

Safety Uni-REPM module – Assessment Instrument

Level 1 - Basic					
Action ID	Question	C	IC	IA	Comment / Reason if Inapplicable
RE	Requirements Elicitation				
RE.SM	Supplier Management				
RE.SM.a4	Do you specify all external systems and safety-related software?				
RE.SM.a5	Do you establish and maintain detailed system integration procedures for the external systems and safety-related software?				
RE.SM.a6	Do you define the safety standards that suppliers must follow?				
DS	Documentation and Requirements Specification				
DS.HF	Human Factors				
DS.HF.a2	Do you document human factors design and analysis?				
DS.HF.a3	Do you evaluate prototypes, requirements and technical UI restrictions?				
DS.HF.a2	Do you document human factors design and analysis?				
DS.SDO	Safety Documentation				
DS.SDO.a2	Do you ensure that safety requirements are incorporated into system and subsystem specifications, including human-machine interface requirements?				
DS.SDO.a3	Do you document all lifecycle and modification activities?				
DS.SDO.a5	Do you document System Limitations?				
DS.SDO.a10	Do you include a summary of safety requirements?				
RA	Requirements Analysis				
RA. PSA	Preliminary Safety Analysis				
RA. PSA.a1	Do you identify and document safety-critical computer software components and units?				
RA. PSA.a3	Do you identify and document system hazards?				
RA. PSA.a4	Do you identify and document hazards, hazardous situations and harmful events due to interaction with other equipment or systems (installed or to be installed)?				
RA. PSA.a5	Do you specify the type of initiating events that need to be considered?				
RA. PSA.a6	Do you obtain and document information about the determined hazards (causes, probability, severity, duration, intensity, toxicity, exposure limit, mechanical force, explosive conditions, reactivity, flammability etc.) ?				
RA. PSA.a7	Do you identify and document hazardous materials?				
RA. PSA.a8	Do you identify and document consequences of hazards, severity categories and affected assets?				
RA. PSA.a9	Do you conduct risk estimation?				
RA. PSA.a10	Do you conduct risk evaluation for each identified hazard?				
RA. PSA.a11	Do you identify and document risk mitigation procedures for each identified hazard?				
RA. PSA.a13	Do you identify and document pure safety requirements?				
RA. PSA.a14	Do you identify and document safety-significant requirements and safety integrity levels?				
RA. PSA.a15	Do you identify and document safety constraints and how they could be violated?				
RA. PSA.a16	Do you identify and document possible control flaws and inadequate control actions?				
RA. PSA.a17	Do you identify and document safety functional requirements?				
RA. PSA.a18	Do you identify and document operational requirements?				
RA. PSA.a21	Do you identify and document analysis and verification requirements, possible safety-interface problems, including the human-machine interface, and operating support requirements?				
RA. PSA.a23	Do you consolidate preliminary system safety technical specification?				
RA.FH	Failure Handling				
RA.FH.a1	Do you define requirements for the avoidance of systematic faults?				
RA.FH.a2	Do you specify Fault-detection procedures?				
RA.FH.a3	Do you specify Restart-up procedures?				
RA.FH.a6	Do you perform reliability and system performance analysis?				

Level 1 - Basic					
RP	Release Planning				
RP.SC	Safety Certification				
RP.SC.a2	Do you demonstrate the preliminary level of safety achieved by the system?				
RP.SC.a3	Do you evaluate the threat to society from the hazards that cannot be eliminated or avoided?				
RP.SC.a4	Do you construct preliminary safety and hazard reports?				
RP.SC.a5	Do you construct preliminary safety cases?				
RP.SC.a9	Do you specify a maintenance plan?				
RV	Requirements Validation				
RV.SVV	Safety Validation and Verification				
RV.SVV.a1	Do you define the safety validation plan for software aspects of system safety?				
RV.SVV.a2	Do you define the safety verification plan?				
RV.SVV.a6	Do you define and maintain a software integration test plan?				
RV.SVV.a9	Do you perform safety evaluation and verification at the system and subsystem levels?				
OS	Organizational Support				
OS.SP	Safety Planning				
OS.SP.a1	Do you develop an integrated system safety program plan?				
OS.SP.a3	Do you define and document the interface between system safety and all other applicable safety disciplines?				
OS.SP.a4	Do you delineate the scope of safety analysis?				
OS.SP.a5	Do you establish the hazards auditing and log file?				
OS.SP.a6	Do you establish working groups and structures?				
OS.SP.a7	Do you define and document the regulations and safety standards to be followed?				
OS.SP.a8	Do you identify any certification requirements for software, safety or warning devices or other special safety feature?				
OS.SP.a12	Do you specify operating conditions of the machine and installation conditions of the electronic parts?				
OS.SP.a13	Do you determine the required performance level?				
OS.SP.a14	Do you identify and document the hazard analysis to be performed; the analytical techniques (qualitative or quantitative) to be used; and depth within the system that each analytical technique will be used (e.g., system level, subsystem level, component level) ?				
OS.GSM	General Safety Management				
OS.GSM.a1	Do you identify and document the system development methodology?				
OS.GSM.a2	Do you identify and document safety lifecycle for the system development?				
OS.GSM.a3	Do you identify and document competence requirements for the safety activities?				
OS.GSM.a4	Do you set safety policy and define safety goals?				
OS.GSM.a5	Do you identify and document responsibility, accountability and authority?				
OS.GSM.a6	Do you define system safety program milestones and relate these to major program milestones, program element responsibility, and required inputs and outputs?				
PM	Requirements Process Management				
PM.SCM	Safety Configuration Management				
PM.SCM.a3	Do you define and document safety configuration items to be included in the baseline?				
PM.SCM.a5	Do you document the release of safety-related software?				
PM.SCM.a7	Do you specify and follow the template for software modification request?				
PM.SCO	Safety Communication				
PM.SCO.a2	Do you define a method of exchanging safety information with the suppliers?				
PM.SCO.a3	Do you establish a common nomenclature?				
PM.SCO.a4	Do you train people continuously in system engineering and safety techniques (education) ?				
PM.SCO.a8	Do you define and follow templates for system artifacts?				
PM.SCO.a9	Do you document how conflicts will be resolved?				
PM.SCO.a10	Do you identify, record and resolve conflicts?				

Level 1 - Basic					
PM.SCO.a12	Do you make available safety-related software specification to every person involved in the lifecycle?				

Level 2- Intermediate					
Action ID	Question	C	IC	IA	Comment / Reason if Inapplicable
RE	Requirements Elicitation				
RE.SM	Supplier Management				
RE.SM.a1	Do you establish and maintain formal agreements among organization and suppliers?				
RE.SM.a2	Do you identify and document the products to be acquired?				
RE.SM.a3	Do you select suppliers and record rationale?				
DS	Documentation and Requirements Specification				
DS.HF	Human Factors				
DS.HF.a1	Do you construct operator task models				
DS.HF.a4	Do you model and evaluate operator tasks and component black-box behavior				
DS.HF.a5	Do you define interfaces considering ergonomic principles				
DS.HF.a6	Do you specify Human Machine Interface requirements				
DS.SDO	Safety Documentation				
DS.SDO.a4	Do you develop and document training, operational and software user manuals?				
DS.SDO.a6	Do you provide a safety manual?				
DS.SDO.a7	Do you document lessons learned?				
DS.SDO.a8	Do you ensure that safety-related information is incorporated into user and maintenance documents?				
RA	Requirements Analysis				
RA. PSA	Preliminary Safety Analysis				
RA. PSA.a19	Do you perform and document the feasibility evaluation of safety functional requirements?				
RA. PSA.a20	Do you prioritize hazards and safety requirements?				
RA. PSA.a22	Do you perform interface analysis, including interfaces within subsystems (such as between safety-critical and non-safety-critical software components) ?				
RA.FH	Failure Handling				
RA.FH.a4	Do you document the system behavioral model?				
RA.FH.a5	Do you identify and document Common-cause failures (CCF) and how to prevent them?				
RP	Release Planning				
RP.SC	Safety Certification				
RP.SC.a1	Do you conduct safety audits?				
RP.SC.a6	Do you demonstrate preliminary compliance with safety standards?				
RP.SC.a8	Do you document the division of responsibility for system certification and compliance with safety standards during safety planning?				
RV	Requirements Validation				
RV.SVV	Safety Validation and Verification				
RV.SVV.a3	Do you define the technical strategy for the validation of external systems and safety-related software?				
RV.SVV.a4	Do you define pass/fail criteria for accomplishing software validation and verification?				
RV.SVV.a5	Do you develop safety test plans, test descriptions, test procedures, and validation and verification safety requirements?				
RV.SVV.a7	Do you validate safety-related software aspects?				
RV.SVV.a8	Do you ensure that there is no potentially hazardous control actions?				
RV.SVV.a10	Do you conduct joint reviews (company and customer)?				
RV.SVV.a11	Do you ensure that the stakeholders understand software-related system safety requirements and constraints?				
RV.SVV.a12	Do you document discrepancies between expected and actual results?				
RV.SVV.a13	Do you verify the behavioral model?				

Level 2- Intermediate					
RV.SVV.a14	Do you ensure that software requirements and interface specification are consistent?				
RV.SVV.a15	Do you perform safety inspections?				
RV.SVV.a16	Do you identify and fix inconsistencies safety requirements specification?				
OS	Organizational Support				
OS.SP	Safety Planning				
OS.SP.a2	Do you define and document requirements for periodic functional safety audits?				
OS.SP.a10	Do you review safety experience on similar systems?				
OS.GSM	General Safety Management				
OS.GSM.a8	Do you prepare progress reports in a period of time defined by the project?				
OS.GSM.a9	Do you monitor project and take corrective actions?				
OS. STO	Safety Tool support				
OS. STO.a1	Do you use of verification and validation tools ?				
OS. STO.a4	Do you record information of the tools in the baseline?				
OS. STO.a6	Do you use of computer-aided specification tools?				
OS. SKM	Safety Knowledge Management				
OS. SKM.a5	Do you document a strategy to manage the knowledge?				
OS. SKM.a6	Do you define a lifecycle for projects artifacts?				
PM	Requirements Process Management				
PM.SCM	Safety Configuration Management				
PM.SCM.a6	Do you perform safety impact analysis on changes?				
PM.SCM.a8	Do you document the procedures for initiating modifications to the safety-related systems, and to obtain approval and authority for modifications?				
PM.SCM.a9	Do you maintain and make available the software configuration management log?				
PM.SCM.a10	Do you appoint all deliverable documents according to the rules defined in the Configuration Management Plan?				
PM.SCO	Safety Communication				
PM.SCO.a1	Do you establish formal communication channels among different organizational levels?				

Level 3- Advanced					
Action ID	Question	C	IC	IA	Comment / Reason if Inapplicable
DS.SDO	Safety Documentation				
DS.SDO.a1	Do you record safety decisions and rationale?				
DS.SDO.a9	Do you maintain hazard and risk analysis results for the system throughout the overall safety lifecycle?				
RA	Requirements Analysis				
RA. PSA	Preliminary Safety Analysis				
RA. PSA.a2	Do you simulate the process?				
RA. PSA.a12	Do you collect safety requirements from multiple viewpoints?				
RP	Release Planning				
RP.SC	Safety Certification				
RP.SC.a7	Do you ensure that the hazard report is updated with embedded links to the resolution of each hazard, such as safety functional requirements, safety constraints, operational requirements, and system limitations?				
OS	Organizational Support				
OS.SP	Safety Planning				
OS.SP.a9	Do you define and document requirements completeness criteria and safety criteria?				
OS.SP.a11	Do you specify the general safety control structure?				
OS.GSM	General Safety Management				
OS.GSM.a7	Do you use of indicators on engineering documentation to assess the product properties and the development progress?				
OS.STO	Safety Tool support				

Level 3- Advanced					
OS.STO.a2	Do you specify justifications for the selection of the off-line support tools?				
OS.STO.a3	Do you assess offline support tools which can directly or indirectly contribute to the executable code of the safety related system?				
OS.STO.a5	Do you use of tools with support to cross referencing and maintain the traceability among safety information in the software specification?				
OS.STO.a7	Do you define and use tools to support the safety process and workflow management?				
OS.SKM	Safety Knowledge Management				
OS.SKM.a1	Do you establish and maintain an infrastructure to share knowledge?				
OS.SKM.a2	Do you develop a safety information system to share knowledge in the organization?				
OS.SKM.a3	Do you define control access mechanisms to the safety information system?				
OS.SKM.a4	Do you maintain employees competence information?				
OS.SKM.a7	Do you define and maintain a strategy for reuse?				
OS.SKM.a8	Do you reuse the stored knowledge?				
OS.SKM.a9	Do you document the use of stored knowledge?				
OS.SKM.a10	Do you notify users about problems, new versions and exclusions of artifacts in use?				
OS.SKM.a11	Do you manage assets?				
PM	Requirements Process Management				
PM.SCM	Safety Configuration Management				
PM.SCM.a1	Do you maintain accurately and with unique identification all safety configuration items and safety information (hazards, safety requirements, risks, etc.)				
PM.SCM.a2	Do you define and document change-control procedures				
PM.SCM.a4	Do you document configuration status, release status, the justification (taking account of the impact analysis) for and approval of all modifications, and the details of the modification				
PM.SCM.a11	Do you upload all documents on the safety information system				
PM.SCO	Safety Communication				
PM.SCO.a5	Do you use of a common safety information system for system specification and safety analysis				
PM.SCO.a6	Do you keep stakeholders updated regarding the progress of all safety-related activities				
PM.ST	Safety Traceability				
PM.ST.a1	Do you define and maintain traceability policies?				
PM.ST.a2	Do you define and maintain bi-directional traceability between the system safety requirements and the software safety requirements?				
PM.ST.a3	Do you define and maintain bi-directional traceability between the safety requirements and the perceived safety needs?				
PM.ST.a4	Do you link and maintain bi-directional between environmental assumptions and the parts of the hazard analysis based on the assumption ?				
PM.ST.a5	Do you define and maintain bi-directional traceability between system and subsystem verification results and system specification?				
PM.ST.a6	Do you define and maintain bi-directional traceability between validation results and system specification?				
PM.ST.a7	Do you define and maintain bi-directional traceability among system hazards into components?				
PM.ST.a8	Do you justify reasons for not traced software requirements?				