The Risk Situation Awareness Provision Capability and its Degradation in the Überlingen Accident Over Time

Maria Mikela CHATZIMICHAILIDOU

Research Associate, Engineering Design Centre

University of Cambridge, UK

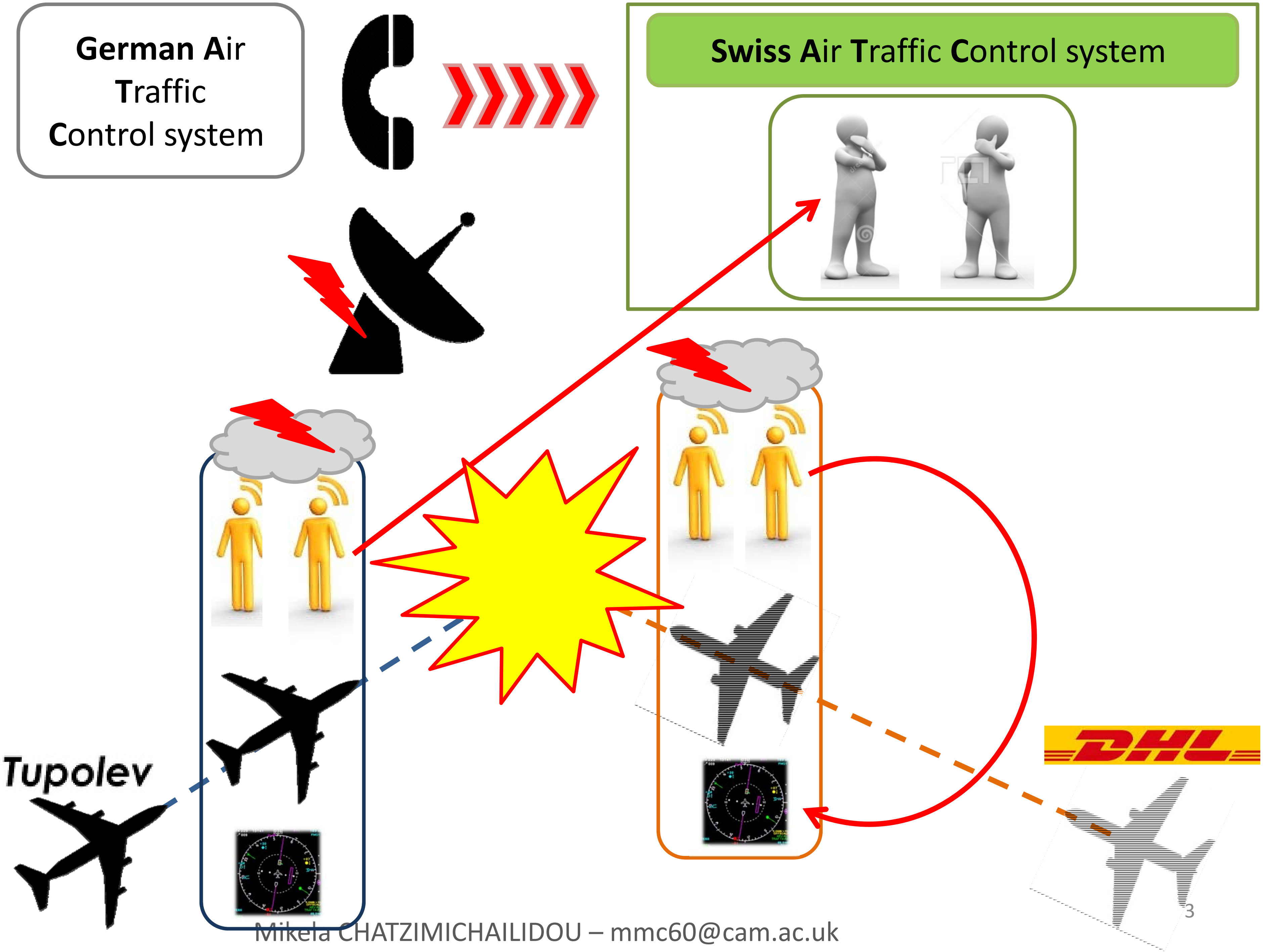
Ioannis DOKAS

Assistant Professor, Department of Civil Engineering

Democritus University of Thrace, Greece

Starting from the end..

The *Überlingen* mid-air collision accident



German Air Traffic Control system

Swiss Air Traffic Control system

Contributing factors

- Violated control actions and safety constraints

- Technical, human services & information content (partly) lost during the development of the accident

- “Systemic causes” (BFU 2002; Johnson 2004); combined events
  - Downgraded STCA: provided the ATC with auditory alarm; no visual warning
  - “Single Manned Operation”: no distribution of workload; ATC’s distraction

‘Erosion’ of system’s composition & capabilities

- Inadequate or missing system elements not acknowledged, replaced, or fixed

  → safety *“drift”* (Dekker 2012)

- BFU (2002): *“The staffing level **eroded** the system’s defenses, particularly in a time of **degraded** technical **system capability***.”*

‘erosion’ of the system’s composition → negative impact on system **capabilities*** & on safety

The **Risk** **S**ituati**O**n **A**wareness **P**rovision **(RiskSOAP)** capability*

Definition and theory

RiskSOAP; **inherent capability*** of each system part to **provide its agent(s) with support for enhancing their SA** in terms of the presence of system **threats and vulnerabilities** that may possibly lead to accidents

- The RiskSOAP capability is **hinted at** by:
  a. accident investigation reports (e.g. BFU 2002; Johnson 2004) &
  b. outstanding researchers in the field of SA (e.g. Stanton et al. 2010)

but.. **either hard to be described in words – or simply considered as identical to SA,**

but.. **RiskSOAP capability ≠ SA**

Scope of research

The Implication: There is a relationship & a **positive correlation between the RiskSOAP capability & safety**

The Question: *Is the RiskSOAP capability quantifiable?*

✗ Existing SA measurement techniques inadequate

✓ **RiskSOAP methodology & indicator**

The Answer: Apply the **STAMP-based RiskSOAP indicator** throughout an **accident's timeline** to demonstrate the degradation of the RiskSOAP capability

♦ milestones [t-1, t, t+1, t+2]

The 2 direct findings

1. Degradation of the RiskSOAP capability over time in alignment to the milestones on the accident timeline – as revealed by the calculated value of the RiskSOAP indicator

2. Deterioration of the RiskSOAP indicator attributed to

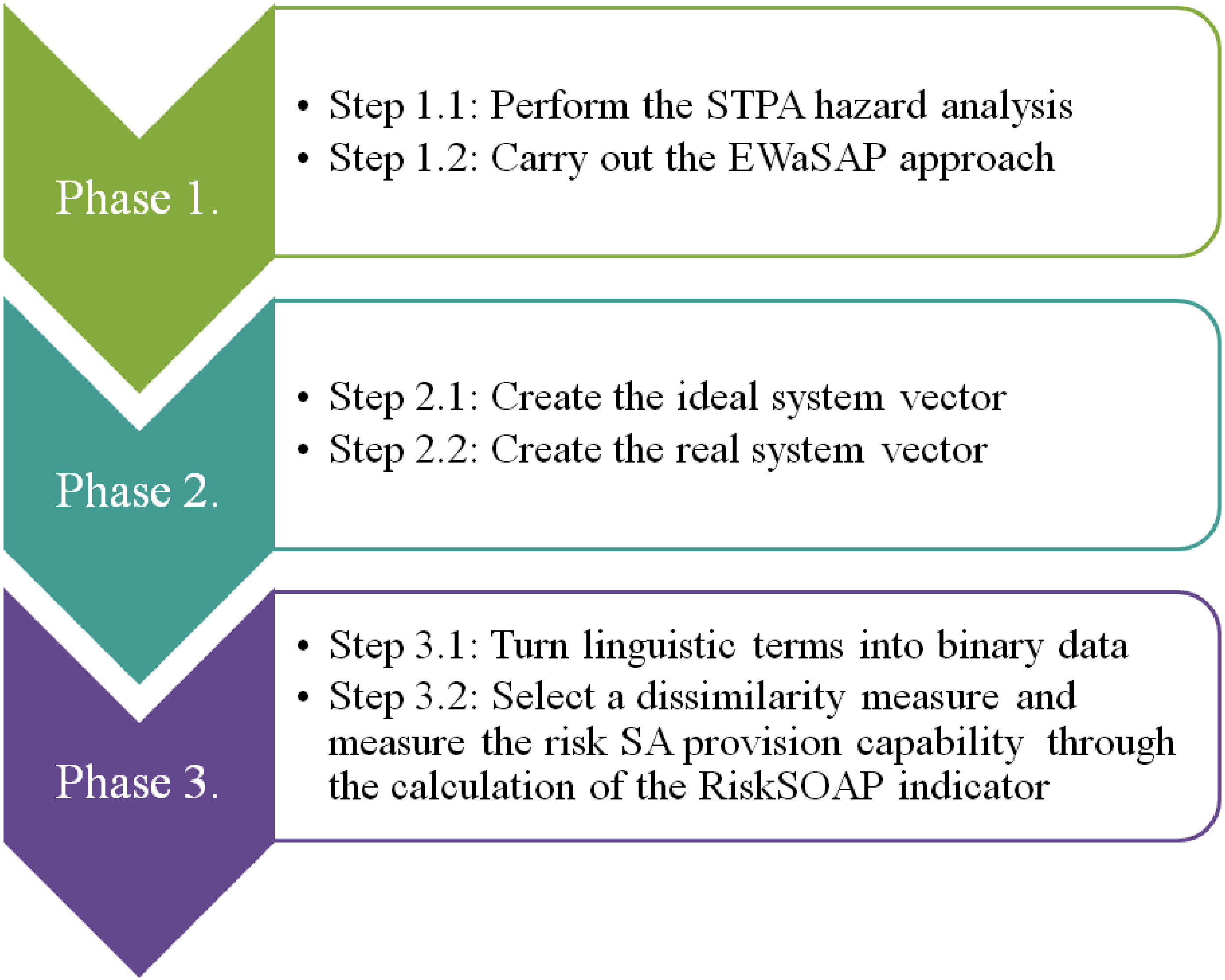
   (a) the absence or malfunction of specific system elements

   (b) and their interactions, as well as the

   (c) presence of flaws through which accident scenarios are verified and, in turn, the system is headed for an accident

The RiskSOAP methodology

The process



Phase 1.

- Step 1.1: Perform the STPA hazard analysis
- Step 1.2: Carry out the EWaSAP approach

Phase 2.

- Step 2.1: Create the ideal system vector
- Step 2.2: Create the real system vector

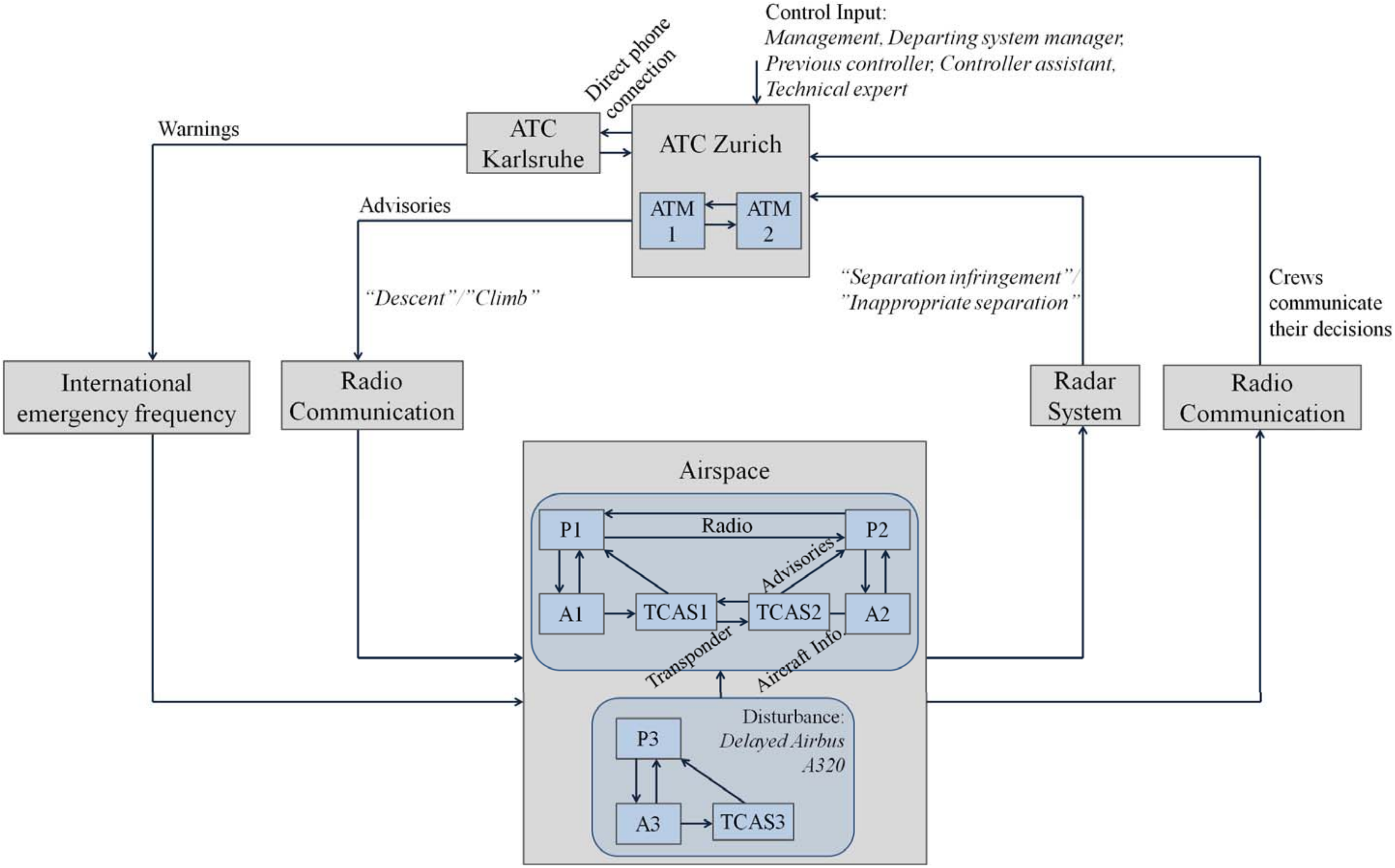
Phase 3.

- Step 3.1: Turn linguistic terms into binary data
- Step 3.2: Select a dissimilarity measure and measure the risk SA provision capability through the calculation of the RiskSOAP indicator

Analysis of the Überlingen case

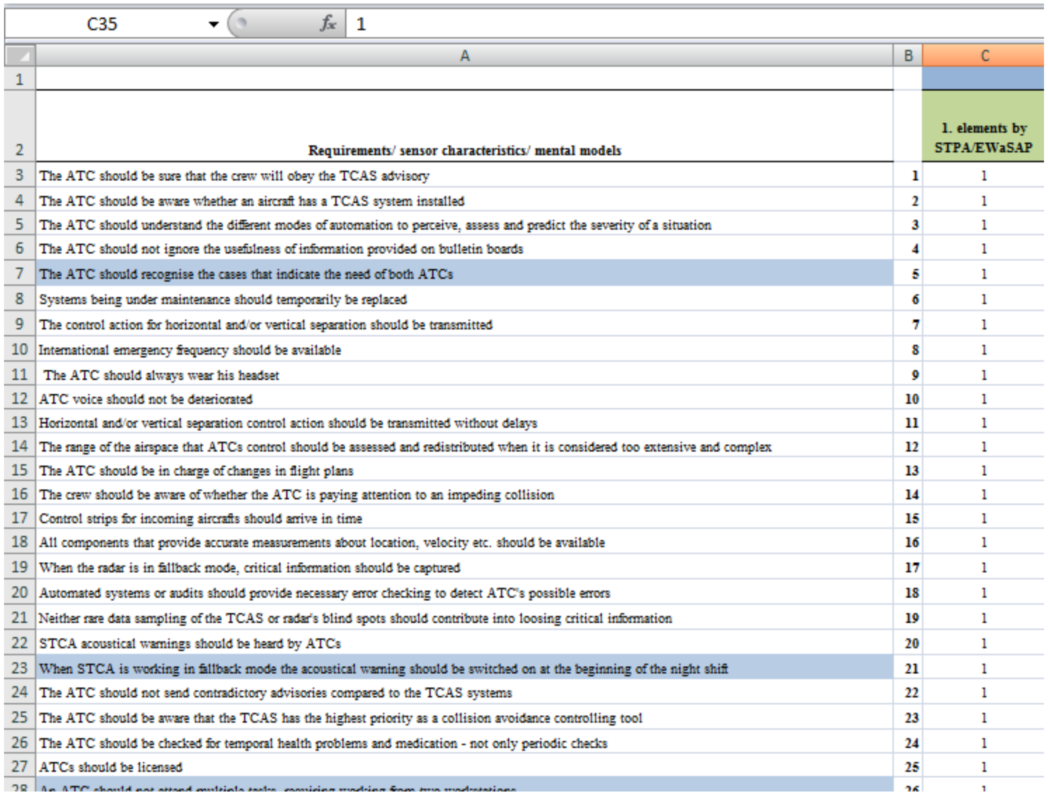
Accident: *Loss of human life due to aircraft collision*
Hazard: *A pair of controlled aircraft violate minimum separation standards*

Safety control structure

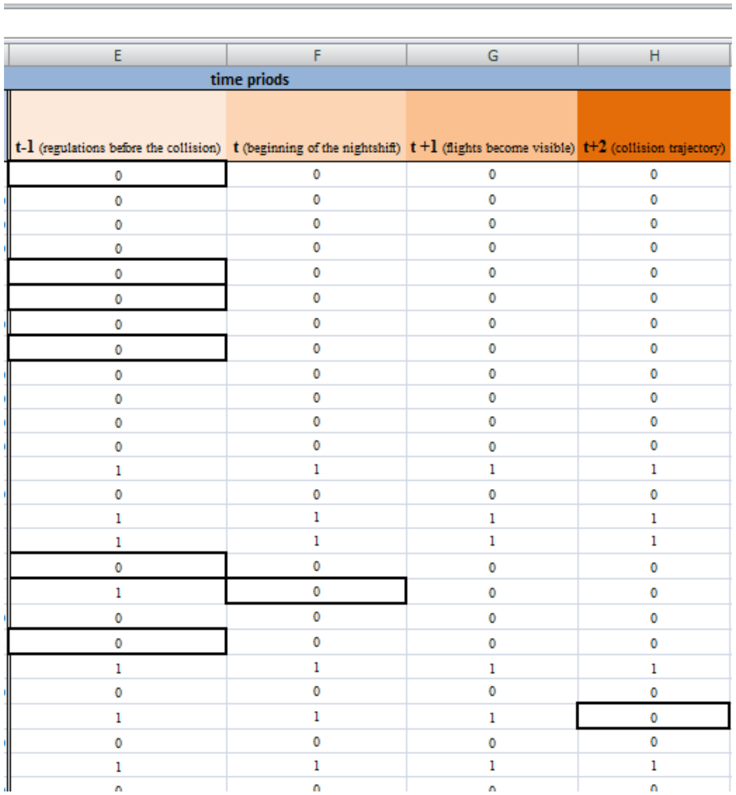

Control Input:
Management, Departing system manager, Previous controller, Controller assistant, Technical expert
Direct phone connection
ATC Karlsruhe
ATC Zurich
ATM 1
ATM 2
Warnings
Advisories
"Descent"/"Climb"
"Separation infringement"/ "Inappropriate separation"
Crews communicate their decisions
International emergency frequency
Radio Communication
Radar System
Radio Communication
Airspace
P1
Radio
P2
Advisories
A1
TCAS1
TCAS2
A2
Transponder
Aircraft Info
Disturbance: Delayed Airbus A320
P3
A3
TCAS3

Safety requirements

ideal . . . *1* *2* *3* *4*

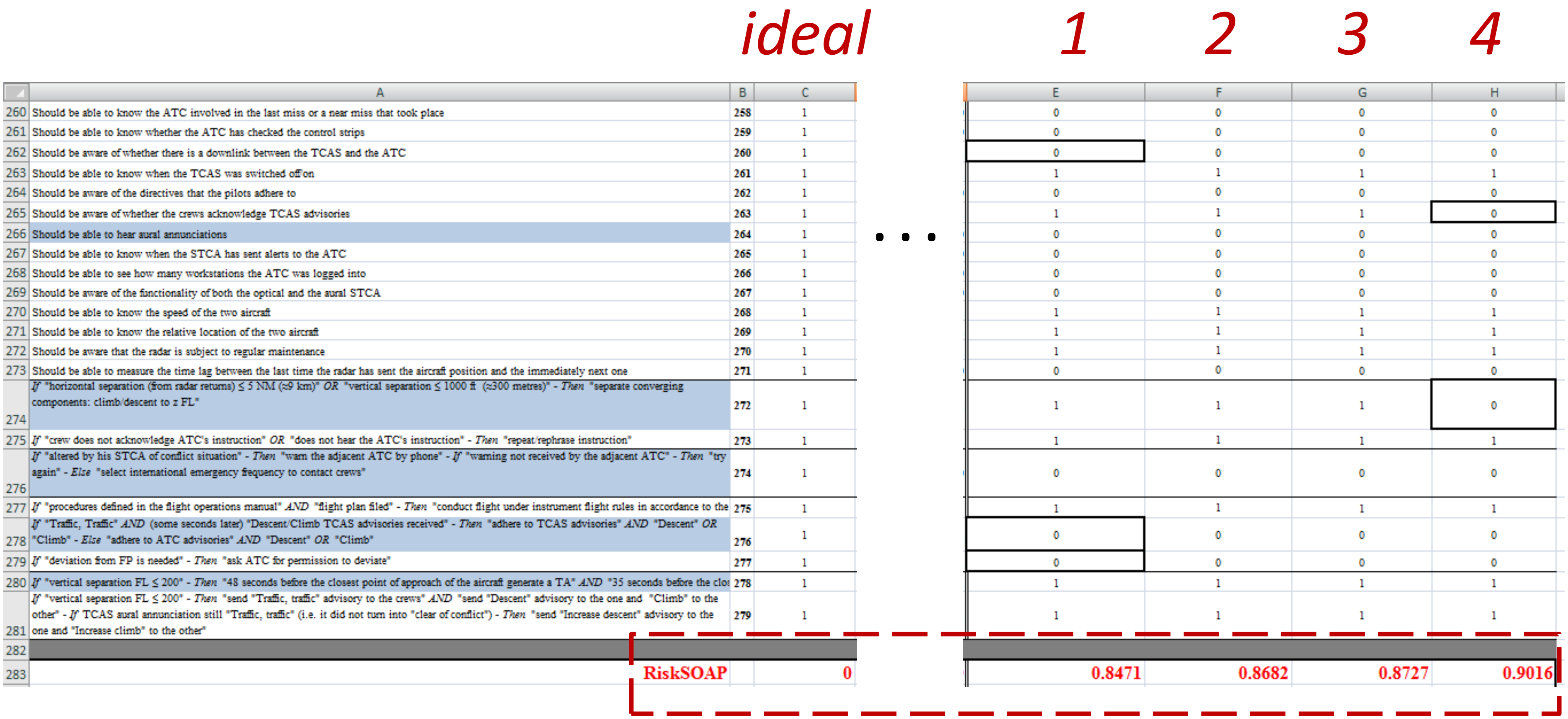


C35 fx 1



	A	B	C	E	F	G	H
1				time priods			
2	Requirements/ sensor characteristics/ mental models		1. elements by STPA/EWaSAP	t-1 (regulations before the collision)	t (beginning of the nightshift)	t +1 (flights become visible)	t+2 (collision trajectory)
3	The ATC should be sure that the crew will obey the TCAS advisory	1	1	0	0	0	0
4	The ATC should be aware whether an aircraft has a TCAS system installed	2	1	0	0	0	0
5	The ATC should understand the different modes of automation to perceive, assess and predict the severity of a situation	3	1	0	0	0	0
6	The ATC should not ignore the usefulness of information provided on bulletin boards	4	1	0	0	0	0
7	The ATC should recognise the cases that indicate the need of both ATCs	5	1	0	0	0	0
8	Systems being under maintenance should temporarily be replaced	6	1	0	0	0	0
9	The control action for horizontal and/or vertical separation should be transmitted	7	1	0	0	0	0
10	International emergency frequency should be available	8	1	0	0	0	0
11	The ATC should always wear his headset	9	1	0	0	0	0
12	ATC voice should not be deteriorated	10	1	0	0	0	0
13	Horizontal and/or vertical separation control action should be transmitted without delays	11	1	0	0	0	0
14	The range of the airspace that ATCs control should be assessed and redistributed when it is considered too extensive and complex	12	1	0	0	0	0
15	The ATC should be in charge of changes in flight plans	13	1	1	1	1	1
16	The crew should be aware of whether the ATC is paying attention to an impeding collision	14	1	0	0	0	0
17	Control strips for incoming aircrafts should arrive in time	15	1	1	1	1	1
18	All components that provide accurate measurements about location, velocity etc. should be available	16	1	1	1	1	1
19	When the radar is in fallback mode, critical information should be captured	17	1	0	0	0	0
20	Automated systems or audits should provide necessary error checking to detect ATC's possible errors	18	1	1	0	0	0
21	Neither rare data sampling of the TCAS or radar's blind spots should contribute into loosing critical information	19	1	0	0	0	0
22	STCA acoustical warnings should be heard by ATCs	20	1	0	0	0	0
23	When STCA is working in fallback mode the acoustical warning should be switched on at the beginning of the night shift	21	1	1	1	1	1
24	The ATC should not send contradictory advisories compared to the TCAS systems	22	1	0	0	0	0
25	The ATC should be aware that the TCAS has the highest priority as a collision avoidance controlling tool	23	1	1	1	1	0
26	The ATC should be checked for temporal health problems and medication - not only periodic checks	24	1	0	0	0	0
27	ATCs should be licensed	25	1	1	1	1	1
28	An ATC should not attend multiple tasks, requiring working from two workstations	26	1	0	0	0	0

Sensor characteristics & control algorithms

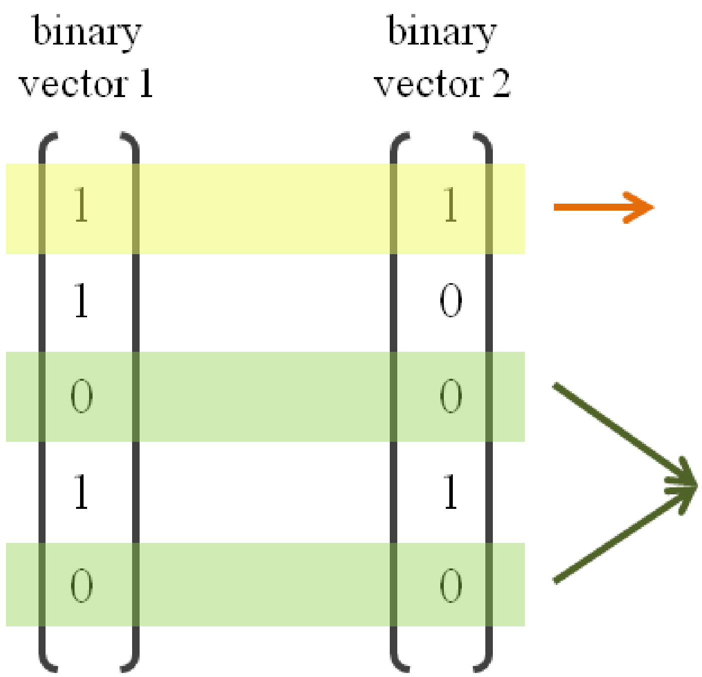


			ideal		*1*	*2*	*3*	*4*
	A	B	C		E	F	G	H
260	Should be able to know the ATC involved in the last miss or a near miss that took place	258	1		0	0	0	0
261	Should be able to know whether the ATC has checked the control strips	259	1		0	0	0	0
262	Should be aware of whether there is a downlink between the TCAS and the ATC	260	1		0	0	0	0
263	Should be able to know when the TCAS was switched off/on	261	1		1	1	1	1
264	Should be aware of the directives that the pilots adhere to	262	1		0	0	0	0
265	Should be aware of whether the crews acknowledge TCAS advisories	263	1		1	1	1	0
266	Should be able to hear aural annunciations	264	1	. . .	0	0	0	0
267	Should be able to know when the STCA has sent alerts to the ATC	265	1		0	0	0	0
268	Should be able to see how many workstations the ATC was logged into	266	1		0	0	0	0
269	Should be aware of the functionality of both the optical and the aural STCA	267	1		0	0	0	0
270	Should be able to know the speed of the two aircraft	268	1		1	1	1	1
271	Should be able to know the relative location of the two aircraft	269	1		1	1	1	1
272	Should be aware that the radar is subject to regular maintenance	270	1		1	1	1	1
273	Should be able to measure the time lag between the last time the radar has sent the aircraft position and the immediately next one	271	1		0	0	0	0
274	*If* "horizontal separation (from radar returns) ≤ 5 NM (≈9 km)" *OR* "vertical separation ≤ 1000 ft (≈300 metres)" - *Then* "separate converging components: climb/descent to z FL"	272	1		1	1	1	0
275	*If* "crew does not acknowledge ATC's instruction" *OR* "does not hear the ATC's instruction" - *Then* "repeat/rephrase instruction"	273	1		1	1	1	1
276	*If* "altered by his STCA of conflict situation" - *Then* "warn the adjacent ATC by phone" - *If* "warning not received by the adjacent ATC" - *Then* "try again" - *Else* "select international emergency frequency to contact crews"	274	1		0	0	0	0
277	*If* "procedures defined in the flight operations manual" *AND* "flight plan filed" - *Then* "conduct flight under instrument flight rules in accordance to the	275	1		1	1	1	1
278	*If* "Traffic, Traffic" *AND* (some seconds later) "Descent/Climb TCAS advisories received" - *Then* "adhere to TCAS advisories" *AND* "Descent" *OR* "Climb" - *Else* "adhere to ATC advisories" *AND* "Descent" *OR* "Climb"	276	1		0	0	0	0
279	*If* "deviation from FP is needed" - *Then* "ask ATC for permission to deviate"	277	1		0	0	0	0
280	*If* "vertical separation FL ≤ 200" - *Then* "48 seconds before the closest point of approach of the aircraft generate a TA" *AND* "35 seconds before the clos	278	1		1	1	1	1
281	*If* "vertical separation FL ≤ 200" - *Then* "send "Traffic, traffic" advisory to the crews" *AND* "send "Descent" advisory to the one and "Climb" to the other" - *If* TCAS aural annunciation still "Traffic, traffic" (i.e. it did not turn into "clear of conflict") - *Then* "send "Increase descent" advisory to the one and "Increase climb" to the other"	279	1		1	1	1	1
282								
283	**RiskSOAP**		**0**		**0.8471**	**0.8682**	**0.8727**	**0.9016**

Binary data & Rogers-Tanimoto calculation

Checklist
(point of reference: ‘ideal’ system)

Present → 1
Absent → 0



binary vector 1	binary vector 2
1	1
1	0
0	0
1	1
0	0

Examples of:

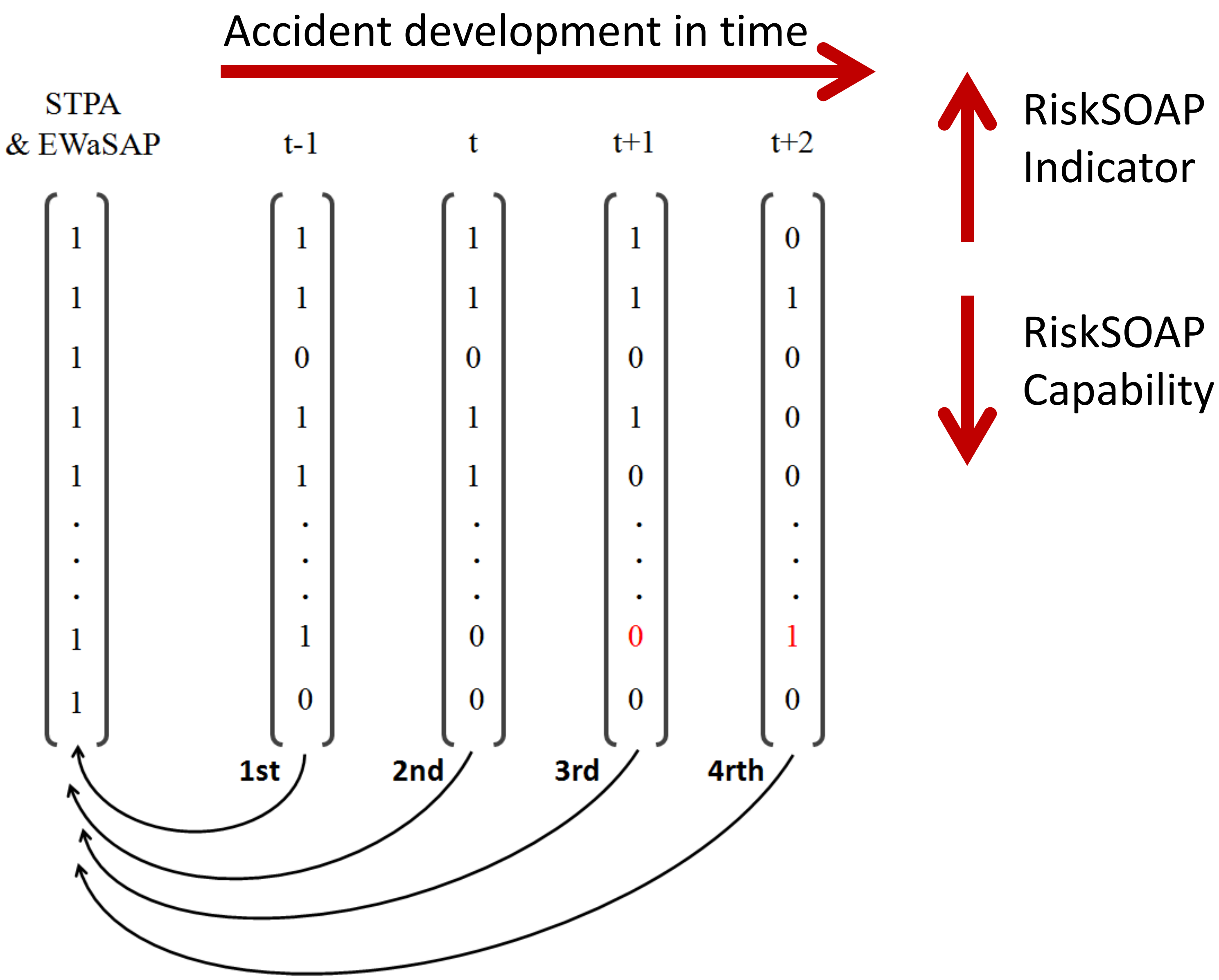
a ‘pair’ of binary integers:
pair = (1,1)

the total number of a specific ‘pair’:
$S(0,0) = 2$

$$\mathrm{RTd}(i, r) = \frac{2S10 + 2S01}{S11 + S00 + 2S10 + 2S01}$$

x 4 time-points/ milestones

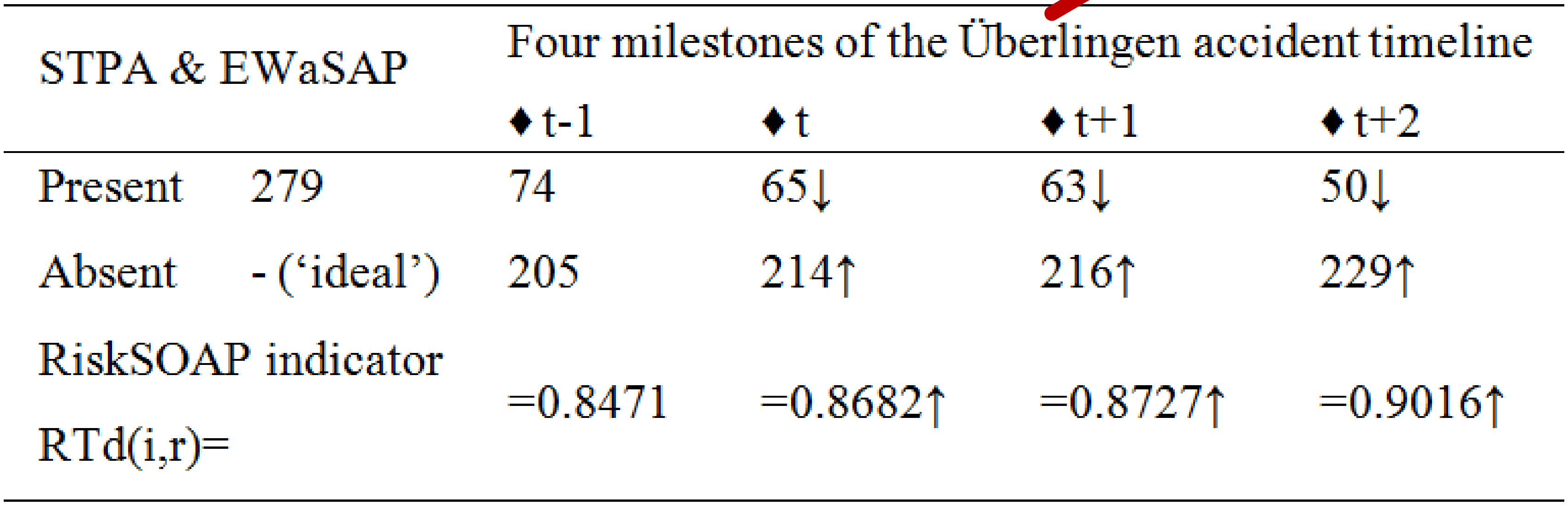
Compared vectors



$$\begin{array}{ccccc}
\text{STPA \& EWaSAP} & \text{t-1} & \text{t} & \text{t+1} & \text{t+2} \\
\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ \vdots \\ 1 \\ 1 \end{bmatrix} &
\begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ \vdots \\ 1 \\ 0 \end{bmatrix} &
\begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ \vdots \\ 0 \\ 0 \end{bmatrix} &
\begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix} &
\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{bmatrix}
\end{array}$$

RiskSOAP capability degradation - in numbers

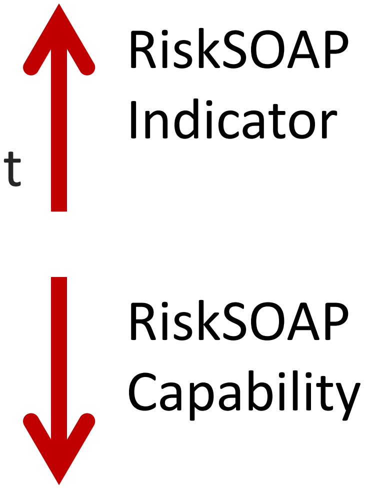
Accident development in time



STPA & EWaSAP		Four milestones of the Überlingen accident timeline			
		♦ t-1	♦ t	♦ t+1	♦ t+2
Present	279	74	65↓	63↓	50↓
Absent	- (‘ideal’)	205	214↑	216↑	229↑
RiskSOAP indicator RTd(i,r)=		=0.8471	=0.8682↑	=0.8727↑	=0.9016↑

Presence/absence of system elements mapped 4 times:

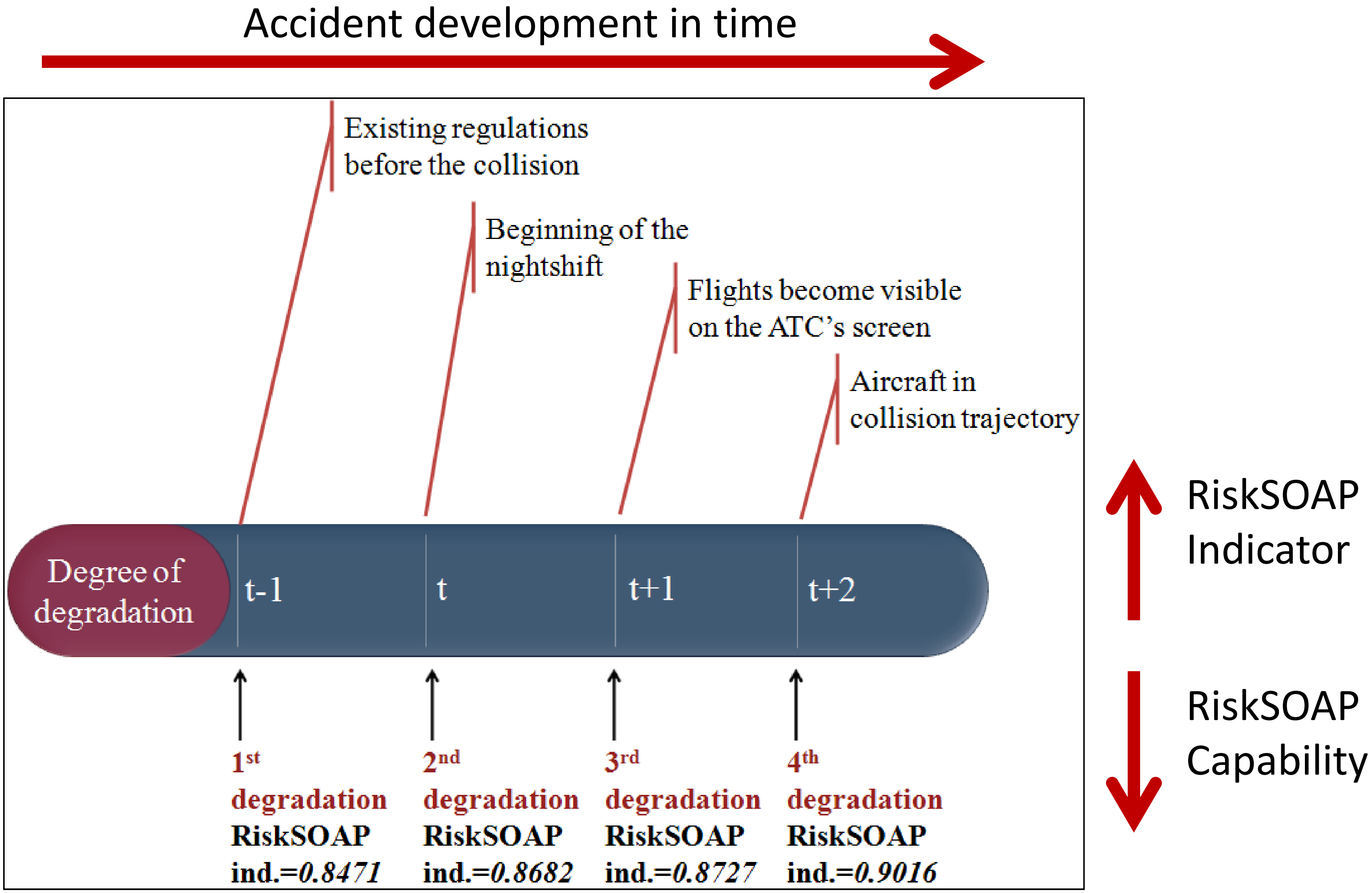
- *t-1* system’s composition; regulations before the accident
- *t* when the nightshift begins
- *t+1* conflicting flights become visible on radar
- *t+2* two aircraft are in collision trajectory



RiskSOAP Indicator

RiskSOAP Capability

Accident timeline & RiskSOAP indicator



Accident development in time

Existing regulations before the collision

Beginning of the nightshift

Flights become visible on the ATC's screen

Aircraft in collision trajectory

Degree of degradation

t-1

t

t+1

t+2

1st degradation RiskSOAP ind.=*0.8471*

2nd degradation RiskSOAP ind.=*0.8682*

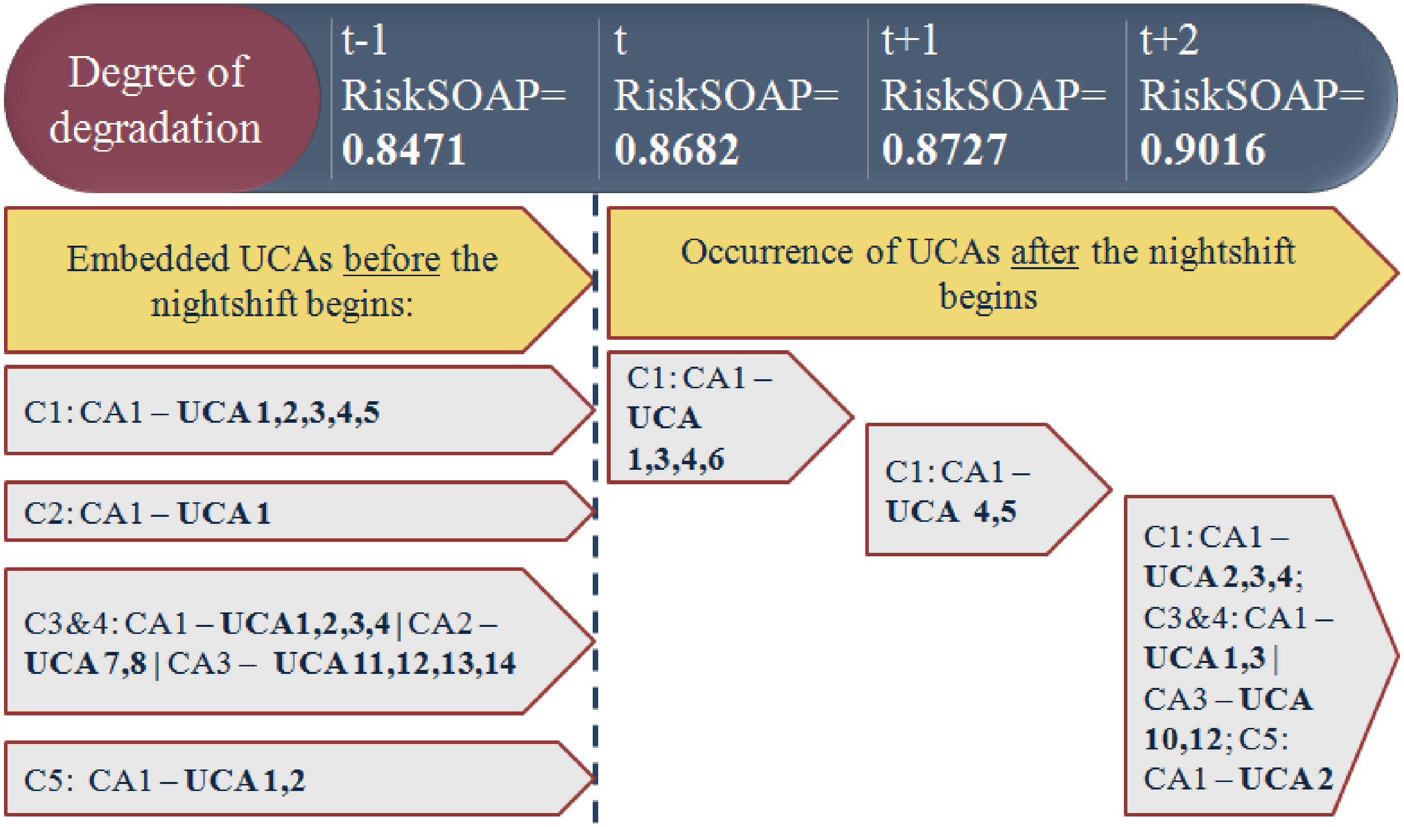
3rd degradation RiskSOAP ind.=*0.8727*

4th degradation RiskSOAP ind.=*0.9016*

RiskSOAP Indicator

RiskSOAP Capability

Accident scenarios verified 1/3



Degree of degradation

t-1 RiskSOAP= **0.8471**

t RiskSOAP= **0.8682**

t+1 RiskSOAP= **0.8727**

t+2 RiskSOAP= **0.9016**

Embedded UCAs before the nightshift begins:

C1: CA1 – **UCA 1,2,3,4,5**

C2: CA1 – **UCA 1**

C3&4: CA1 – **UCA1,2,3,4** | CA2 – **UCA 7,8** | CA3 – **UCA 11,12,13,14**

C5: CA1 – **UCA 1,2**

Occurrence of UCAs after the nightshift begins

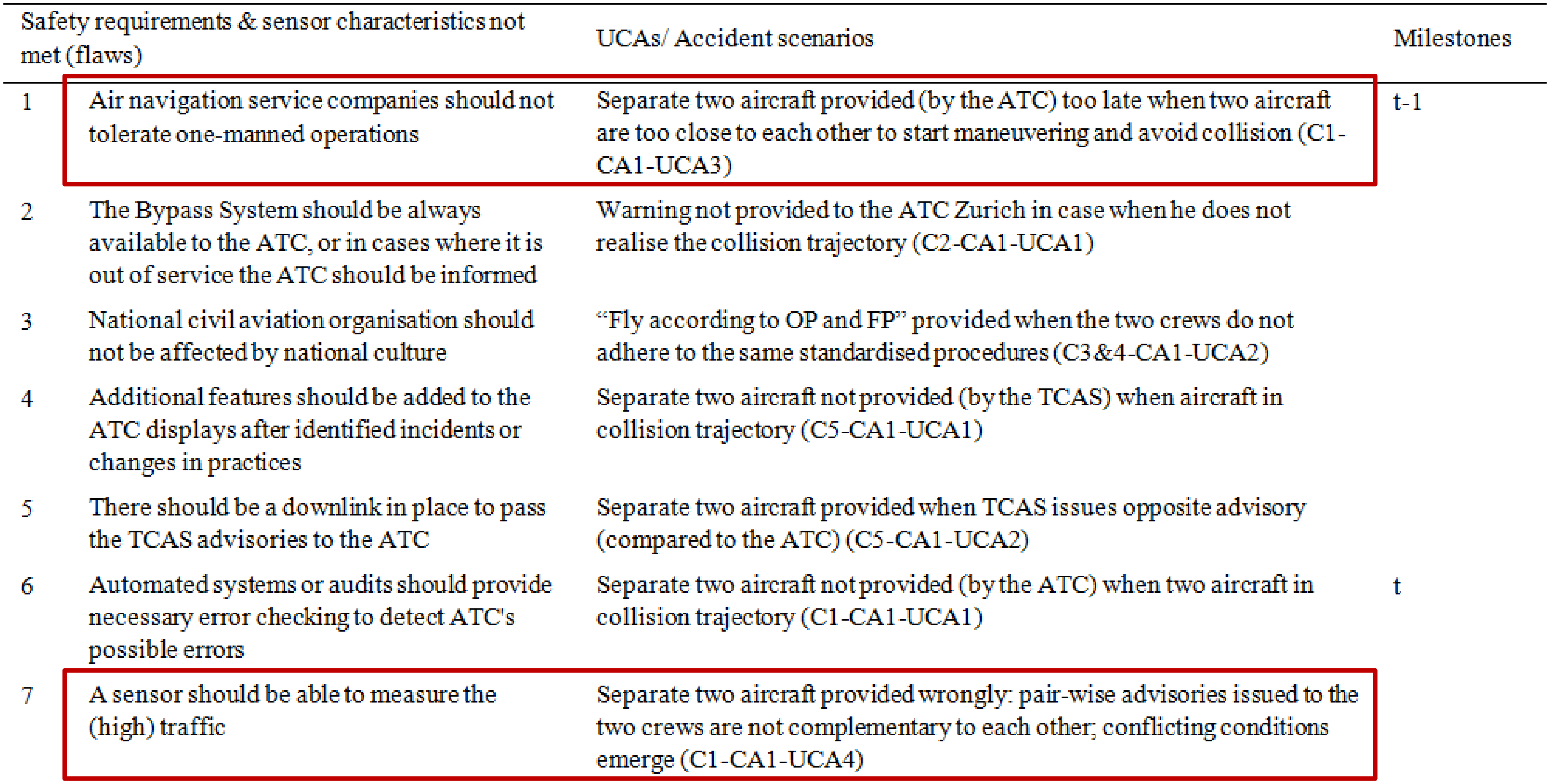
C1: CA1 – **UCA 1,3,4,6**

C1: CA1 – **UCA 4,5**

C1: CA1 – **UCA 2,3,4;** C3&4: CA1 – **UCA 1,3** | CA3 – **UCA 10,12;** C5: CA1 – **UCA 2**

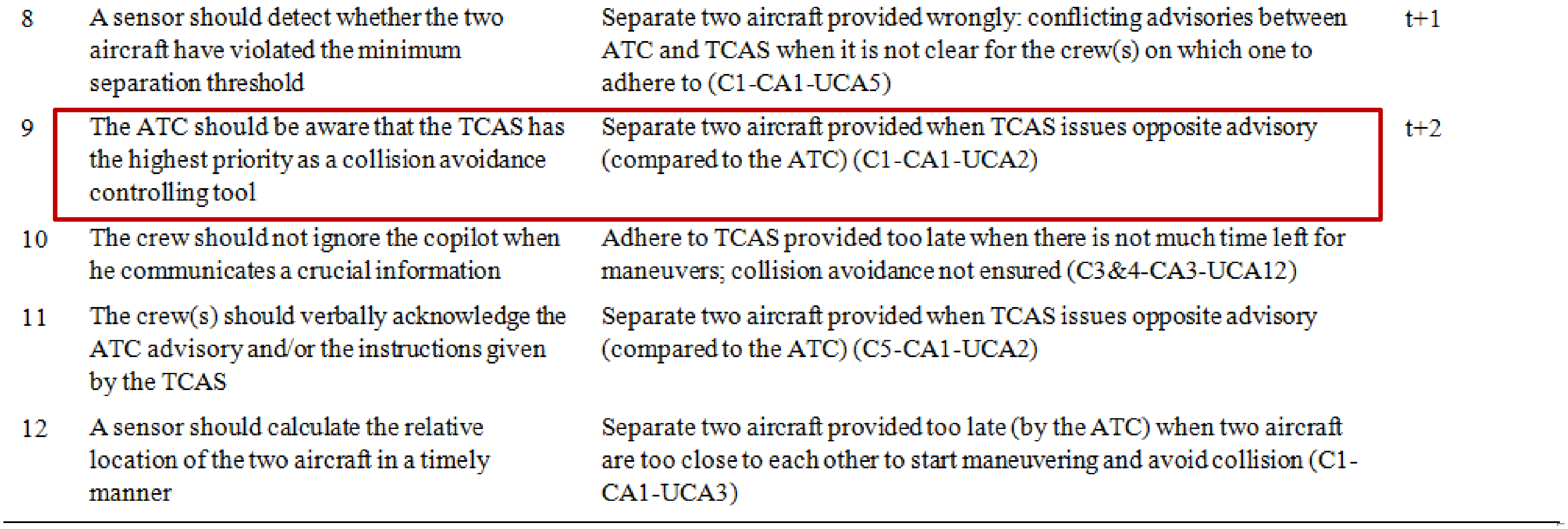
- **RiskSOAP** indicator gets **worse** → system headed for **accident**
- presence of **flaws** → group flaws →UCAs
- (real) **accident scenarios** verified

Accident scenarios verified 2/3



	Safety requirements & sensor characteristics not met (flaws)	UCAs/ Accident scenarios	Milestones
1	Air navigation service companies should not tolerate one-manned operations	Separate two aircraft provided (by the ATC) too late when two aircraft are too close to each other to start maneuvering and avoid collision (C1-CA1-UCA3)	t-1
2	The Bypass System should be always available to the ATC, or in cases where it is out of service the ATC should be informed	Warning not provided to the ATC Zurich in case when he does not realise the collision trajectory (C2-CA1-UCA1)	
3	National civil aviation organisation should not be affected by national culture	"Fly according to OP and FP" provided when the two crews do not adhere to the same standardised procedures (C3&4-CA1-UCA2)	
4	Additional features should be added to the ATC displays after identified incidents or changes in practices	Separate two aircraft not provided (by the TCAS) when aircraft in collision trajectory (C5-CA1-UCA1)	
5	There should be a downlink in place to pass the TCAS advisories to the ATC	Separate two aircraft provided when TCAS issues opposite advisory (compared to the ATC) (C5-CA1-UCA2)	
6	Automated systems or audits should provide necessary error checking to detect ATC's possible errors	Separate two aircraft not provided (by the ATC) when two aircraft in collision trajectory (C1-CA1-UCA1)	t
7	A sensor should be able to measure the (high) traffic	Separate two aircraft provided wrongly: pair-wise advisories issued to the two crews are not complementary to each other; conflicting conditions emerge (C1-CA1-UCA4)	

Accident scenarios verified 3/3



8	A sensor should detect whether the two aircraft have violated the minimum separation threshold	Separate two aircraft provided wrongly: conflicting advisories between ATC and TCAS when it is not clear for the crew(s) on which one to adhere to (C1-CA1-UCA5)	t+1
9	The ATC should be aware that the TCAS has the highest priority as a collision avoidance controlling tool	Separate two aircraft provided when TCAS issues opposite advisory (compared to the ATC) (C1-CA1-UCA2)	t+2
10	The crew should not ignore the copilot when he communicates a crucial information	Adhere to TCAS provided too late when there is not much time left for maneuvers; collision avoidance not ensured (C3&4-CA3-UCA12)	
11	The crew(s) should verbally acknowledge the ATC advisory and/or the instructions given by the TCAS	Separate two aircraft provided when TCAS issues opposite advisory (compared to the ATC) (C5-CA1-UCA2)	
12	A sensor should calculate the relative location of the two aircraft in a timely manner	Separate two aircraft provided too late (by the ATC) when two aircraft are too close to each other to start maneuvering and avoid collision (C1-CA1-UCA3)	

Every time the value of the RiskSOAP indicator was calculated (↑), the accident scenarios (which in reality lead to the examined accident) were verified → primary results suggest the **positive correlation between safety and the RiskSOAP capability**

Final remarks

- Exploratory research **towards** providing evidence of the **positive correlation** between the RiskSOAP **capability & safety**
- BFU (2002): **deterioration & loss of system elements**, along with violated control actions and safety constraints cause **safety drift**
- **Degraded** RiskSOAP **capability**; a **contributing factor** in Überlingen
- STAMP-based RiskSOAP indicator throughout the Überlingen timeline → **demonstration & quantitative description** of the degradation of the RiskSOAP capability
- **Dynamic** RiskSOAP capability: fluctuates in value across time, due to changes in safety specifications & short- or long-term conditions

Thank you!

Dankuwel!

Contact:

mmc60@cam.ac.uk

mikelachatzimichailidou@gmail.com