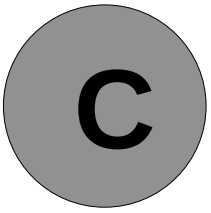

APPENDIX C:

EXAMPLES OF SAFETY OBJECTIVE CLASSIFICATION SCHEME

1 ATCC BUILDING QUANTITATIVE SAFETY OBJECTIVE CLASSIFICATION SCHEME

Quantitative frequency classes are based on the following criteria:

- First a TLS (Target Level of Safety) has to be set for ATCC (Air Traffic Control Center) system;
- Then this TLS has to be derived to set quantitative Safety Objective per severity class for each single hazard;
- For Severity Class 1, ESARR4 sets a TLS (Target Level of Safety) for the overall ATM direct contribution to accident of 1.55×10^{-8} per flight-hour;
- The approximate air traffic volume in the airspace in year 2000 was of 102.400 flight-hours (+/- 10%);
- ESARR4 traffic evolution was considered (+6.7 % per year till 2015);
- A conservative approach was to consider 2015 TLS (as required by ESARR4) as applicable to the ATCC design as the building is supposed to be operated at that time;
- A conservative approach was to allocate entirely Airspace TLS to the ATCC, as no mitigation means were considered as acceptable (so the tolerable frequency of occurrence of the effect is fully allocated to the safety objective of the hazard);
- An order of magnitude of 1 has been considered for severity classes 2 and 3 and of 2 for severity class 4 (as it seems to be a domain characteristic to have a lot of low severity events). Order of magnitude 2 means 10^{-2}, order of magnitude 1 means 10^{-1} ;
- A maximum of 10 (ten) hazards having an end effect severity of Class 1 can be identified (this analysis has found 8);
- A conservative approach was to consider as 1 the probability (Pe) that once a hazard occurs, then the worst credible effect occurs too;
- The quantitative safety objectives unit will be per operational hour.

Consequently, the TLS for the ATCC is: 5.27×10^{-7} /h

$1.55 \times 10^{-8} \times 102400 \times 1.1 \times (1.067)^{15} = 4.62 \times 10^{-3}$ per year

So 1 accident every 216.5 years. As 1 year = 365.25*24 = 8766 hours

4.62×10^{-3} /Year = 5.27×10^{-7} /hour

From this TLS, quantitative objectives can be derived **per hazard** having an end effect whose worst credible severity is SCX.

In that case, we have assumed that:

- tolerable occurrence of effect equals safety objective of the hazard by conservative approach (Pe = 1);
- per SCX: 10 hazards that have a worst credible effect having a SCX.

The Quantitative SOCS for that specific System is:

- For Severity Class 1: $5.27x10^{-8}$ /h so every 2165 years;
- For Severity Class 2: $5.27x10^{-7}$ /h so every 215 years;
- For Severity Class 3: $5.27x10^{-6}$ /h so every 21,5 years;
- For Severity Class 4: $5.27x10^{-4}$ /h so every 79 days.

In case of quantitative approach, the following Safety Objective Classes definition is used:

Qualitative Safety Objective	Quantitative Safety Objective	Comment
Extremely Rare	$5.27x10^{-8}$ /h	Shall never happen during the building operational lifetime
Rare	$5.27x10^{-7}$ /h	As approximately 10 of such safety objectives have been identified, it means that one single event (severity 2) is accepted to occur once during the building operational lifetime
Occasional	$5.27x10^{-6}$ /h	As approximately 10 of such safety objectives have been identified, it means that one single event (severity 3) is accepted to occur once every 2 years.
Likely	$5.27x10^{-4}$ /h	As approximately 10 of such safety objectives have been identified, it means that it can happen that one single event (severity 4) is accepted to occur once every week.

2 LINK2000+ SAFETY OBJECTIVE CLASSIFICATION SCHEME

The following assumptions have been made to quantify Safety Objectives for hazards whose worst credible effect have been allocated a Severity = 3.

- 10^6 flight-hours per year per ATSU;
- 10 messages (total: initiation + clearance + response) per flight-hour (which could lead to Class 3 hazards);

The following ATM Risk Classification Scheme has been used for Link2000+:

Severity of the effect (iaw ESARR4)	Safety Target: Maximum acceptable frequency of occurrence of an effect
SC1	ST1 = 10^{-8} /fh
SC2	ST2 = 10^{-6} /fh
SC3	ST3 = 10^{-4} /fh
SC4	ST4 = 10^{-2} /fh
SC5	ST5 = 10^{-0} /fh

An order of magnitude of 2 between 2 severity classes is assumed based on existing practices in other domains such as airworthiness (See JAR25-1309) and ATM domain experts' judgement on the acceptability of such an approach.

For Link2000+, only effects of Severity 3, 4 and 5 have been assessed as being the worst credible effect of Link2000+ services hazards.

A number of 100 hazards has been assumed to lead to worst credible effects SC3 (so leading to Safety Objective for SC3 worst credible effect = 10^{-6}/fh per hazard).

Besides, taking into account environmental mitigations means (so part of ATM system but external to Link2000+ services), it has been estimated by the group of experts member of the EUROCAE/RTCA WG53/SC189, that 1 hazard occurrence out of 10 would really lead to a SC3 effect.

Consequently, the Link2000+ Safety Objective Classification Scheme is:

Severity of the worst credible hazard effect (iaw ESARR4)	Safety Objective: Maximum acceptable frequency of occurrence of a hazard
SC1	N/A
SC2	N/A
SC3	SO3 = 10^{-5} /fh
SC4	SO4 = 10^{-3} /fh
SC5	None

Assumptions listed at the beginning leading to:

- 10^{-5} /fh # 10^{-6} /Msg

So the quantitative Safety Objective for SC3 worst credible effect is:

- 10^{-5} /fh for the aircraft or;
- 10^{-6} /Msg for the ATSU or;
- 10^{-3} /h for the ATSU/airspace.

So the quantitative Safety Objective for SC4 worst credible effect is:

- 10^{-3} /fh for the aircraft or;
- 10^{-4} /Msg for the ATSU or;
- 10^{-1} /h for the ATSU/airspace.

3 CORA2 SAFETY OBJECTIVE

See CORA2 PSSA which includes a quantitative SOCS.