UNIK4750 - Measurable Security for the Internet of Things

L12 – Multi-Metrics Analysis

György Kálmán,
Mnemonic/NTNU/UiO ITS
gyorgy.kalman@its.uio.no

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

Overview

- Your project
- Recap: Security Ontologies (see L8)
- Use case (application) SocialMobility
- Values for Security, Privacy
- Analyze the system of systems
- Identify Security, Privacy attributes and functionality for a sub-system
- Multi-Metrics analysis
- Future work

UNIK4750: Lecture plan

- 19.01 L1: Introduction
- 26.01 L2: Internet of Things
- 02.02 L3: Security of IoT + Paper selection
- 09.02
  - L4: Smart Grid, Automatic Meter Readings
  - L5: Service implications on functional requirements
- 16.02
  - L6: Technology mapping
  - L7: Practical implementation of ontologies
- 23.02 ---- Vinterferie
- 02.03 L8-9: Paper analysis with 15 min presentation
- 09.03 L10-11: Paper analysis with 15 min presentation
- **16.03**
  - **L12: Multi-Metrics Method for measurable Security**
  - **L13: System Security and Privacy analysis, Intrusion Detecion**
- 23.03
  - L14: Real world examples, quest lecture
  - L15: Multi-Metrics Weighting of an AMR sub-system
- 30.03
  - ---- no lecture
- 06.04
  - L16: Real world IoT service evaluation group work
  - L17: Wrap-up of the course
- 13.04 ---- Påskeferie
- 20.04 ---- Exam

Expected Learning outcomes

Having followed the lecture, you can

- establish a scenario
- 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)

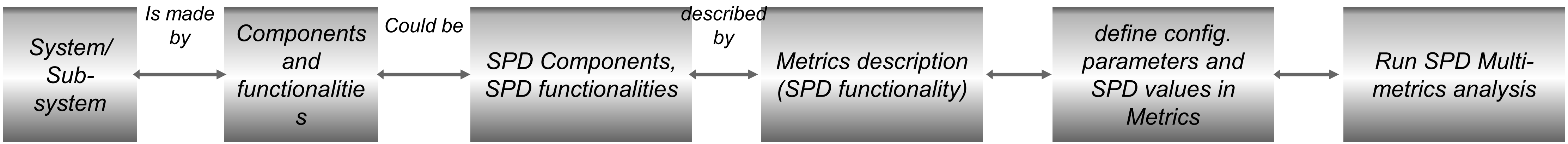
Thanks to our colleagues from SHIELD for the collaboration

nSHIELD

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

Feb2015

Methodology:
From System description to SPD level



System/ Sub-system

Is made by

Components and functionalities

Could be

SPD Components, SPD functionalities

described by

Metrics description (SPD functionality)

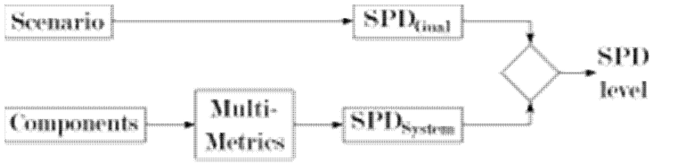
define config. parameters and SPD values in Metrics

Run SPD Multi-metrics analysis

- 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=?

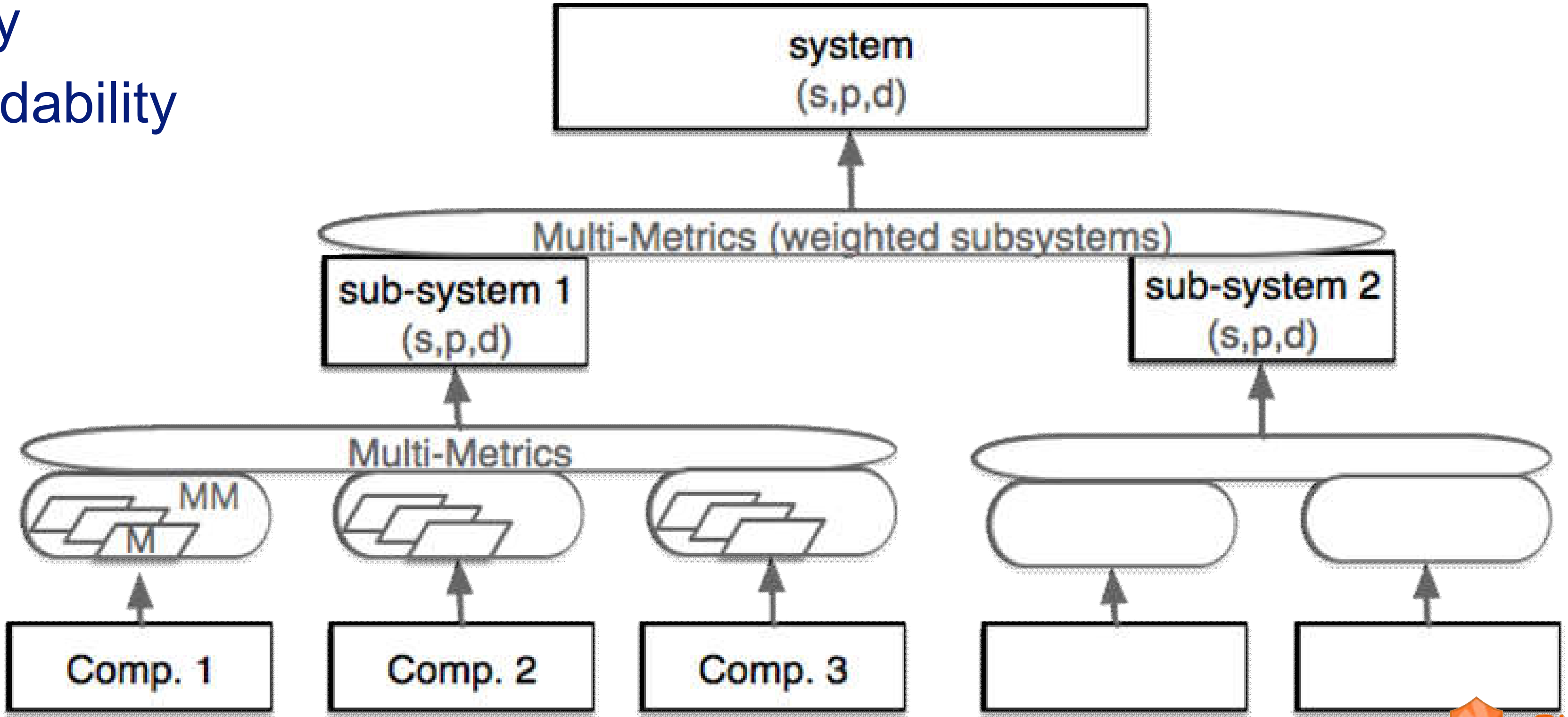
Social Mobility Main Focus

- Focus on the industrial market
- Identified challenges
  - industry «needs security» - with appropriate architectures
  - Communication module
  - Role-based access
  - Middleware
- System Security, Privacy and Dependability is assessed
- System$_{SPD}$
  is compared
  to Goals$_{SPD}$



Multi-Metrics - system composition

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



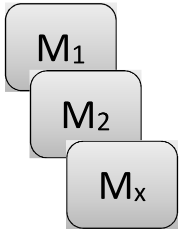
nSHIELD

SHIELD Multi Metrics Approach

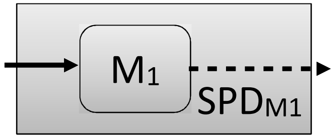
		SPD_{Goal}	SPD level	
Scenario 1	**Conf. A**	(s,80,d)	(s,100,d)	(s,🟡,d)
	Conf. B		(s,80,d)	(s,🟢,d)
	Conf. C		(s,80,d)	(s,🟢,d)

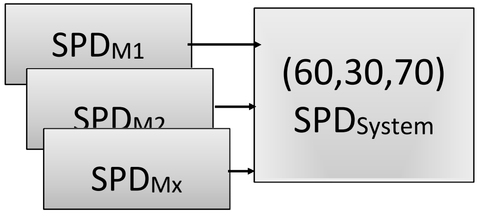
- Security, Privacy and Dependability
  - Specific application
  - Social Mobility: privacy scenario

- 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)

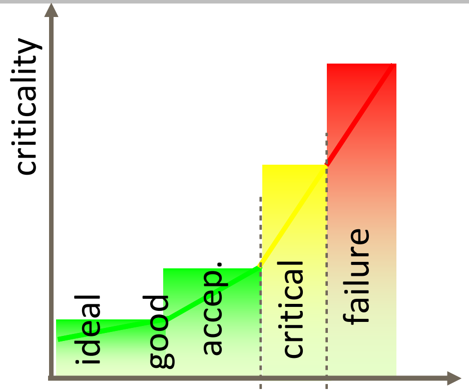


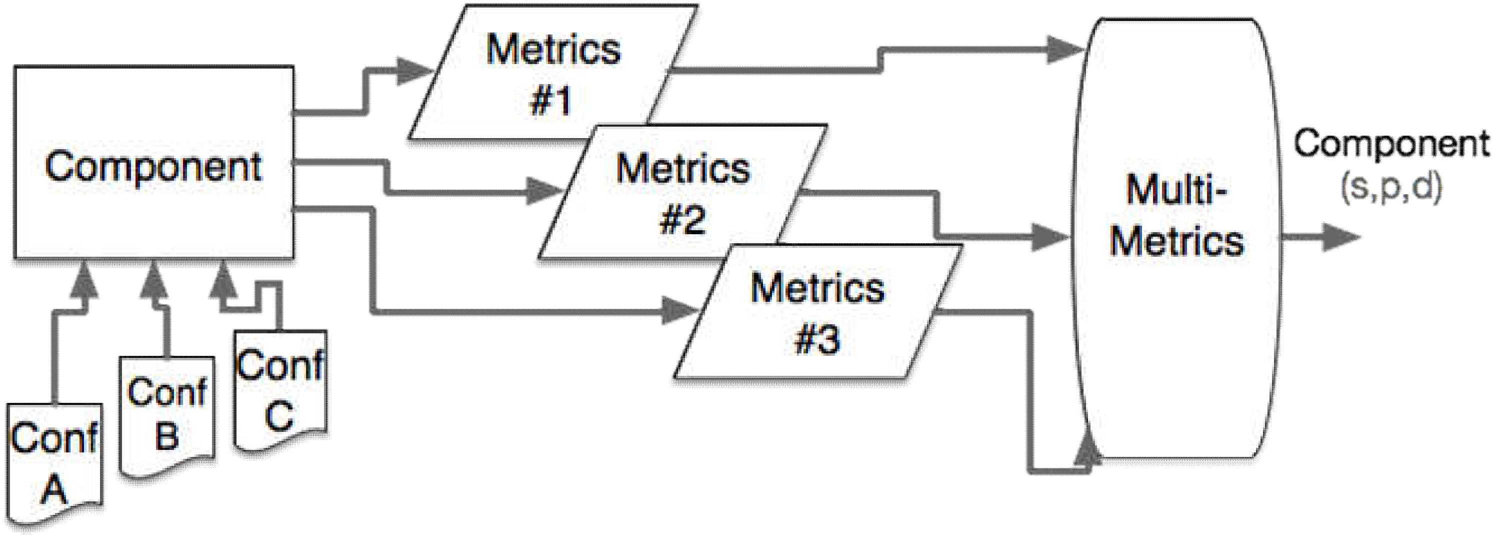


- Metrics combination to provide an SPD triplet: (60, 30, 70)

Multi-Metrics components

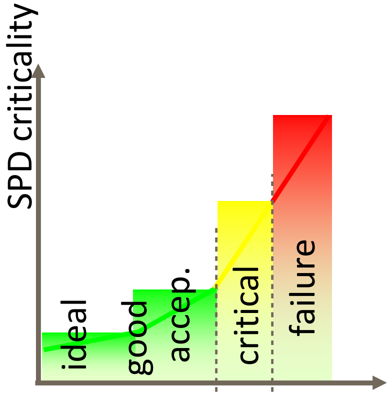
- Components have a security, privacy and dependability factor.
- Metrics assess the components



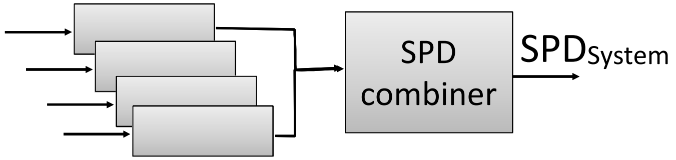


SHIELD Multi Metrics$_{v2}$

- 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

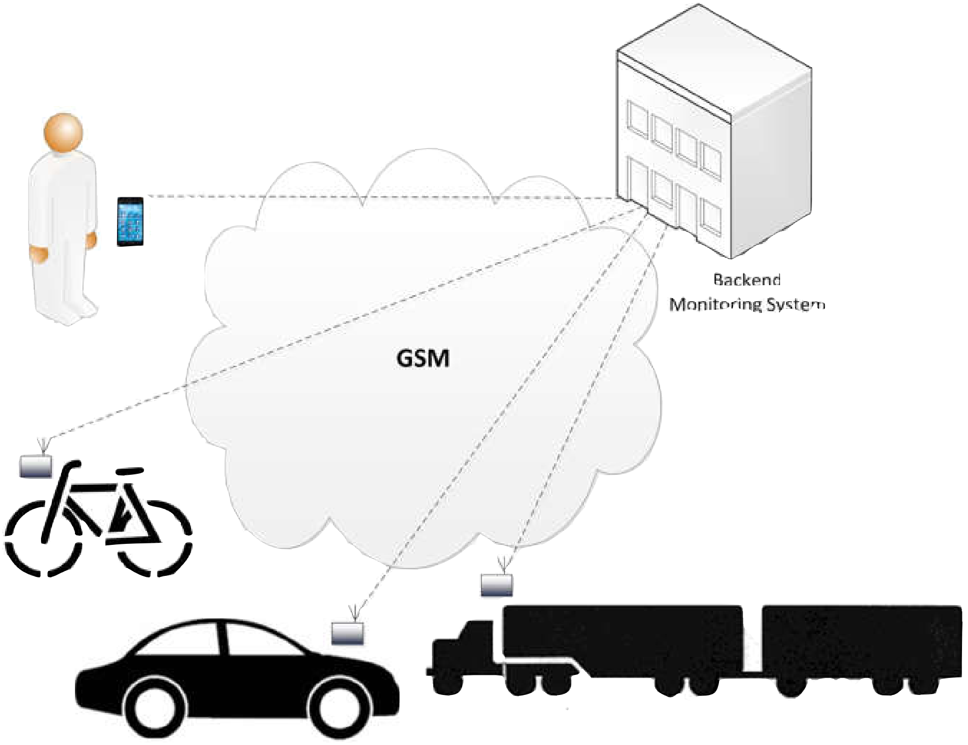


- Metrics combination to provide SPD_{System}: (60, 30, 70)
  - Mathematical combination, e.g. $S_{System}=100 - SQRT(S_1^2+S_2^2+\ldots S_x^2)$



Example:
Privacy in a Social Mobility Use Case

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



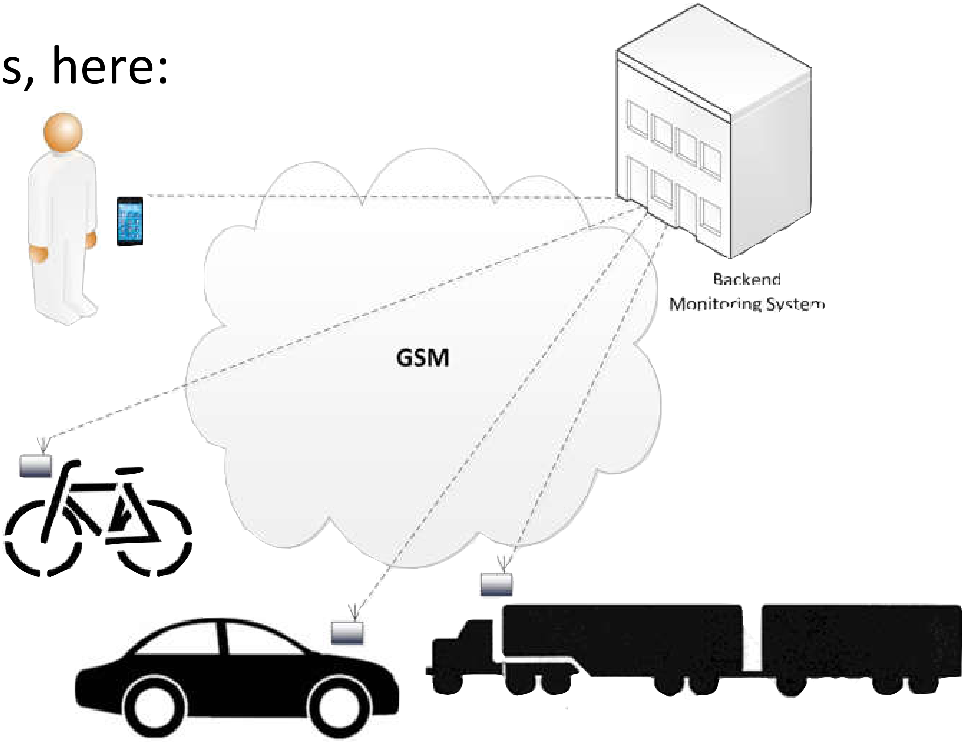
⑩ «User behaves»: privacy ensured

⑩ «User drives too fast»: track is visible

⑩ «Crash»:
emergency actions

Social Mobility Use Case

- Social Mobility, including social networks, here: loan of vehicle



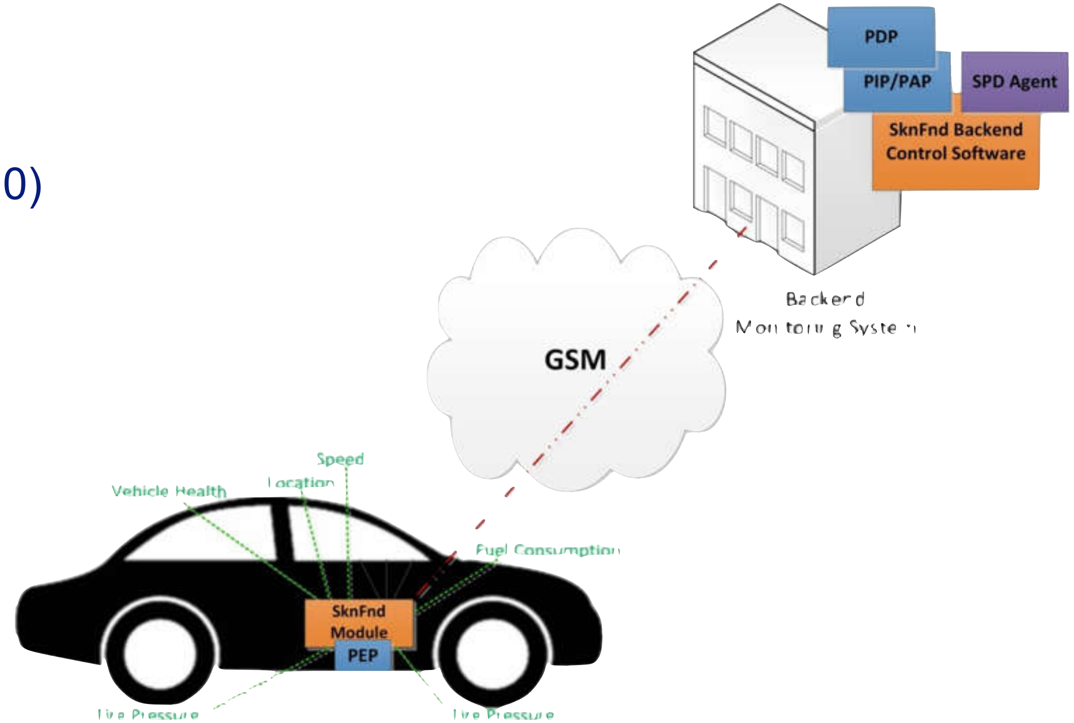
- Sc1: privacy ensured, «user behaves»
- Sc2: track is visible as user drives too fast
- Sc3: Crash, emergency actions

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

Social Mobility Components

Applicable nSHIELD Components (Px):

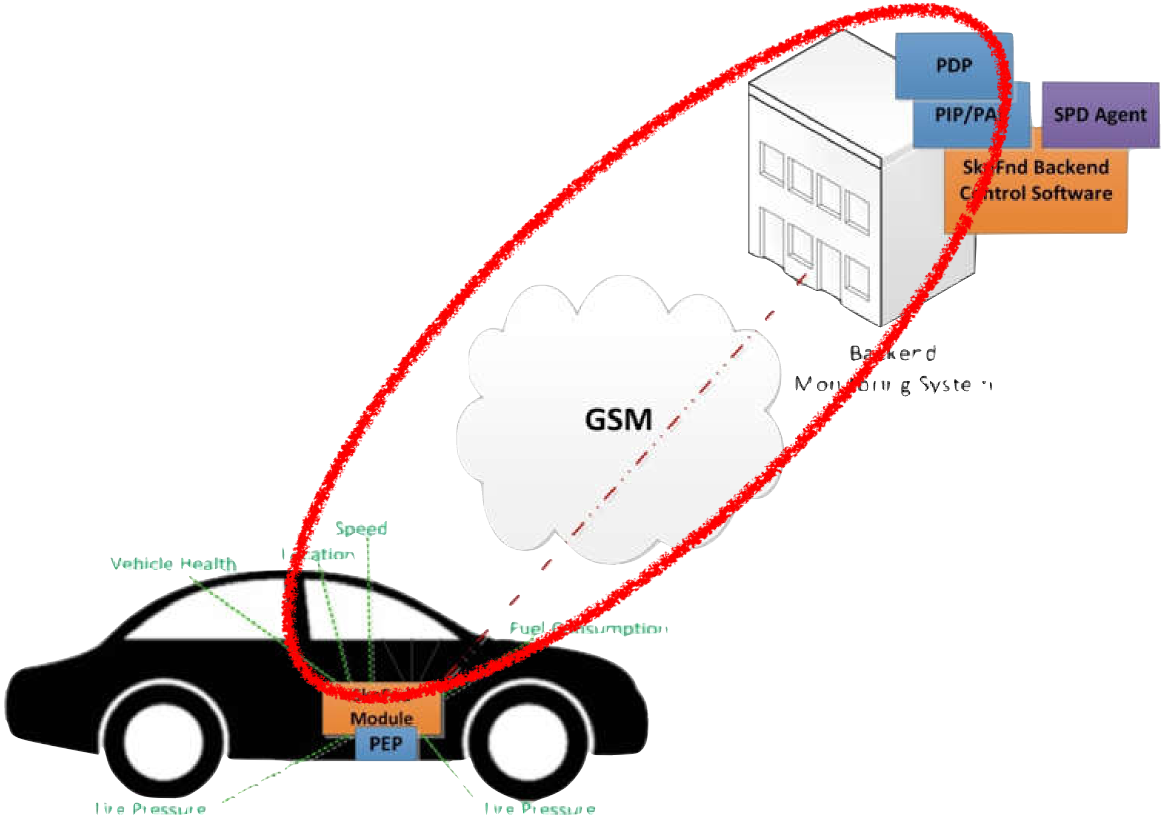
- 1- Lightweight Cyphering (P1)
- 2- Key exchange (P2)
- 3- Anonymity & Location Privacy (P10)
- 4- Automatic Access Control (P11)
- 5- Recognizing DoS Attack (P13)
- 6- Intrusion Detection System (P15)
- 7- Attack surface metrics (P28)
- 8- Embedded SIM, sensor (P38)
- 9- Multimetrics (P27)



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

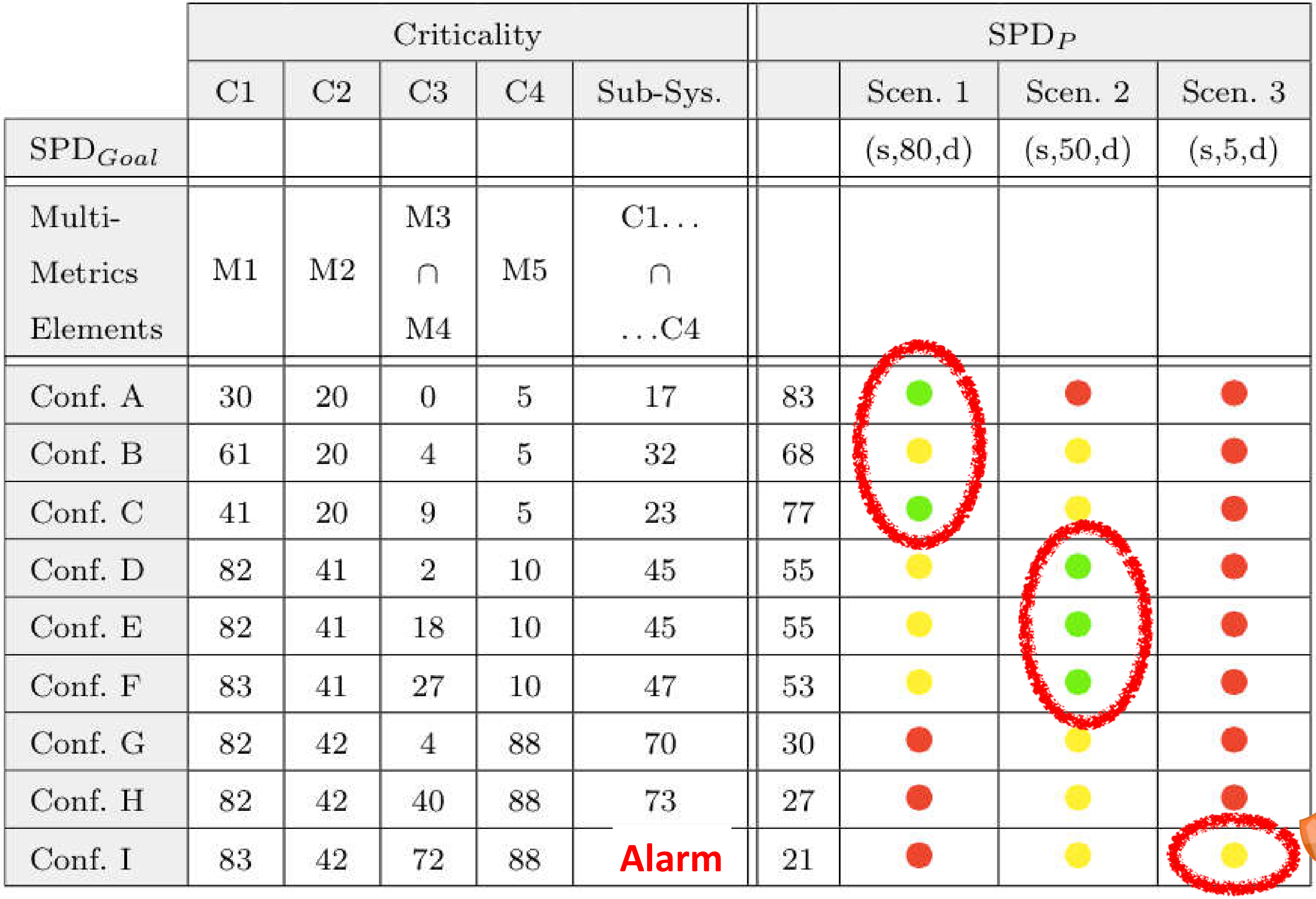
Parameter	No encryption	Key 64 bits	Key 128 bits	Not applicable
Cp	88	10	5	0

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

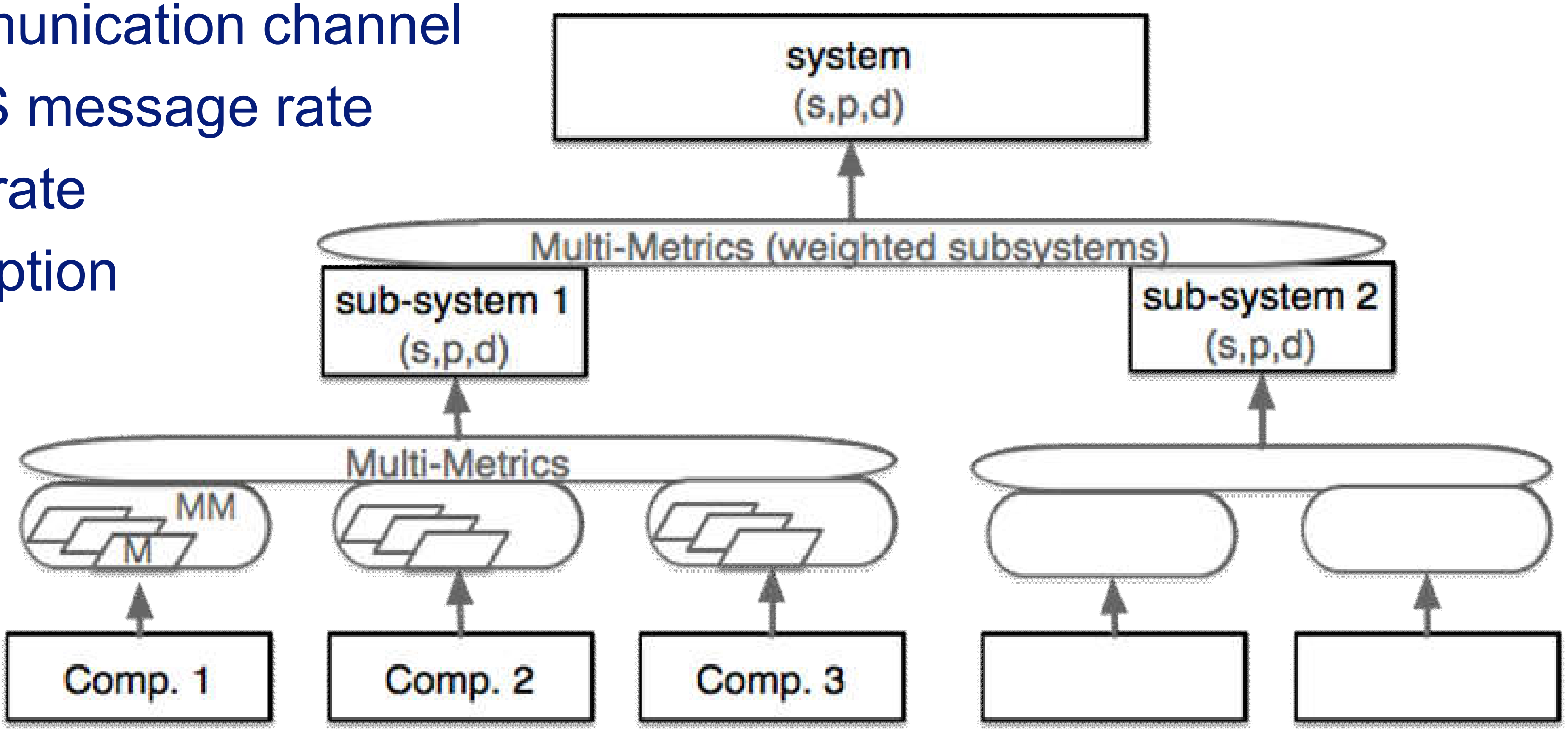


	Criticality					SPD_P			
	C1	C2	C3	C4	Sub-Sys.		Scen. 1	Scen. 2	Scen. 3
SPD_{Goal}							(s,80,d)	(s,50,d)	(s,5,d)
Multi- Metrics Elements	M1	M2	M3 $\cap$ M4	M5	C1. . . $\cap$ . . .C4				
Conf. A	30	20	0	5	17	83	🟢	🔴	🔴
Conf. B	61	20	4	5	32	68	🟡	🟡	🔴
Conf. C	41	20	9	5	23	77	🟢	🟡	🔴
Conf. D	82	41	2	10	45	55	🟡	🟢	🔴
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	🔴	🟡	🟡

Run-Through Example

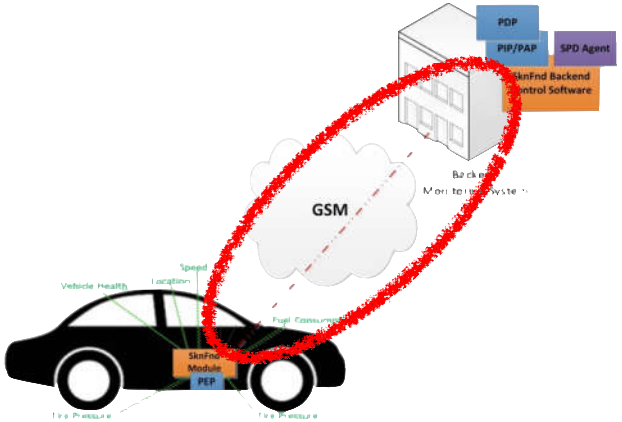
Multi-Metrics$_{v2}$ - system composition

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



Configurations
Communication Subsystem

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

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

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*

2) Communication channel metric, weight w_p=20

	Cp	*SPDp*
GPRS with GEA/3	*20*	*80*
SMS over GSM with A5/1	*40*	*60*

3) GPRS message rate metric w_p=80

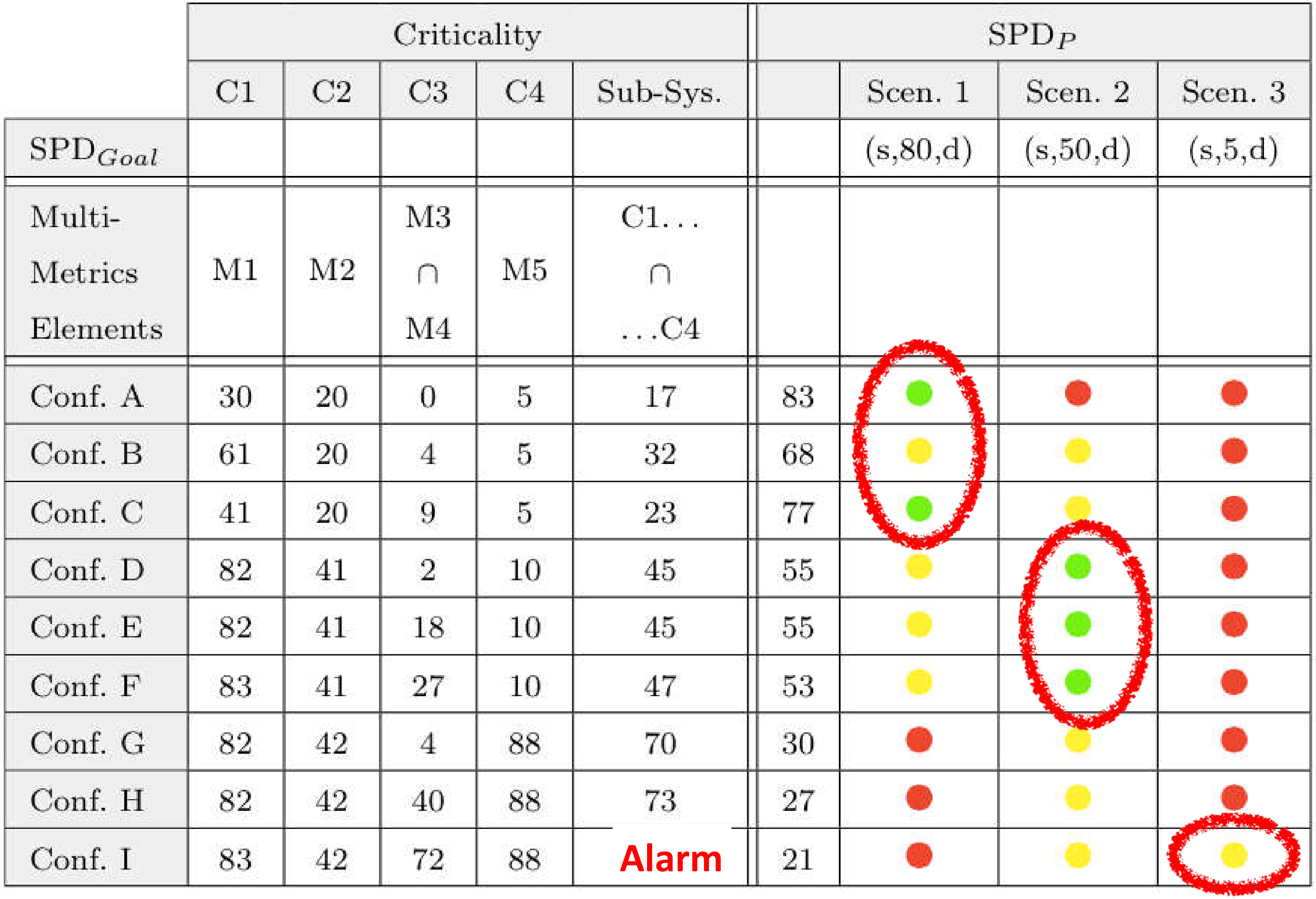
message delay	*Cp*	*SPDp*
0.5 sec	*80*	*20*
1 sec	*60*	*40*
2 sec	*45*	*65*
5 sec	*30*	*70*
10 sec	*20*	*80*
20 sec	*15*	*85*
60 sec	*10*	*90*
120 sec	*5*	*95*

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 $\cap$ M4	M5	C1… $\cap$ …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	🔴	🟡	🟡

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 -> S**P**D$_{goal}$ = (s,**80**,d)
  - «speeding» - limited privacy -> S**P**D$_{goal}$ = (s,**50**,d)
  - «accident» - no privacy -> S**P**D$_{goal}$ = (s,**5**,d)
- 11 configurations assessed
  - 2 satisfy «behave», 3 satisfy «speeding», 0 satisfies «accident»
- Goal: apply SHIELD methodology in various industrial domains