22 April 2016

Ministry of Defence

Field Service Evidence:

Practical Examples and Potential Refinements to Support Qualification Arguments

Elizabeth Lennon, Dr Mark Hadley, Mike Standish

Dstl, Software and Systems Dependability Team

14th April 2016, Safety Critical Systems Club

DSTL/PUB94694

The Premise

- All evidence is admissible towards a software and Complex Electronic Hardware (CEH) safety argument.
- There are issues and inconsistencies in how evidence, such as field data, supports a safety argument.
- Subjective opinion can allow a measurement of confidence to be gained in the evidence when placed within a suitable framework.

What's To Come

- Context to the UK MOD software and Complex Electronic Hardware (CEH) safety assurance
- Putting service history and field data into practise
- Some potential improvements
- Illustrative example

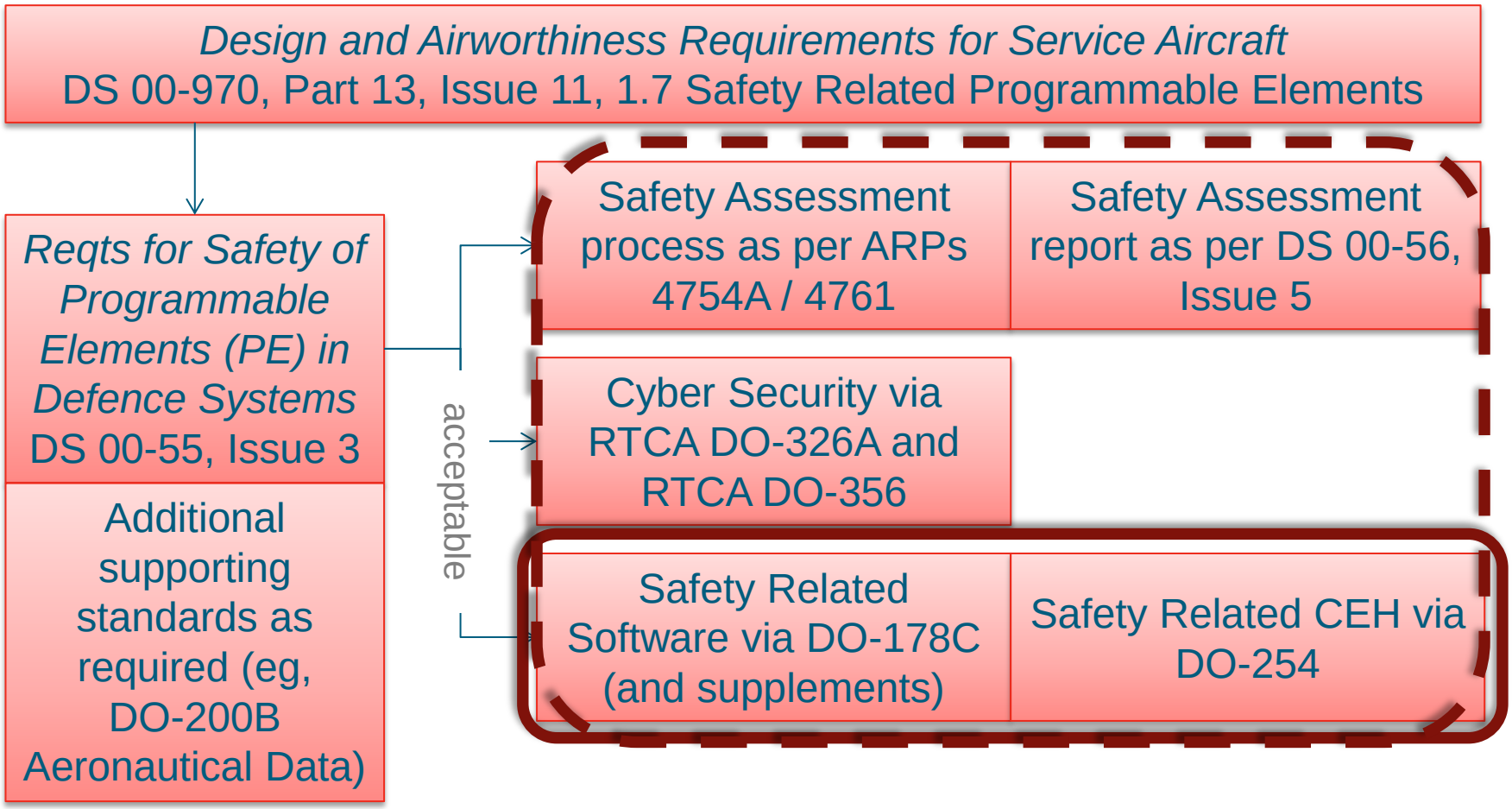
Caveat

- The contents of this presentation should not be interpreted as representing the views of the Ministry of Defence (MOD), nor should it be assumed that they reflect any current or future MOD policy.

- The information contained in this presentation cannot supersede any statutory or contractual requirements or liabilities and is offered without prejudice or commitment.

Some Context

Defence Standard (DS) 00-970



DS – Defence Standard
Reqt - Requirement
ARP - Aerospace Recommended Practice
CEH - Complex Electronic Hardware

Ministry of Defence

RTCA DO-178C

Software Considerations in Airborne Systems and Equipment Certification

*If equivalent safety for the software can be demonstrated by the use of the software's product service history, **some** certification credit may be granted*

12.3.4 Product Service History

- Configuration management of the software
- Effectiveness of problem reporting activity
- Stability and maturity of the software
- Relevance of product service history environment
- Length of the product service history
- Actual error rates in the product service history
- Impact of modifications

CAST-1 Position Paper

Guidance for Assessing the Software Aspects of Product Service History of Airborne Systems and Equipment

*Guidance is offered on an approach for assessing the product service history data and for determining the **amount** of certification credit to allow based on the assessment of these attributes*

Table 3.3-1 Product Service History Attributes Acceptability

Service Duration Length	Change Control During Service	Proposed Use Versus Service Use	Proposed Environment to Service Environment	Number of Significant Mods During Service
Number of Software Mods During Service	Number of Hardware Mods During Service	Error Detection Capability	Error Reporting Capability	Number of In-Service Errors
		Amount/ Quality of Service History Data		

Putting it into Practise

When Is Field Data Used?

- The use of service data to form part of a software safety argument can arise due to a number of factors:
  - No (or limited) process evidence available
    - No credit to be gained in processes adopted
    - No (or limited) access to compliant process evidence
  - Partial argument provided by process evidence
    - Field data bolsters the safety argument

Some Examples…

Field Data as an Argument

- No process evidence available
  - No credit to be gained in processes adopted
  - No (or very limited) access to complaint process evidence

Field data *is* the safety argument

Issue:
No process evidence available to support a safety argument for an airborne platform

Action:
Initial review of PSH conducted and full CAST-1 evidence process adopted

Result:
CAST-1 PSH argument successful with full endorsement provided by the MAA

PSH – Product Service History
MAA – Military Aviation Authority

Field Data to Support an Argument

- Partial argument provided by process evidence

Issue:
Airborne platform developed to a baseline that is not recognised by the current MAA guidance

Action:
A diverse software evidence approach adopted which had confidence from field data as a key strand

Result:
Reliability figures successfully adopted to complement other sets of evidence. Full software safety confidence gained.

Field data *bolsters* the safety argument

Some Lessons Identified

- Can be difficult to put forward as an argument due to traditional focus on process evidence

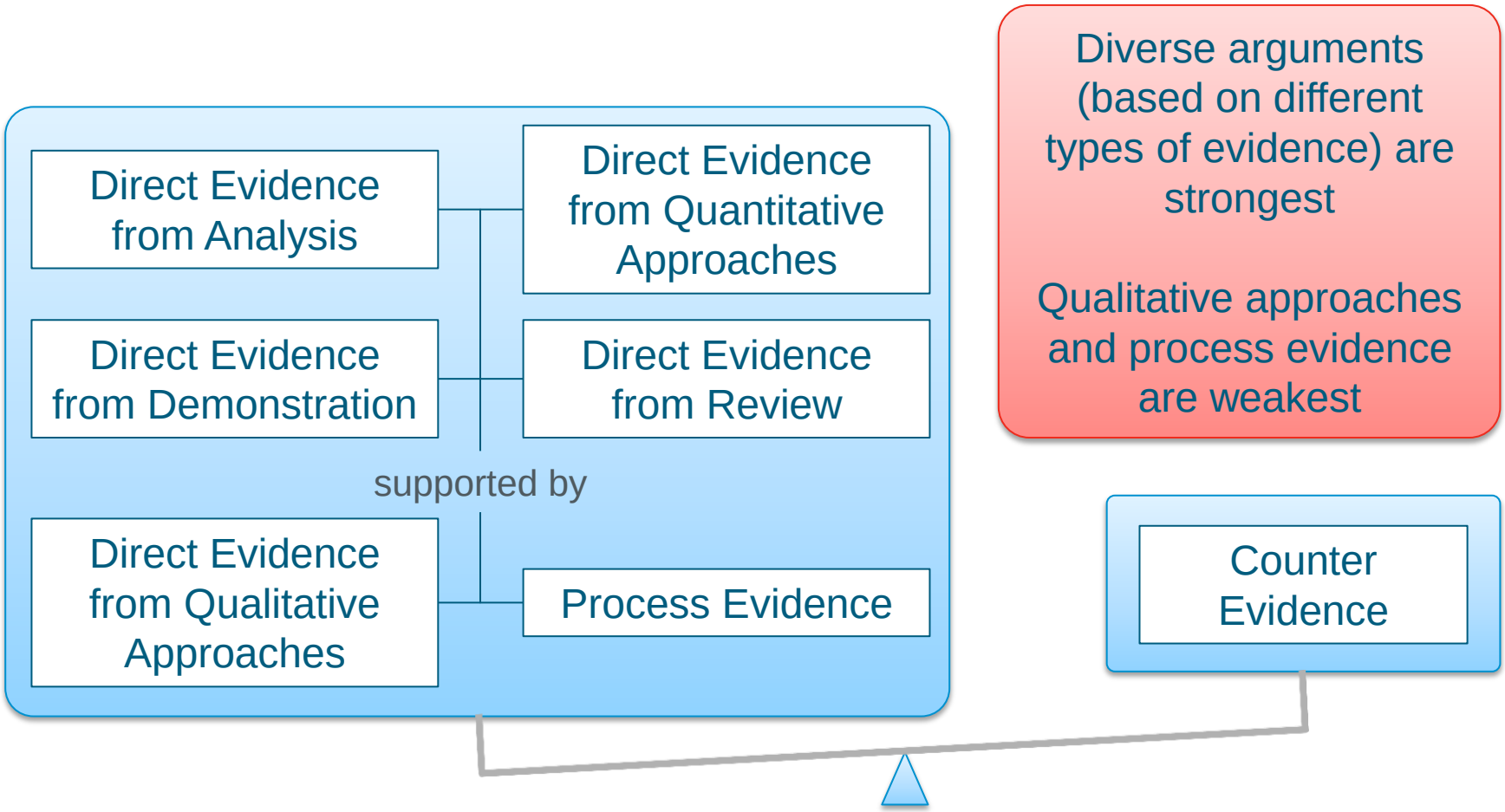
- Field data is not widely used as evidence. Therefore, there is a lack of detailed guidance

Some Lessons Identified (2)

- Systems may have a large quantity of in-service data
  - one of the strongest forms of evidence
- Any prior belief in the system can be validated
- In-service data can provide a measurement of the pedigree and effectiveness of the process itself

Some Potential Improvements to the Approach

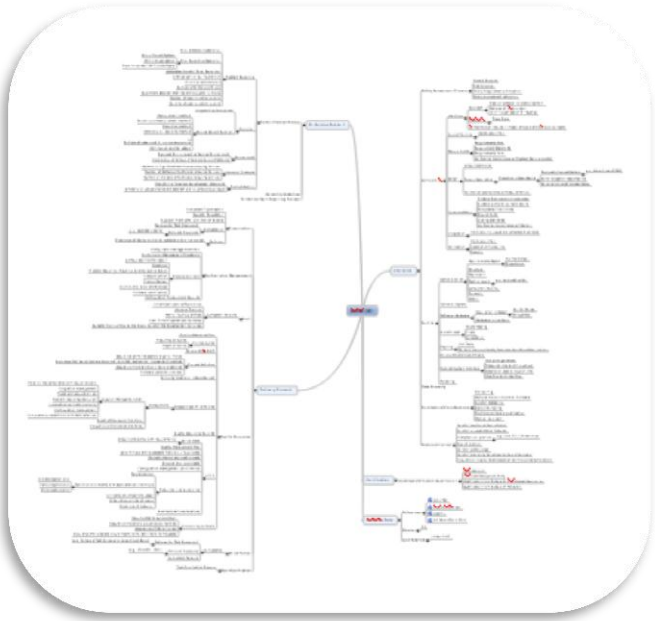
Types of Evidence



How to Incorporate Evidence

- A suggested approach:
  - Determine the evi… …nsidered admissible to the softw… …SH) (the *what*)
  - Assess the evidenc… …can be formed to allow a defensible level of confidence to be gained (the *how*)

The *What* (Input References)



DO-178C: SW Considerations in Airborne Systems and Equipment Certification

DO-254: Design Assurance Guidance for Airborne Electronic Hardware

DS 00-56: Safety Management Requirements for Defence Systems

CAA CAP 670: Air Traffic Services Safety Requirements

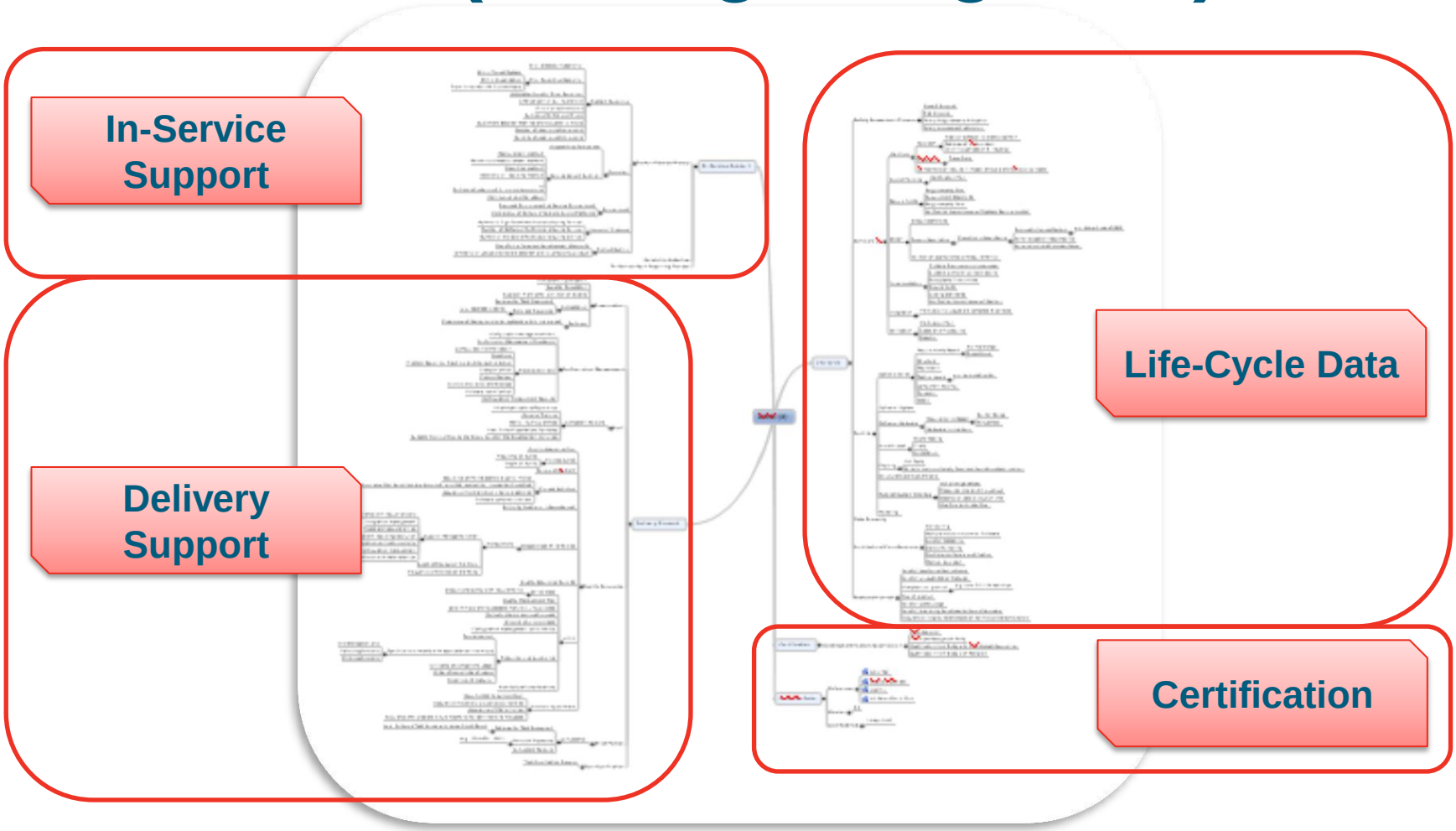
CAST-1: Guidance for Assessing the SW Aspects of PSH of Airborne Systems & Equipment

Others…

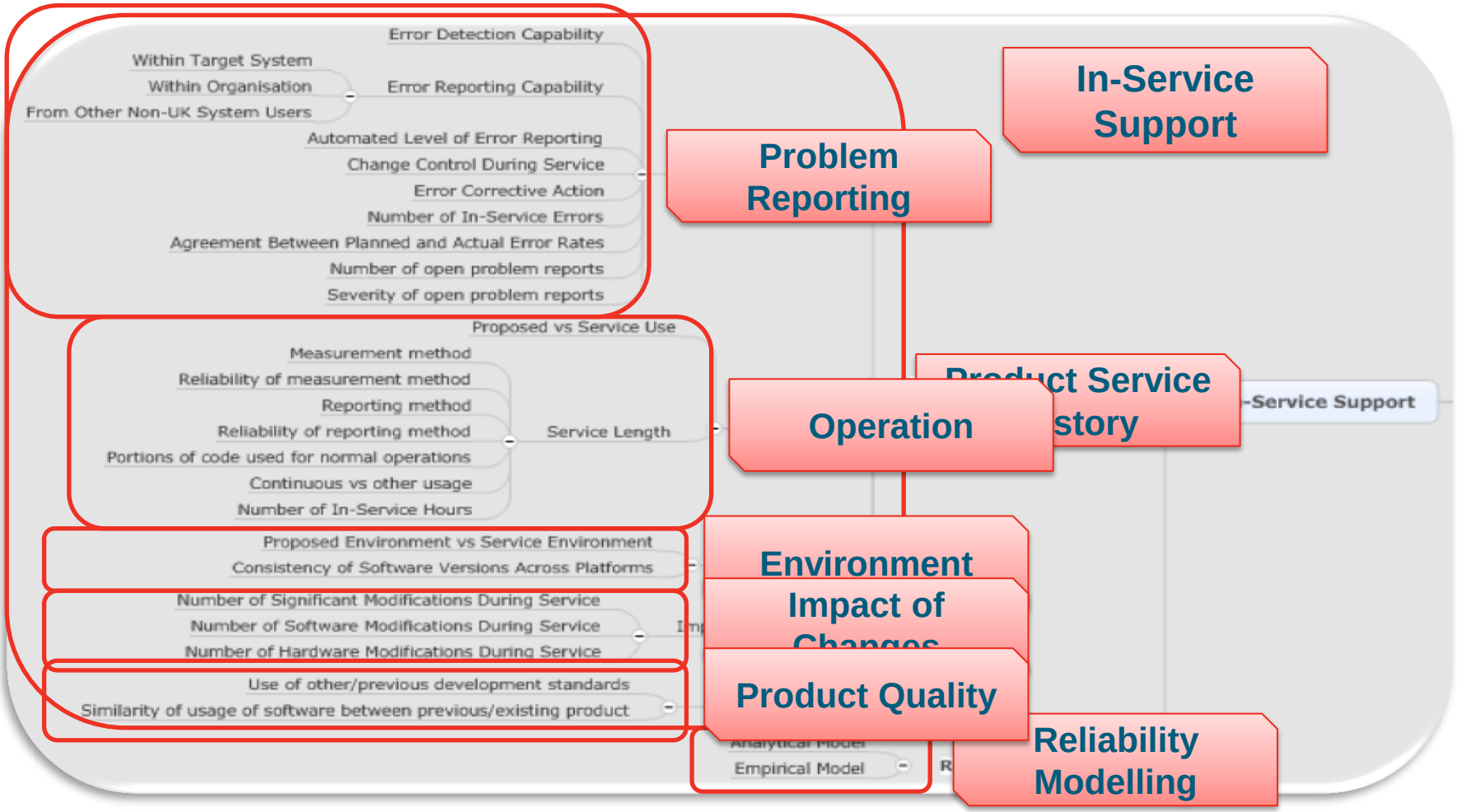
SW - Software
PSH - Product Service History
DS – Defence Standard
CAA – Civil Aviation Authority

Ministry of Defence

The *What* (Putting it Together)



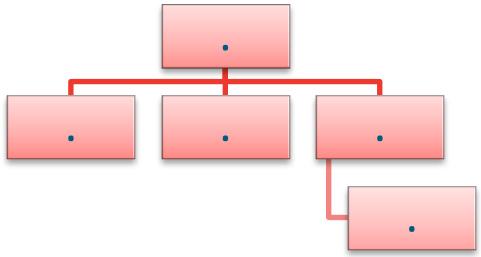
The *What* (In-Service Support)

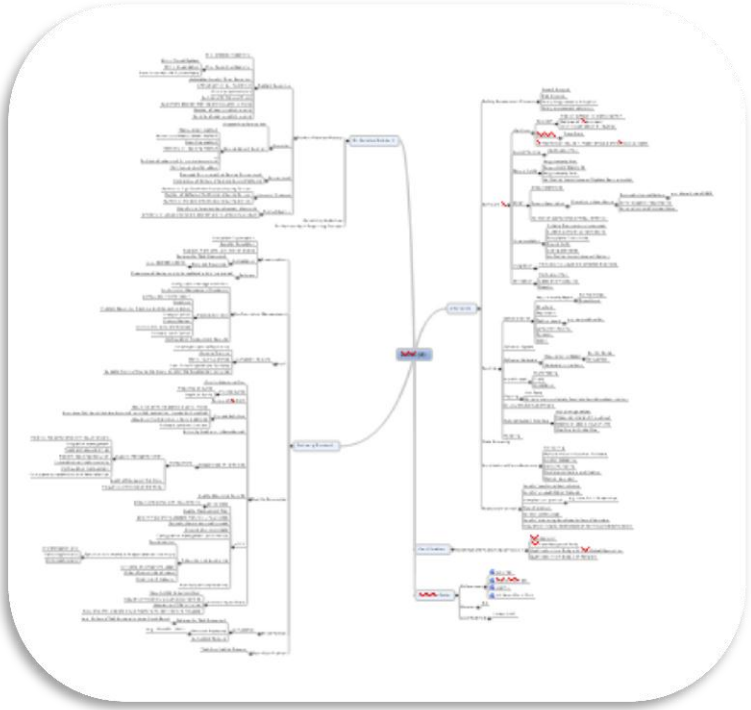


How to Incorporate Evidence

- A suggested approach:
  - Determine the evidence that could be considered admissible to the software safety argument (including PSH) (the *what*)
  - Assess the evidence so that judgements can be formed to allow a defensible level of confidence to be gained (the *how*)

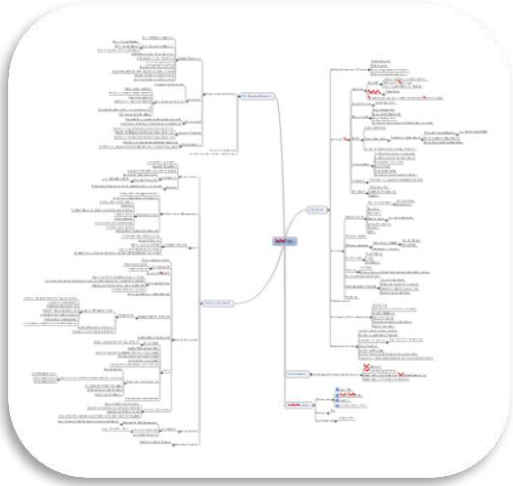
The *How* (Framework)

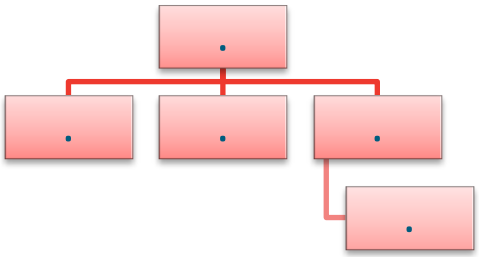




- Number of methods to allow judgements to be formed:
  - Bayesian Belief Networks
  - Fuzzy Logic
  - Evidential Reasoning
  - Others…
  - A combination…

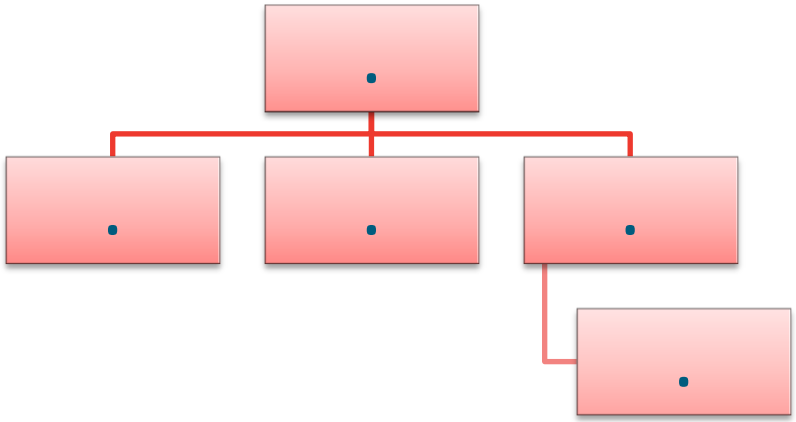
The *How* (Attributes)





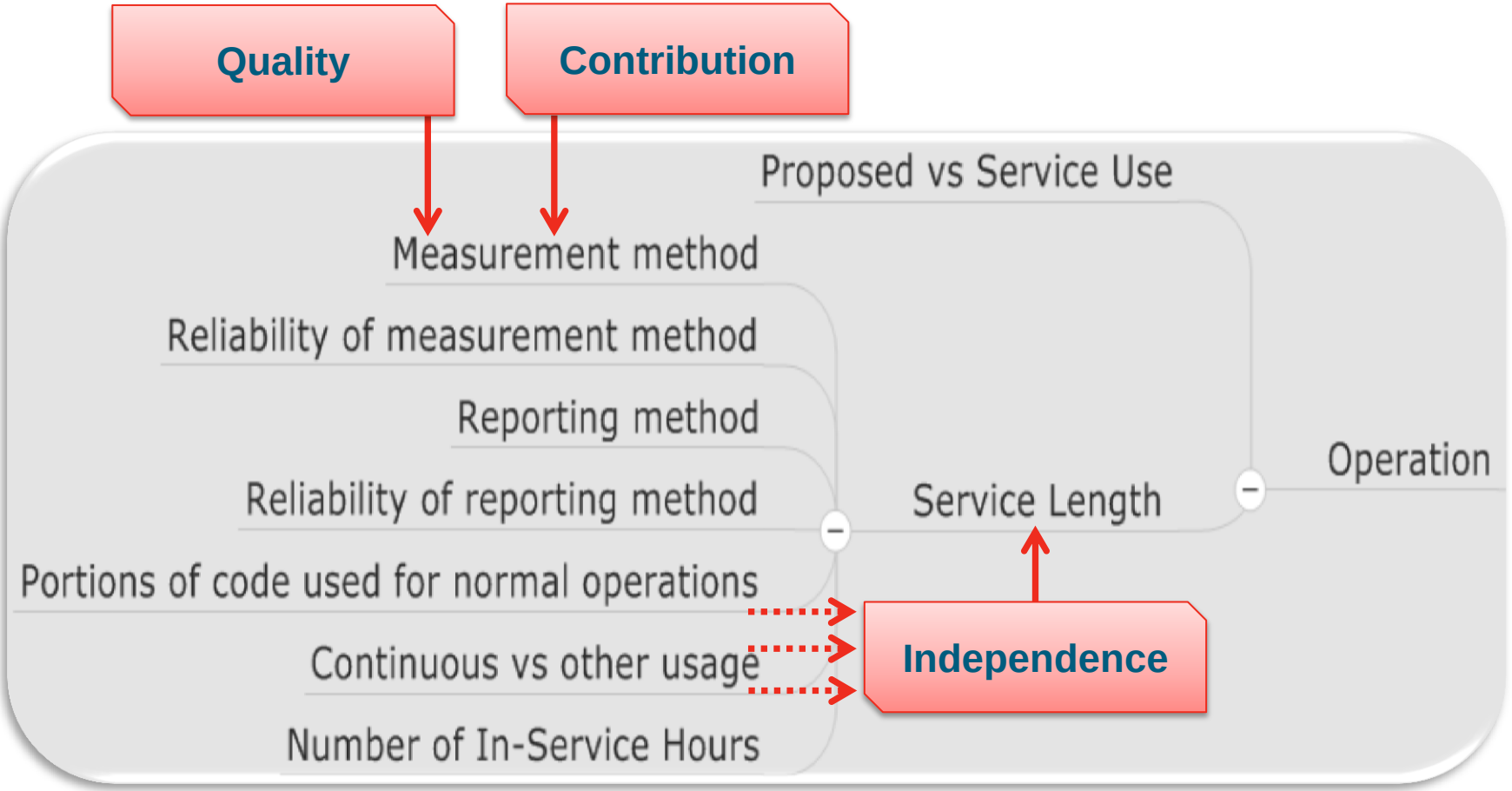
- With any method there is a decision on what attributes will be judged for the evidence, for example:
  - Quality
  - Contribution
  - Independence
    - Distinct
    - Mutual

The *How* (Attribute Combination)



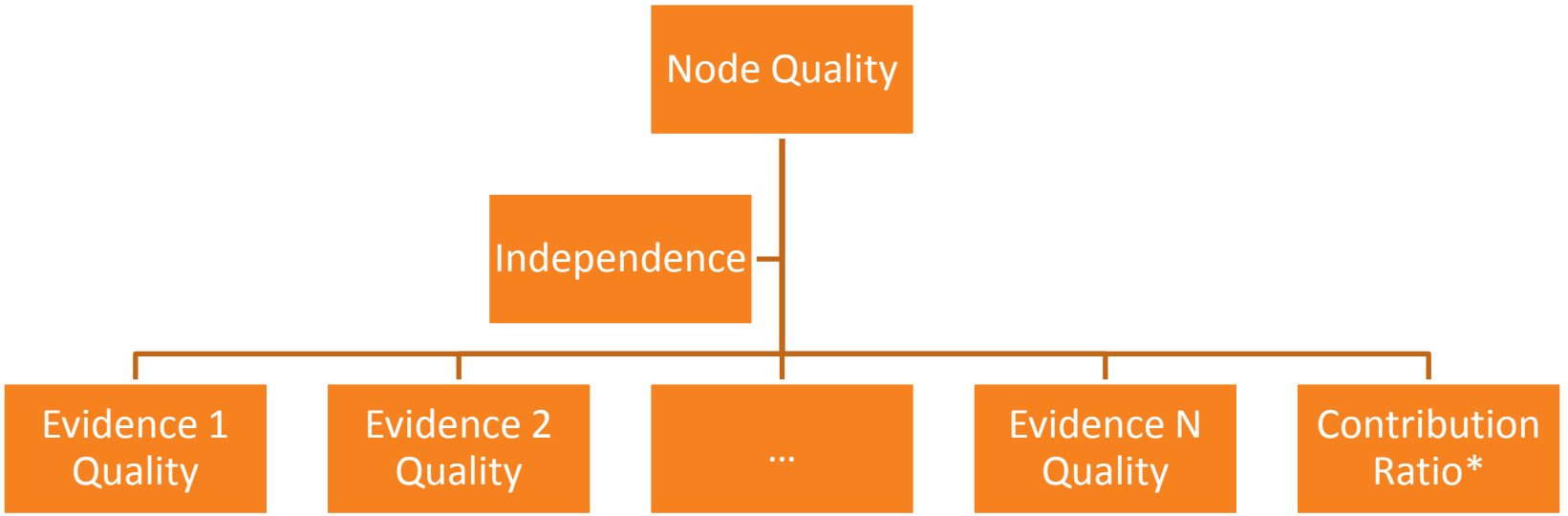
- Quality
- Contribution
- Independence

The *How* (Attribute Combination) (2)



Using the *What* and the *How* - An Illustrative Example

The Framework



** Where applicable.*

Evidential Reasoning Approach

- Evidence is inputted in the form:
  - [Belief, Non-belief, Uncertainty]

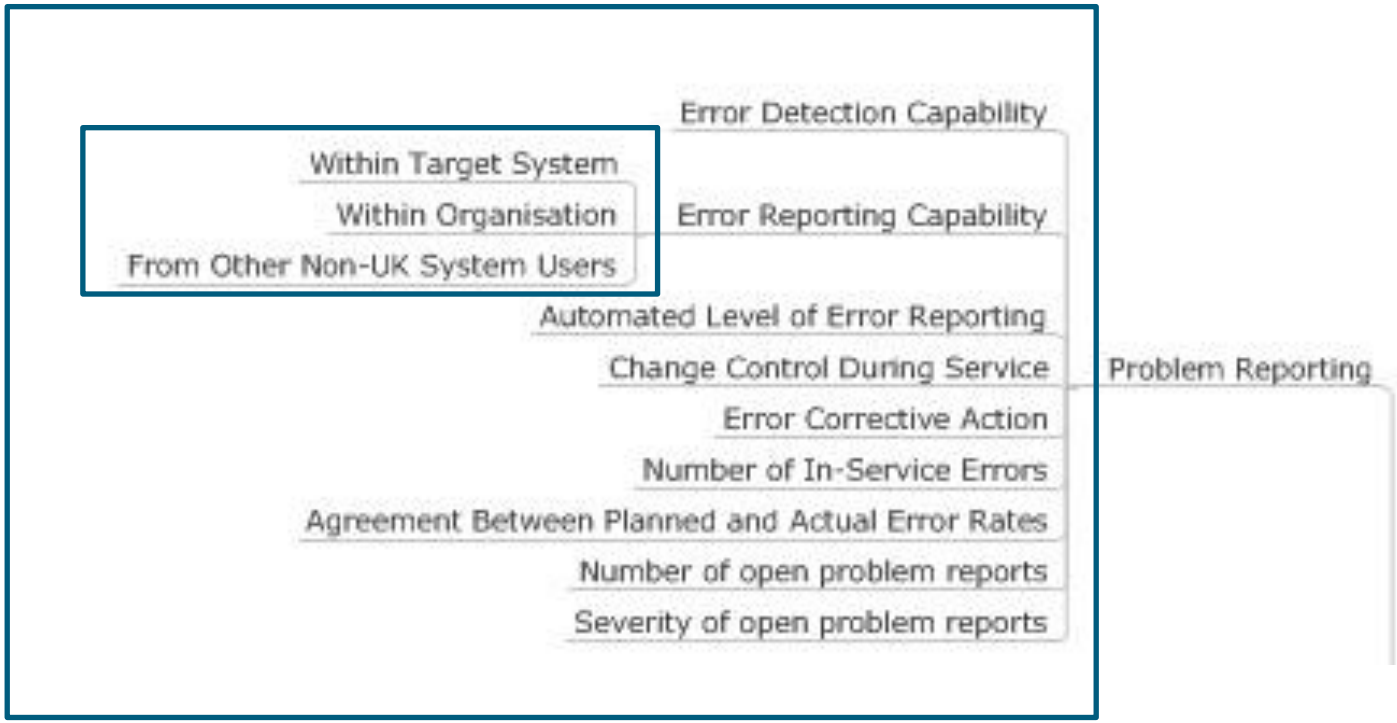
- We have investigated three methods of combining information in the ER framework:
  - Dempster's Rule of Combination
  - P-Average
  - Yager's Rule

Evidential Reasoning Approach

- Evidence is inputted in the form:
  - [Belief, Non-belief, Uncertainty]

- We have investigated three methods of combining information in the ER framework:
  - ~~Dempster's Rule of Combination~~
  - P-Average
  - Yager's Rule

Error Reporting Capability



A Comparison of Combination

- *Complementary Evidences*

Evidence Type	% Belief	% Non-Belief	% Uncertainty
Within Target System	90	5	5
Within Organisation	85	5	10
Non-UK Users	95	5	0

Contribution - 2:1:1

Independence - [60%, 40%, 0%]

Combination Method	% Belief	% Non-Belief	% Uncertainty
P-Average	82	5	13
Yager	78	0*	22

*More accurately, 0.07%

A Comparison of Combination

- *Conflicting Evidences*

Evidence Type	% Belief	% Non-Belief	% Uncertainty
Within Target System	90	5	5
Within Organisation	5	85	10
Non-UK Users	95	5	0

Contribution - 2:1:1

Independence - [60%, 40%, 0%]

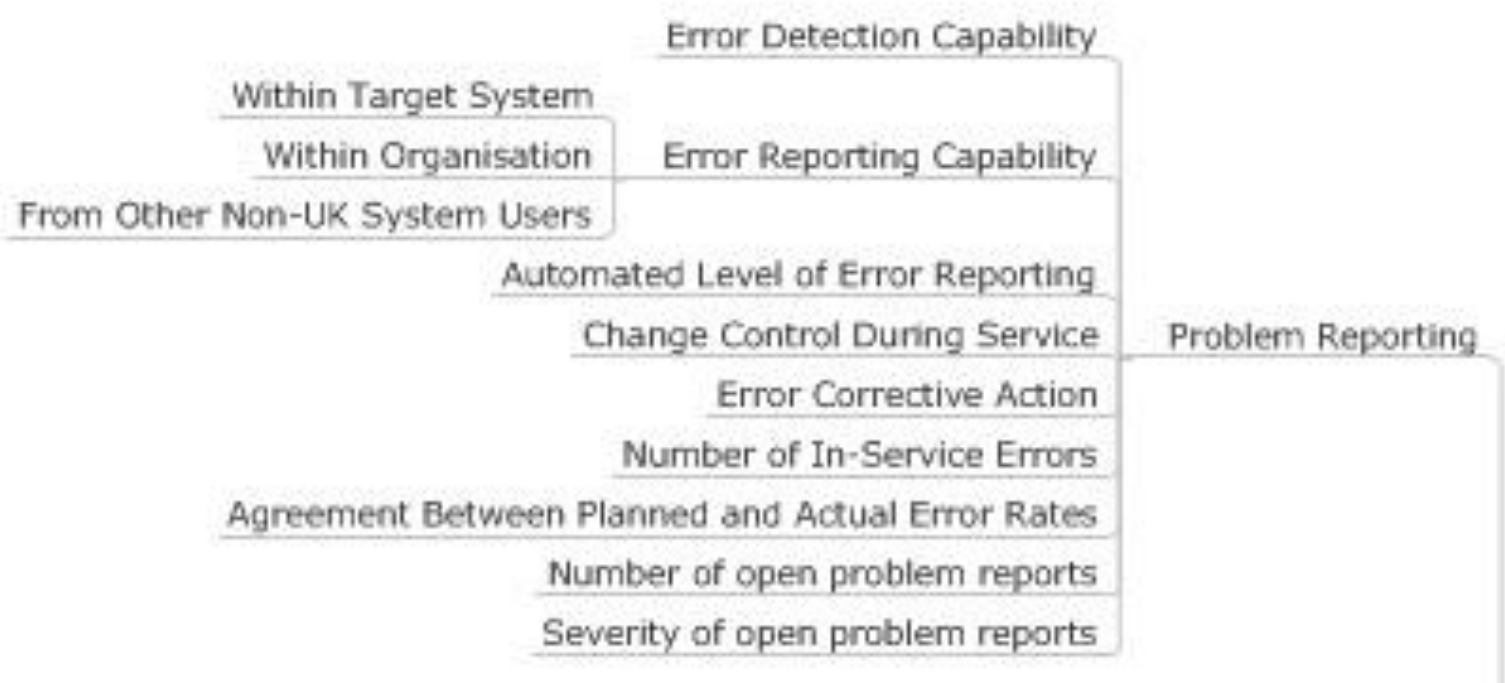
Combination Method	% Belief	% Non-Belief	% Uncertainty
P-Average	64 *(comp 82)*	23 *(comp 5)*	13 *(comp 13)*
Yager	12 *(comp 78)*	0* *(comp 0)*	87 *(comp 22)*

*More accurately, 0.4% , *(comp 0.07).*

Combination Methods in Conflict

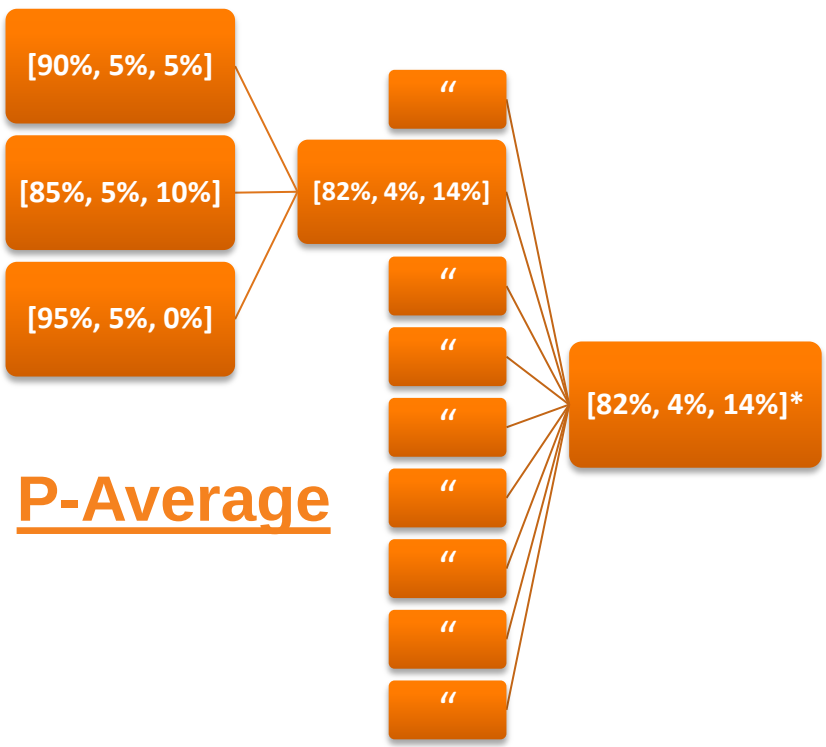
- P-Average
  - Contribution ratio can be incorporated and therefore conflicting evidence will only have a significant impact if it is deemed of high importance.
- Yager's Method
  - Any element of conflict is recognised.
  - Level of recognition is scaled to the level of conflict.

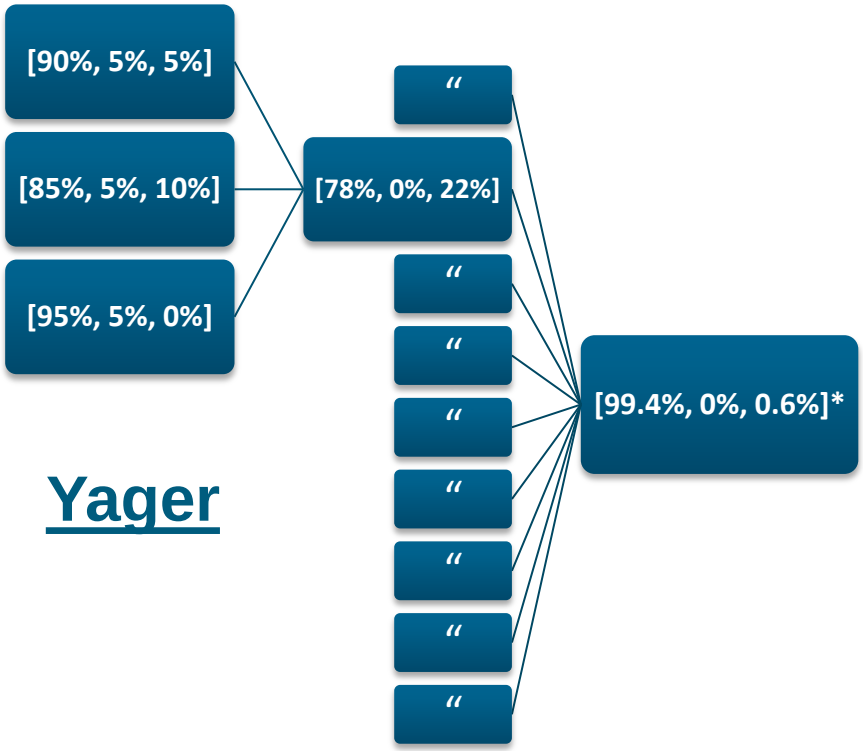
Problem Reporting Quality



Problem Reporting

- Complementary Evidence

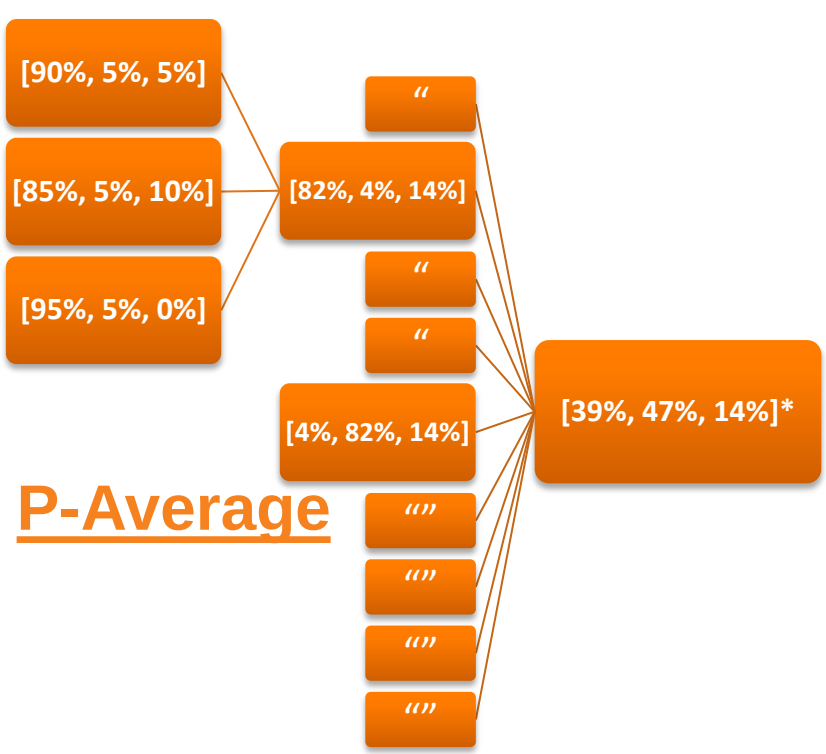


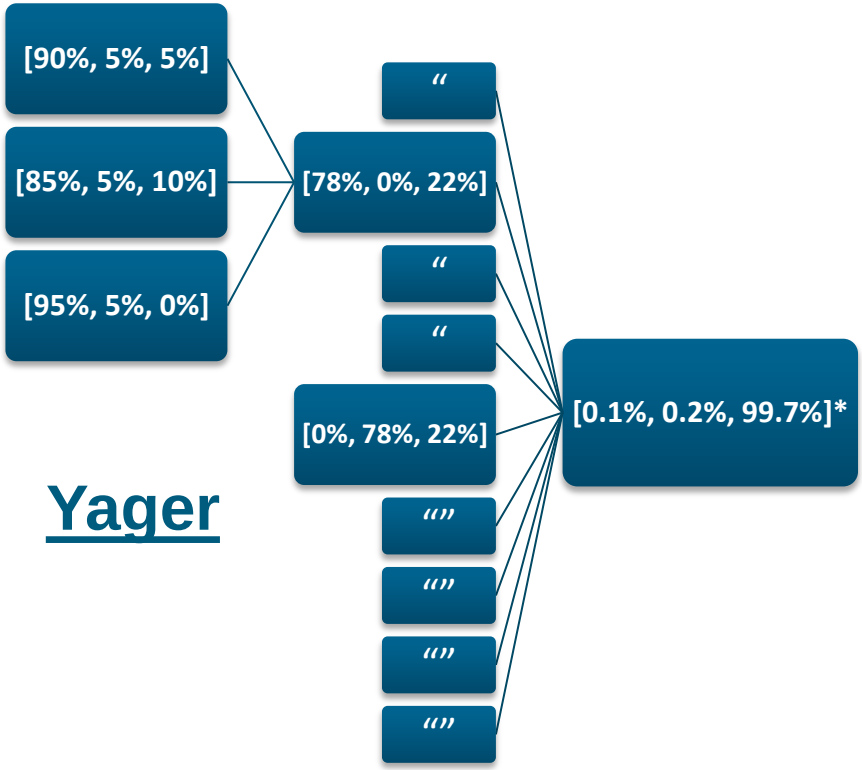


**Assume independence value of [1,0,0] and contribution ratio representing a uniform distribution.*

Problem Reporting

- Conflicting Evidence





**Assume an independence value of [1,0,0] and a contribution ratio representing a uniform distribution.*

Combination of Evidence

- *A Summary*

- **ER**
  - Examples show how the two specified combination techniques react in situations of complimentary or conflicting evidence.
  - Next step is to conclude which of the combination methods is most suited to our particular application.
- **Fuzzy Logic**
  - Fuzzy rules have been defined.
  - Follows the framework as described, but allows for qualitative statements to be interpreted, which could prove to be much more user friendly.

Conclusions

- At present not all potential evidence is utilised. We propose that all evidence is admissible towards a safety argument.
- There needs to be subjective opinion in order to review any admissible evidence but a suitable framework to do this to date has been missing.
- Subjective opinion needs to be provided by Suitably Qualified and Experienced Personnel.

Next Steps

- Further refine the framework and implement further case studies.
- Implement the framework to make firm recommendations for a particular project.
- Implement the framework to support wider projects.
- Continue to adopt the use of service history as part of a justified and defensible software safety argument
  - With an aim to enhance the process!

Any Questions?

References

- UK MOD 2014. Defence Standard 00-56. Safety Management Requirements for Defence Systems. Issue 5.
- UK MOD 2014. Defence Standard 00-55. Requirements for Safety of Programmable Elements (PE) in Defence Systems. Part 1: Requirements and Guidance. Issue 3.
- UK MOD 2014. Defence Standard 00-970. Design and Airworthiness Requirements for Service Aircraft. Part 13 Military Common Fit Equipment. Issue 8.
- RTCA 2014. DO-326A. Airworthiness Security Process Specification.
- RTCA 2014. DO-356. Airworthiness Security Methods and Considerations.
- RTCA 2011. DO-178C. Software Considerations in Airborne Systems and Equipment Certification.
- SAE 2010. Aerospace Recommended Practice 4754A. Guidelines for Development of Civil Aircraft and Systems.
- CAA 2010. Acceptable Means of Compliance to CAP 670 SW 01. Guidance for Producing SW 01 Safety Arguments for COTS Equipment. Issue 3.
- RTCA 2000. DO-254. Design Assurance Guidance for Airborne Electronic Hardware.
- CAST 1998. Position Paper: Certification Authorities Software Team (CAST)-1. Guidance for Assessing the Software Aspects of Product Service History of Airborne Systems and Equipment.
- SAE 1996. Aerospace Recommended Practice 4761. Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.

Backup

CAST 1 Position Paper (2)

Guidance for Assessing the Software Aspects of Product Service History of Airborne Systems and Equipment

PSH Attribute	Not Acceptable	<----------	----------	--------->	Acceptable
Service Duration Length	Short	<->	Moderate	<->	Long
Change Control During Service	None	<->	Marginal	<->	Total

PSH Attribute	Not Acceptable	<---------	----------	-------->	Acceptable
Service Duration Length	Short	<->	Moderate	<->	Long

Number of Hardware Mods During Service	Many	<->	Few	<->	None
Error Detection Capability	None	<->	Some	<->	All
Error Reporting Capability	None	<->	Some	<->	All
Number of In-Service Errors	Many	<->	Some	<->	None
Amount/Quality of Service History Data Available and Reviewed	None/Low	<->	Some/OK	<->	Much/High

CAST 1 Position Paper (3)

Guidance for Assessing the Software Aspects of Product Service History of Airborne Systems and Equipment

PSH Attribute	SwL A/1	SwL B/1	SwL C/2	SwL D/3	SwL E/3
Acceptable Service Period Duration	VI	VI	VI	I	
Similar/Identical Proposed Use to Service Use	VI	VI	VI	I	I

PSH Attribute	SwL A/1	SwL B/1	SwL C/2	SwL D/3	SwL E/3
Acceptable Service Period Duration	VI	VI	VI	I	

High Quality of Error Detection Capability	VI	VI	VI	I	
High Quality of Error Detection Capability	VI	VI	VI	I	
High Quality of Error Reporting Capability	VI	VI	VI	I	
Acceptably Low Number of In-service Errors	VI	VI	I	I	
Acceptable Amount and Quality of Service History Data Available and Reviewed	VI	VI	I	I	

SwL - Software Level DO-178B/A
VI – Very Important
I – Important

22 April 2016

Ministry of Defence