SESSION ONE EVALUATION QUESTIONS

Modelling Process Evaluation

It would be beneficial for us to be able to argue over your expertise in the field of software safety practice. To that end we would be grateful if you could list the attributes of your experience as a software safety practitioner and indicate in parentheses afterwards the number of years' experience you have. For example:

1. Software Safety Engineer (5 years)
2. Principle Software Safety Engineer (3 years)
3. Safety Manager (3 years)
4. Independent Safety Assessor (2 years).

Please use the text box below and list all attributes you believe are relevant. There is no word count limit, but please complete this digitally using an appropriate word-processing software package (such as Microsoft Word), so that we can ensure all comments are fully legible.

General software safety practitioner (25 years – academia and industry)
This includes:
Independent safety assessor and auditor inc. software (6.5 years industry experience)
Software verification tool R&D manager (1.5 years industry experience) (MC/DC and timing)

I have worked in defence (land, aviation, maritime), civil aviation, nuclear, rail and automotive.

Having completed the process to model and understand safety engineering practice, you are now invited to state your levels of agreement with the following statements. Each statement is written at the start of a row, and you are requested to place an 'X' in the column which aligns your level of agreement with that statement. To avoid any ambiguity of responses, please complete this table digitally, using an appropriate word-processing software package (such as Microsoft Word), and only place an 'X' against one column for each statement (statements have a suffix of `EQn').

At the end of each question, a free-text box is provided for you to make any comments you wish to. There is no word count limit, but please complete this digitally using an appropriate word-processing software package (such as Microsoft Word), so that we can ensure all comments are fully legible.

This is not a 'test' of your knowledge, and there is no 'correct' or 'incorrect' answer. Your opinion matters.

Statement	**Fully Disagree 1**	**Somewhat Disagree 2**	**Neither Agree/ Disagree 3**	**Somewhat Agree 4**	**Fully Agree 5**
Completeness: Reflecting on your understanding of the process to understand software safety engineering practice, we would like your opinion on the following statement. In considering your response, we ask that you **also** consider applications and technologies **not** covered by the artefacts we provided you with (i.e. from experience throughout your career), and don't restrict your response to **just** the artefacts sent to you					
EQ1: The process considers all elements that together constitute software safety engineering practice (the 10 'steps')				**X**	
For this I considered: **1) Tool qual 2) tabular SW quality audit of non-safety OTS sw 3) goal based assessment 4) CI/CD** **I think they all work, 2 may be challenging but I think shortfall management, limitations on use, justifications for non-compliance all covered. Step 8 assumes there is a project lifecycle (this may be very poorly defined for some OTS devices, I could tell some stories).**					
Ease of Use: Reflecting on your experience of following the steps in the process to model and assess software safety engineering practice, we would like your opinion on how much you agree with the following statement.					
EQ6: The modelling process instructions are easy to follow (you could follow each step)					X
Yes, but a couple of small examples in the process instructions would be helpful.					
Effectiveness: Having applied part of the process to understand software safety engineering practice through the modelling and assessment of practice, we are interested in your thoughts on the overall usefulness of this process. How much do you agree with the following four statements? In considering your response, we ask that you **also** consider applications and technologies **not** covered by the artefacts we provided you with (i.e. from experience throughout your career), and don't restrict your response to **just** the artefacts sent to you					

Statement	**Fully Disagree** **1**	**Somewhat Disagree** **2**	**Neither Agree/ Disagree** **3**	**Somewhat Agree** **4**	**Fully Agree** **5**
EQ10: The process to understand software safety engineering practice will help to identify potential impediments to achieving best practice for software safety engineering				X	
(Pan-industry Applicability) EQ11: The process to understand software safety engineering practice can be used for any industry and any technological application				X	
As noted in detailed comments, I'm not sure if there's an assumption about the sw developer originally being in the SC domain or using an open standard for their development.					
(Consistency) Having applied part of the process to understand software safety engineering practice through the modelling and assessment of practice, we are interested in your thoughts on the consistency of the outputs which the process creates. How much do you agree with the following two statements?					
EQ12: The process uses consistent terminology when considering each different element that constitutes software safety engineering practice					X
EQ13: The process creates models whose symbology is consistent across all elements of software safety engineering practice					X
I had no difficulty understanding the concepts and terminology.					

If you have any additional comments on the process, or on this specific evaluation you are invited to make them in the box below. There is no word count limit, but please complete this digitally using an appropriate word-processing software package (such as Microsoft Word), so that we can ensure all comments are fully legible.

In UPSS you say “Levels of disagreement between your project’s process and the Open Standard which influenced its development”

In the nuclear domain I assessed a number of “smart devices” from other industrial applications that had NO sw standards influencing their project development, or where project development was so long ago it was forgotten. A couple were from very small companies with one sw dev, sometimes sub-contracted. At very low integrity (below SIL1) this is can be okay but we usually did some remedial work.

I think what you propose works fine in this situation (mitigations etc.), but as an observation the as required organisations process on RHS of diamond might be very small!