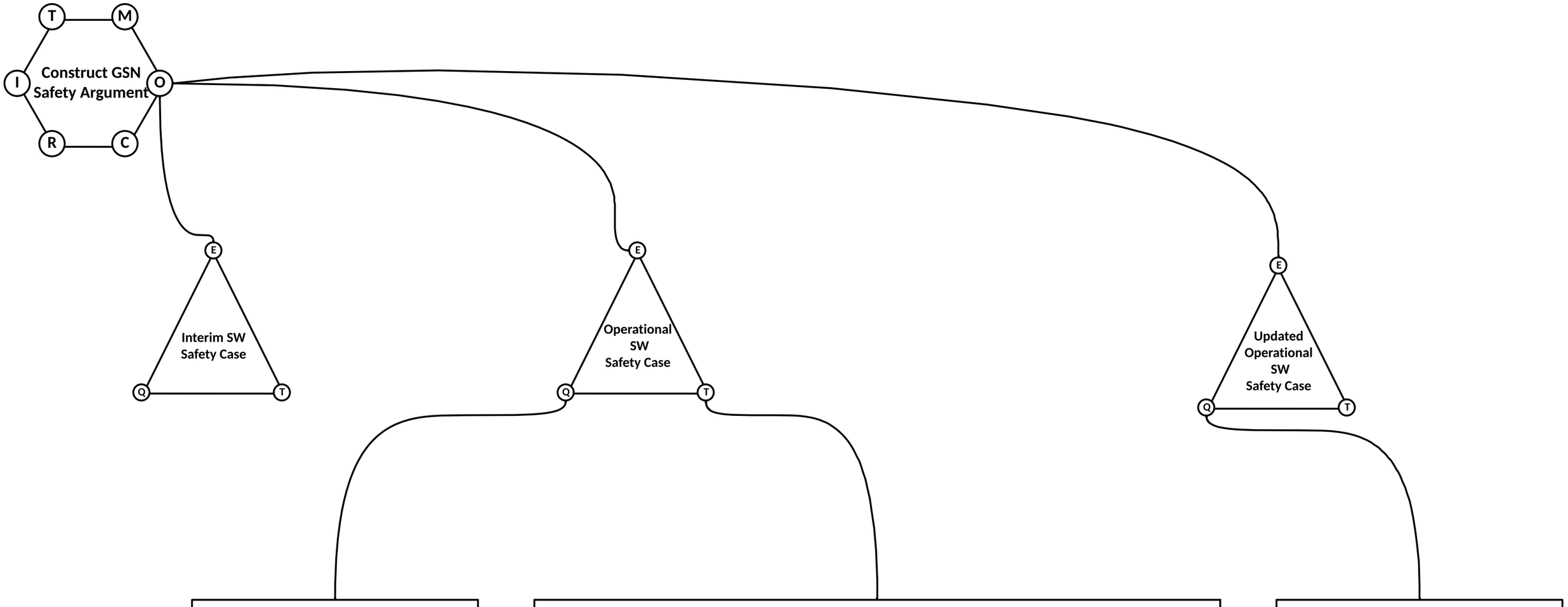
T
M
I
Construct GSN
Safety Argument
O
R
C
E
Interim SW
Safety Case
Q
T
E
Operational
SW
Safety Case
Q
T
E
Updated
Operational
SW
Safety Case
Q
T
Shall include:
1. Updates to the Interim safety Case as previously presented at TRR
2. Completion of all safety goal and solution development
3. Completion of all safety arguments, context information and justifications for each safety argument
4. Completion and provision of the evidence required to support all goals allocated.
Justification of any change in safety argument strategy from those strategies identified in the previous phase.
5. Completion of all actions arising from previous safety reviews.
Contents:
1. Scope – clearly define the boundary of concern; identifying the software to which the safety argument is applicable.
2. References
3. Introduction
4. System and Design Aspects:
(a) Overview of the system architecture including the system boundaries and interfaces
(b) Overview of the system functions
(c) Brief description of the operating environment, including both normal and abnormal modes of operation
(d) A list of the main system safety requirements
(e) The system design report
5. System Hazards – a brief description of the system level hazards that are applicable to the software under consideration (referencing the Hazard Log as an aid to traceability
6. Software Safety Requirements – describe the role that SW plays in ensuring safety. Include a list of the functional and non-functional SW safety requirements, along with the safety integrity requirements for the SW, and any required SW standards
7. Software Description – describe the architecture of the SW and how this contributes towards safety. Including:
(a) Overview of the SW architecture
(b) Description of the main design features of the SW (e.g. real-time aspects, user interfaces, key algorithms etc.)
(c) Means by which SW of different SILs is segregated (if relevant)
8. Safety Arguments – justifying how each SW safety requirement has been met, and that the necessary measures have been taken to reduce the SW contribution to system hazards to an acceptable level. The argument will reference at least 2 independent sources of evidence (e.g. analysis and testing). A complete list of all assumptions (with corresponding justifications) used in constructing the safety argument, and a list of weaknesses in the current argument.
9. Software Development Process – justification that the SW development process is adequate to achieve the required SIL of the SW:
(a) Briefly describe the main methods, tools and key project staff
(b) Describe and justify the use of any previously developed SW
(c) Provide a measure of the performance of the SW development process
(d) The results of any safety/quality audits carried out
(e) If the data is available, provide an analysis of historical data on the safety integrity of SW developed using the proposed/similar SW development process.
A summary of the testing evidence is needed for the argument, and could be placed in this section.
10. Current Status
11. Change History
12. Compliance – statement of compliance against all relevant SW standards
13. In-Service Feedback – from realistic operational testing, trials or in-service usage
14. Software Identification – specifying the current release of the SW, citing a SW release notice
15. Conclusions
16. Notes – definitions and abbreviations used within the document, and the provision of any additional material that may aid in the reading of the SW Safety Case.
Shall include:
1. Updates to the Interim safety Case as previously presented at TRR
2. Completion of all safety goal and solution development
3. Completion of all safety arguments, context information and justifications for each safety argument
4. Completion and provision of the evidence required to support all goals allocated.
Justification of any change in safety argument strategy from those strategies identified in the previous phase.
5. Completion of all actions arising from previous safety reviews.