SEMEM457

Conducting engineering software safety assessments

Overview

This standard identifies the competences you need to conduct a software safety assessment as part of the product definition activity, in accordance with approved procedures. You will be given a detailed brief, and will be required to assess these requirements and to extract all necessary information in order to carry out the software safety assessment. You will need to select the appropriate software safety assessment method to use, based on the safety criticality of the software functions. You will be expected to use current British, European, international and company standards to analyse the software.

Your responsibilities will require you to comply with organisational policy and procedures for software safety assessment. You will be required to report any problems with computer hardware, software or procedures that you cannot personally resolve, or that are outside your permitted authority, to the relevant people. You will be expected to work to verbal/written instructions and draft specifications, with a minimum of supervision, taking personal responsibility for your own actions and for the quality and accuracy of the work that you carry out.

Your underpinning knowledge will provide a good understanding of your work, and will provide an informed approach to applying software safety assessment procedures. You will understand the computer system and the safety assessment software used, and its application, and will know about the various tools and techniques used to assess whether the software integrity is sufficient for its intended role within a defined operational environment.

You will understand the safety precautions required when working in the software development team. You will be required to demonstrate safe working practices throughout, and will understand the responsibility you owe to yourself and others in the workplace.

Performance criteria

You must be able to:

1. work safely at all times, complying with health and safety legislation, regulations, directives and other relevant guidelines
2. plan the software safety assessment activities before you start them
3. use appropriate sources to obtain the required information for the safety assessment activity
4. use references that follow the required conventions
5. determine the evidence required to achieve the necessary level of software integrity
6. perform the software safety assessment
7. review the output from the safety assessment
8. contribute to the software safety assessment review of the overall product
9. report your findings on the safety assessment performed
10. save and archive the software safety assessment results as the appropriate file type and in the correct location
11. deal promptly and effectively with problems within your control, and seek help and guidance from the relevant people if you have problems that you cannot resolve

Knowledge and understanding

You need to know and understand:

1. the specific safety precautions to be taken when working with software development environment hardware (to include such items as safety guidance relating to the use of visual display unit (VDU) equipment and work station environment such as lighting, seating, positioning of equipment; repetitive strain injury (RSI); the dangers of trailing leads and cables; how to spot faulty or dangerous electrical leads, plugs and connections)
2. the importance of good housekeeping arrangements (such as cleaning down work surfaces; putting media, manuals and unwanted items of equipment into safe storage; leaving the work area in a safe and tidy condition)
3. the documentation required for the software safety analysis (such as hazard identification analysis documentation, FMEA documentation, software safety requirements, software test and analysis reports)
4. the basic principles of software safety assessments
5. how the engineering software safety assessment contributes to the overall safety assessment of the product
6. system hazard analysis methodologies, and national, international and relevant company software development procedures, methods and tools
7. identification of the correct version of software tool, and the various techniques that are supported by the tool
8. how to use and configure the software safety analysis tools
9. how to access the specific code analysis results
10. how to access, recognise and use a wide range of standard components and symbol libraries from the tools
11. the need for configuration control on all components (such as ensuring that completed results are approved, labelled and stored on a suitable storage device)
12. why it is necessary to be able to recall previous issues of analysis results
13. when to act on your own initiative, and when to seek help and advice from others

Scope/range related to performance criteria

1. Prepare for the software safety assessment, by carrying out **all** of the following:
    1. check that the working environment is in a safe and appropriate condition and that all working equipment is in a safe, tested and usable condition (such as cables undamaged, correctly connected, safely routed)
    2. identify all potential hazards to which the software can contribute
    3. identify the severity of each hazard (such as catastrophic, severe, minor, negligible)
    4. identify the software's worst case contribution to the hazard (such as direct cause, cause in conjunction with other failure, one of several independent contributors, no contribution)
    5. identify the required standards and all relevant sources (such as customer (contractual) standards and requirements, recognised compliance agency/body's standards, software safety requirements, software design and code standards)
2. Review **five** of the following to obtain sources of data to assess correctly the software safety:
    1. change order/modification request
    2. software design
    3. hazard identification and analysis documentation
    4. software process definition documentation
    5. Failure Modes and Effects Analysis (FMEA) documentation
    6. software test and analysis reports
    7. standards reference documents
    8. software safety requirements
3. Carry out **all** of the following before performing the software safety assessment:
    1. ensure that the data and information you have is current, complete and under configuration control
    2. confirm that the system level hazard identification and analysis have been performed
    3. recognise and deal with problems (such as technical issues and lack of information, or incorrect information)
4. Perform software safety assessment using **five** of the following:

1. change order/modification request
2. hazard identification and analysis documentation
3. Failure Modes and Effects Analysis (FMEA) documentation
4. software safety requirements
5. software design
6. software process definition documentation
7. software test and analysis reports
8. standards reference documents

5. Review and report on a sample of the software safety related evidence for **all** of the following:

    1. completeness
    2. accuracy
    3. traceability
    4. adequacy

6. Save and store the results in appropriate locations, to include carrying out **all** of the following:

    1. check that the results are correctly titled, referenced and annotated
    2. ensure that the results have been checked and that it complies with the company procedure
    3. save the results to an appropriate location (such as storage device, configuration database)
    4. ensure a separate backup copy is created and placed in safe storage

Behaviours

Additional Information

You will be able to apply the appropriate behaviours required in the workplace to meet the job profile and overall company objectives, such as:

- strong work ethic
- positive attitude
- team player
- dependability
- responsibility
- honesty
- integrity
- motivation
- commitment

SEMEM457

Conducting engineering software safety assessments

Developed by	Enginuity
Version Number	1
Date Approved	30 Mar 2017
Indicative Review Date	31 Mar 2020
Validity	Current
Status	Original
Originating Organisation	Semta
Original URN	SEMEM457
Relevant Occupations	Corporate Managers and Senior Officials, Engineering, Engineering and Manufacturing Technologies, Functional Managers
Suite	Engineering and Manufacture Suite 4
Keywords	engineering; leading; completeness; accuracy; traceability; adequacy; software design