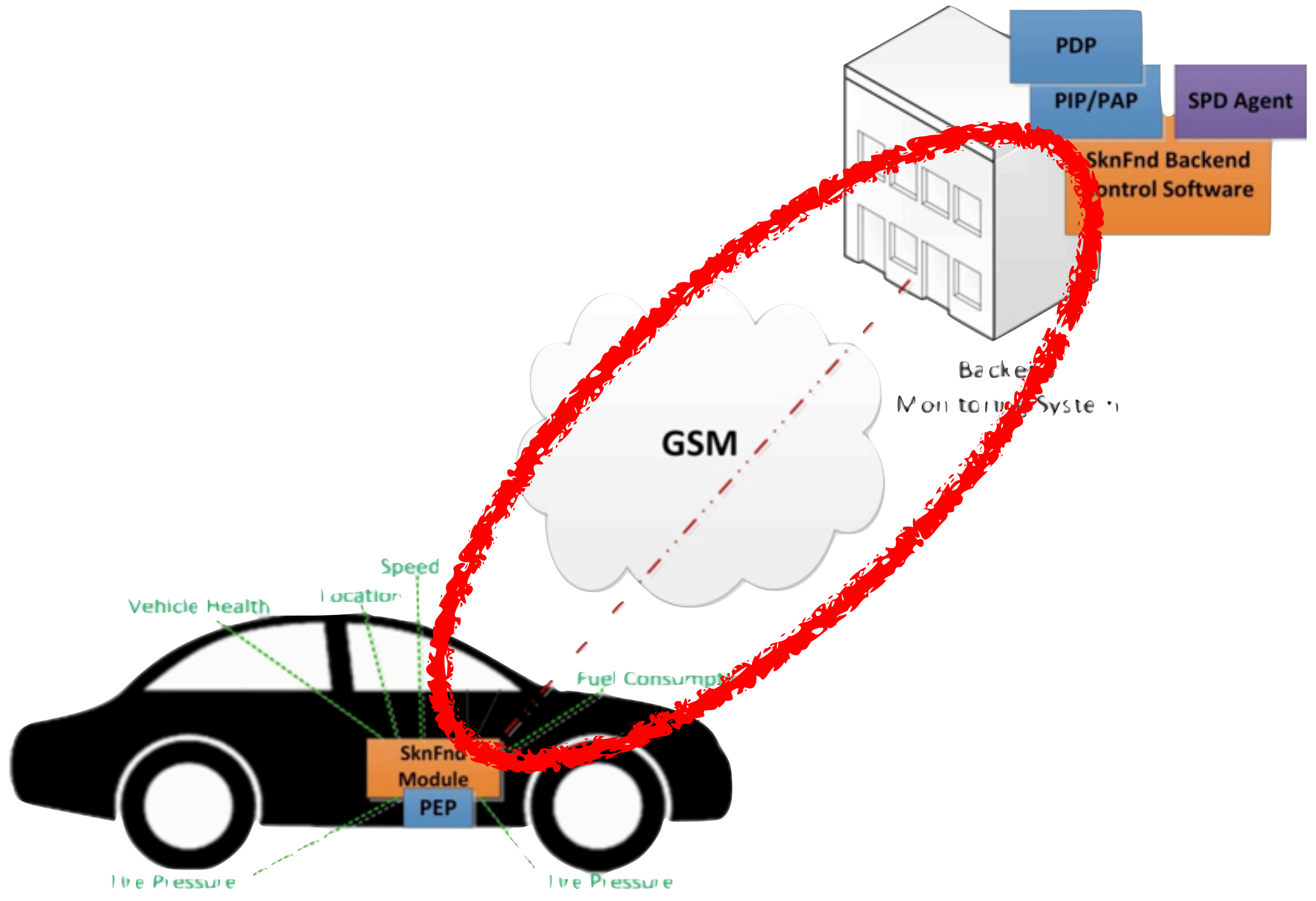
Multi-Metrics$_{v2}$ - system composition

- here: communication sub-system vehicle <-> backend
  - Port metric
  - Communication channel
  - GPRS message rate
  - SMS rate
  - Encryption



Configurations
Communication Subsystem

Scenario 1	*Conf. A*	*SSH*
"privacy"	*Conf. B*	*SSH + SNMP trap*
	Conf. C	*SSH + SNMP*
Scenario 2	*Conf. D*	*SSH + SNMP trap + SMS*
"parents"	*Conf. E*	*SSH + SNMP trap + SMS*
	Conf. F	*SSH + SNMP trap + SNMP + SMS*
Scenario 3	*Conf. G*	*SSH + SNMP trap + SMS*
"emergency"	*Conf. H*	*SSH + SNMP trap + SMS*
	Conf. I	*SSH + SNMP trap + SNMP + SMS*



Simple Network Management Protocol (SNMP) is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. [Wikipedia]
SNMP trap = alerts

Metrics & weight (only privacy)

1) Port metric, weight w_p=40

	Cp	SPDp
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

2) Communication channel metric, weight w_p=20

	Cp	*SPDp*
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 SPDp=90-100

3) GPRS message rate metric w_p=80

message delay	*Cp*	*SPDp*
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*

5) Encryption metric w_p=60

	Cp	*SPDp*
No encryption	*88*	*12*
Key 64 bits	*10*	*90*
Key 128 bits	*5*	*95*
Not applicable	*0*	*100*

Metrics analysis

		Metric 1	Metric 2	Metric 3	Metric 4	Sum	Cp	SPDp
Scenario 1 "privacy"	*Conf. A*	*232*	*52*	*0*	*10*	*294*	*17*	***83***
	Conf. B	***960***	*52*	*4*	*10*	*1 025*	*32*	*68*
	Conf. C	*434*	*52*	*18*	*10*	*513*	*23*	*77*
Scenario 2 "parents"	*Conf. D*	***1 735***	*217*	*1*	*39*	*1 992*	*45*	*55*
	Conf. E	*1 735*	*217*	*73*	*39*	*2 064*	*45*	*55*
	Conf. F	*1 778*	*217*	*165*	*39*	*2 198*	*47*	*53*
Scenario 3 "emergency "	*Conf. G*	*1 735*	*228*	*4*	*2 998*	*4 964*	*70*	*30*
	Conf. H	*1 735*	*228*	*361*	*2 998*	*5 322*	*73*	*27*
	Conf. I	***1 778***	*228*	*1 171*	***2 998***	*6 174*	*79*	***21***

sum of weight: 155

Multi-Metrics subsystem evaluation

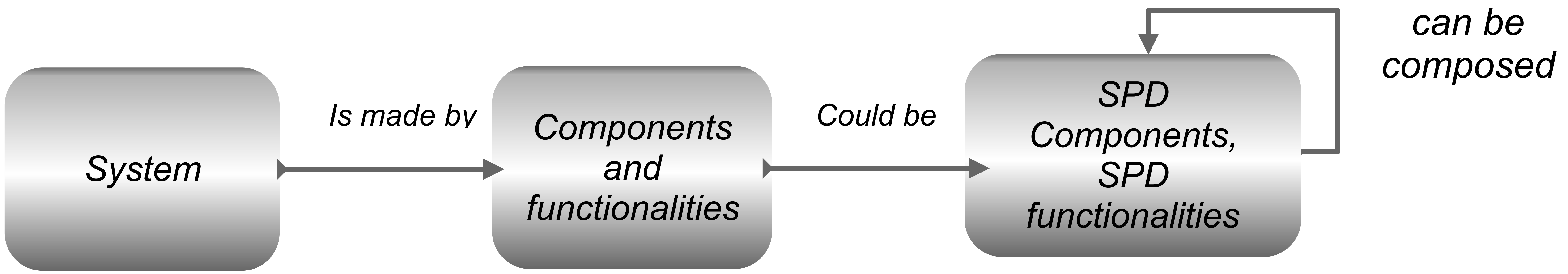
	Criticality					SPD_P			
	C1	C2	C3	C4	Sub-Sys.		Scen. 1	Scen. 2	Scen. 3
SPD_{Goal}							(s,80,d)	(s,50,d)	(s,5,d)
Multi-Metrics Elements	M1	M2	M3 ∩ M4	M5	C1... ∩ ...C4				
Conf. A	30	20	0	5	17	83	green	red	red
Conf. B	61	20	4	5	32	68	yellow	yellow	red
Conf. C	41	20	9	5	23	77	green	yellow	red
Conf. D	82	41	2	10	45	55	yellow	green	red
Conf. E	82	41	18	10	45	55	yellow	green	red
Conf. F	83	41	27	10	47	53	yellow	green	red
Conf. G	82	42	4	88	70	30	red	yellow	red
Conf. H	82	42	40	88	73	27	red	yellow	red
Conf. I	83	42	72	88	Alarm	21	red	yellow	yellow

Conclusions

- SHIELD is the security methodology developed through JU Artemis/ECSEL
- Security, Privacy, and Dependability (SPD) assessment
- Social Mobility Use-Case: loan a car
  - «behave» - full privacy awareness -> SPD_{goal} = (s,**80**,d)
  - «speeding» - limited privacy -> SPD_{goal} = (s,**50**,d)
  - «accident» - no privacy -> SPD_{goal} = (s,**5**,d)
- 11 configurations assessed
  - 2 satisfy «behave», 3 satisfy «speeding», 0 satisfies «accident»
- Goal: apply SHIELD methodology in various industrial domains

Upcoming lectures

- L11: perform Multi-Metrics for a Smart Meter (AMR)



- …. applying Multi-Metrics on your own