Collaborative Large-scale Integrating Project

Open Platform for EvolutioNary Certification Of Safety-critical Systems

List of proposed requirements for Automotive domain
Annex D1.1.a to deliverable D1.1

Work Package:	WP1: Use case Specification and Benchmark
Dissemination level:	PU = Public
Status:	FINAL
Date:	28 March 2012
Responsible partner:	F. Tagliabò (CRF)
Contact information:	fulvio.tagliabo@crf.it

Contributors

Names	Organisation
Fulvio Tagliabò, Alberto Melzi	Centro Ricerche Fiat S.C.p.A.

Document History

Version	Date	Remarks
V0.1	2012-01-23	First emission (CRF)
V0.2	2012-03-16	General revision (CRF)
V0.3	2012-03-20	Ready for PB Approval
V1.0	2012-03-28	Approved by PB

TABLE OF CONTENTS

1 SAFETY POLICY

The proposed automotive requirements which constitute “Safety Policy”, according to the reference standard, are detailed in the following:

<CRF> 0001: <Safety Culture>	
Alias	Organization specific rules and processes for functional safety
Status	Proposed
App. Domain	Automotive
Type	Safety Policy
Priority	High
Description	To evaluate internally to the organization the availability of safety culture that supports and encourages the effective achievement of functional safety
Derived from	ISO 26262 Part 2

<CRF> 0001.a: <Safety Culture>	
Alias	Proactive attitude towards safety
Status	Proposed
App. Domain	Automotive
Type	Safety Policy
Priority	High
Description	Safety and quality issues are discovered and resolved from the earliest stage in the product lifecycle
Derived from	ISO 26262 Part 2

<CRF> 0001.b: <Safety Culture>	
Alias	Independence of checks and balances
Status	Proposed
App. Domain	Automotive
Type	Safety Policy
Priority	High
Description	Appropriate degree of independence in the integral processes (safety, quality, verification, validation and management)
Derived from	ISO 26262 Part 2

<CRF> 0009: <Safety culture>	
Alias	Evidence of field monitoring
Status	Proposed
App. Domain	Automotive
Type	Safety Policy
Priority	High
Description	The organization shall institute, execute and maintain a field monitoring process with respect to the item's functional safety (including the reporting of incidents, the measures for correction, the recall and the corresponding decision-making processes)
Derived from	ISO 26262 Part 2

<CRF> 0002: <Safety Competences>	
Alias	Evidence of competence
Status	Proposed
App. Domain	Automotive
Type	Safety Policy
Priority	High
Description	To evaluate internally that the organization involves persons with competences and categories corresponding to their responsibility and the same for its suppliers
Derived from	ISO 26262 Part 2

<CRF> 0003: <Quality standard>	
Alias	Evidence of quality management
Status	Proposed
App. Domain	Automotive
Type	Safety Policy
Priority	High
Description	To evaluate internally that the organization is compliant with quality reference standards
Derived from	ISO 26262 Part 2

2 SAFETY PROCESSES

2.1 System level

The proposed automotive requirements which constitute “Safety Processes” at System level, according to the reference standard, are detailed in the following:

<CRF> 0008a: <Audit>	
Alias	Review of the configuration management process
Status	Proposed
App. Domain	Automotive
Type	Safety Processes
Priority	High
Description	The review applies to the process that aims: - to ensure that the work products, and the principles and general conditions of their creation, can be uniquely identified and reproduced in a controlled manner at any time - to ensure that the relations and differences between earlier and current versions can be traced
Derived from	ISO 26262 Part 8 (Part 2)

<CRF> 0008b: <Audit>	
Alias	Review of distributed development management (in case of supplier)
Status	Proposed
App. Domain	Automotive
Type	Safety Processes
Priority	High
Description	Review of the management of the work products from #104 to #109 (with related documentation)
Derived from	ISO 26262 Part 8 (Part 2)

<CRF> 0008c: <Audit>	
Alias	Review of the change management process
Status	Proposed
App. Domain	Automotive
Type	Safety Processes
Priority	High
Description	Review of the process that aims to analyse and control changes to safety-related work products throughout the entire safety lifecycle: the change management ensures the systematic planning, control, monitoring, implementation and documentation of changes, while maintaining the consistency of each work product
Derived from	ISO 26262 Part 8 (Part 2)

<CRF> 0008d: <Audit>	
Alias	Review of the verification process
Status	Proposed
App. Domain	Automotive
Type	Safety Processes
Priority	High
Description	The review applies to the process that aims to ensure that the work products for each phase of the safety lifecycle (concept, design, testing, production and operation) of the item comply with their requirements.
Derived from	ISO 26262 Part 8 (Part 2)

<CRF> 0008e: <Audit>	
Alias	Review of the documentation process
Status	Proposed
App. Domain	Automotive
Type	Safety Processes
Priority	High
Description	Review for evaluating the documentation development management strategy for the entire safety lifecycle with respect to the capability to facilitate an effective and repeatable documentation, with a suitable guideline defined in order to guarantee the proper identification, maintainability, change history, traceability of each document
Derived from	ISO 26262 Part 8 (Part 2)

<CRF> 0008f: <Audit>	
Alias	Review of the qualification of SW components
Status	Proposed
App. Domain	Automotive
Type	Safety Processes
Priority	High
Description	Review of the process for the qualification of software components, that provides evidence of their suitability for re-use in items developed in compliance with the reference standard
Derived from	ISO 26262 Part 8 (Part 2)

<CRF> 0008g: <Audit>	
Alias	Review of the qualification of HW components
Status	Proposed
App. Domain	Automotive
Type	Safety Processes
Priority	High
Description	Review of the process for the qualification of hardware components, that provides evidence of their suitability for re-use in items developed in compliance with the reference standard
Derived from	ISO 26262 Part 8 (Part 2)

2.2 Supporting process level

The proposed automotive requirements which constitute “Safety Processes” at Supporting Process level according to the reference standard, from ISO 26262 – Part 8, are detailed in the following:

For managing interfaces within distributed developments (case of supplier):

AUDIT

104	Supplier selection report

COMPLETENESS AND COMPLIANCE WITH REF. STD

105	Development Interface Agreement (DIA) (To give the safety goals and the safety requirements to the involved supplier(s), defining them by a specific document)
106	Supplier's project plan
107	Supplier's safety plan
108	Function safety assessment report at supplier’s premises
109	Supply agreement

For general management:

COMPLETENESS AND COMPLIANCE WITH REF. STD

110	Configuration management plan
111	Change management plan (for analyzing and controlling changes to safety-related work products throughout the safety lifecycle)
112	Change request
113	Impact analysis and change request plan
114	Change report
115	Verification plan (for ensuring that the work products comply with their requirements)
116	Verification specification
117	Verification report
118	Document management plan
119	Documentation guideline requirements
120	Software tool criteria evaluation report
121	Software tool qualification report
122	Software component documentation
123	Software component qualification report
125	Qualification plan
126	Hardware component test plan
127	Qualification report
129	Definition of a candidate for proven in use argument
130	Proven in use analysis reports

3 SAFETY PLANNING

3.1 Management, Concept and System level

The proposed automotive requirements which constitute "Safety Planning" according to the reference standard in relation to Safety Management, Concept and System levels, are detailed in the following:

<CRF> 0004: <Safety plan>	
Alias	Safety plan
Status	Proposed
App. Domain	Automotive
Type	Safety Planning
Priority	High
Description	The initial general planning of the activities and procedures for achieving the functional safety goals of the item under development
Derived from	ISO 26262 Part 2

<CRF> 0007: <Safety plan>	
Alias	Functional safety assessment plan
Status	Proposed
App. Domain	Automotive
Type	Safety Planning
Priority	High
Description	The general planning of the actions for assessing the functional safety compliance with the reference standard of the item under development
Derived from	ISO 26262 Part 2

<CRF> 0012: <Safety plan>	
Alias	Safety plan (refined after tailoring)
Status	Proposed
App. Domain	Automotive
Type	Safety Planning
Priority	High
Description	The general revision of the safety plan after the results of tailoring
Derived from	ISO 26262 Part 3

<CRF> 0019: <Safety plan>	
Alias	Safety plan (refined at system design level)
Status	Proposed
App. Domain	Automotive
Type	Safety Planning
Priority	High
Description	The revision of the safety plan et the system level: this is the planning of the functional safety assessment activities for the product development at the system design level
Derived from	ISO 26262 Part 4

<CRF> 0022: <Safety plan>	
Alias	Functional safety assessment plan (refined at system design level)
Status	Proposed
App. Domain	Automotive
Type	Safety Planning
Priority	High
Description	Planning of functional safety assessment activities for the product development at the system during design phase
Derived from	ISO 26262 Part 4

<CRF> 0085: <Safety plan>	
Alias	Validation plan (refined at system design level)
Status	Proposed
App. Domain	Automotive
Type	Safety Planning
Priority	High
Description	Validation plan (refined at system design level)
Derived from	ISO 26262 Part 4

<CRF> 0005: <Conformity plan>	
Alias	Project plan (refined with reference to the safety plan)
Status	Proposed
App. Domain	Automotive
Type	Safety Planning
Priority	High
Description	The general revision of the first planning of the activities and procedures with reference to the plan for achieving the functional safety goals of the item under development
Derived from	ISO 26262 Part 2

<CRF> 0018: <Conformity plan>	
Alias	Project plan (refined at system design level)
Status	Proposed
App. Domain	Automotive
Type	Safety Planning
Priority	High
Description	The safety activities for the product development at the system level shall be planned including determination of appropriate methods and measures during design and integration
Derived from	ISO 26262 Part 3

<CRF> 0020: <Conformity plan>	
Alias	Item integration and testing plan
Status	Proposed
App. Domain	Automotive
Type	Safety Planning
Priority	High
Description	The results of planning of the verification activities during design are part of the safety plan while the planning of item integration and is represented in a separate item integration and testing plan
Derived from	ISO 26262 Part 4

<CRF> 0021: <Conformity plan>	
Alias	Validation plan
Status	Proposed
App. Domain	Automotive
Type	Safety Planning
Priority	High
Description	Planning of the validation activities during design phase
Derived from	ISO 26262 Part 4

<CRF> 0025: <Conformity plan>	
Alias	Validation plan (refined at system design level)
Status	Proposed
App. Domain	Automotive
Type	Safety Planning
Priority	High
Description	The criteria for safety validation of the item during design phase shall be refined based on the technical safety requirements
Derived from	ISO 26262 Part 4

<CRF> 0082: <Conformity plan>	
Alias	Item integration and testing plan (refined at system level)
Status	Proposed
App. Domain	Automotive
Type	Safety Planning
Priority	High
Description	Item integration and testing plan (refined at system level)
Derived from	ISO 26262 Part 4

<CRF> 0085: <Conformity plan>	
Alias	Validation plan (refined – for the item integrated in a representative vehicle)
Status	Proposed
App. Domain	Automotive
Type	Safety Planning
Priority	High
Description	Validation plan refined for the item integrated in a representative vehicle
Derived from	ISO 26262 Part 4

3.2 Hardware level

The proposed automotive requirements which constitute "Safety Planning" at Hardware level for production development, from ISO 26262 – Part 5, are detailed in the following:

<CRF> 0032: <Safety plan>	
Alias	Safety plan (refined at HW level)
Status	Proposed
App. Domain	Automotive
Type	Safety Planning
Priority	High
Description	The safety plan shall be detailed, including determination of appropriate methods and measures, with respect to the activities for the product development at the hardware level, consistent with the planning of activities
Derived from	ISO 26262 Part 5

<CRF> 0046: <Conformity plan>	
Alias	Planning and execution of HW component tests
Status	Proposed
App. Domain	Automotive
Type	Safety Planning
Priority	High
Description	Planning and execution of HW component tests
Derived from	ISO 26262 Part 5

3.3 Software level

The proposed automotive requirements which constitute "Safety Planning" at Software level for production development, from ISO 26262 – Part 6, are listed more briefly resumed for Sub-Type in the following:

SAFETY PLAN

47	Safety plan (refined – SW starting level)
56	Safety plan (refined – at SW architectural level)
76	Safety plan (refined at SW level after configuration and calibration specification)

CONFORMITY PLAN

48	Software verification plan
53	Software verification plan (refined – at level of SW safety requirements and of the refined specification of the HW-SW interface)
64	Software verification plan (refined – at SW functionality level – testing plan)
67	Software verification plan (refined – at SW integration level)
71	Software verification plan (refined – at SW embedded level)
79	Software verification plan (refined with configuration and calibration data - Capability of enabling controlled changes in the behaviour of the software for different applications)

3.4 Supporting process level

The proposed automotive requirements which constitute “Safety Planning” at Supporting Process, from ISO 26262 – Part 8, are listed more briefly resumed in the following:

SAFETY PLAN

124	Safety plan (refined – with software component qualification planning)
128	Safety Plan (refined – at proven in use argument level)

4 SAFETY PRODUCT

4.1 Management, Concept and System level

The proposed automotive requirements which constitute "safety product" according to the reference standard in relation to Safety Management, Concept and System levels, are detailed in the following:

<CRF> 0008: <Safety measures review >	
Alias	Confirmation measure reports
Status	Proposed
App. Domain	Automotive
Type	Safety Product
Priority	High
Description	Reporting of all the reviews done on the confirmation measures: •Confirmation review of the hazard analysis and risk assessment •Confirmation review of safety plan •Confirmation review of the safety analyses •Confirmation review of the qualification of software tools •Confirmation review of the proven in use arguments of the candidates, if applicable •Confirmation review of the item integration and testing plan •Confirmation review of the validation plan •Confirmation review report of the completeness of the safety case •Functional safety assessment audit
Derived from	ISO 26262 Part 2

<CRF> 0010: <Boundary definition >	
Alias	Item definition
Status	Proposed
App. Domain	Automotive
Type	Safety Product
Priority	High
Description	Complete definition of the item under development
Derived from	ISO 26262 Part 3

<CRF> 0011: <Boundary definition >	
Alias	Impact analysis
Status	Proposed
App. Domain	Automotive
Type	Safety Product
Priority	High
Description	An analysis that has the aim to identify and describe the intended modification applied to the item or its environment and to assess the impact of these modifications
Derived from	ISO 26262 Part 3

<CRF> 0014: < Boundary definition >	
Alias	Safety goals
Status	Proposed
App. Domain	Automotive
Type	Safety Product
Priority	High
Description	Safety goals are top-level safety requirements for the item: they lead to the functional safety requirements needed to avoid an unreasonable risk for each hazardous event; they are not expressed in terms of technological solutions, but in terms of functional objectives
Derived from	ISO 26262 Part 3

<CRF> 0016: <Boundary definition >	
Alias	Functional safety concept
Status	Proposed
App. Domain	Automotive
Type	Safety Product
Priority	High
Description	The objective of the functional safety concept is to derive the functional safety requirements from the safety goals and to allocate them to the preliminary architectural elements of the item, or to external measures
Derived from	ISO 26262 Part 3

<CRF> 0023: <Boundary definition >	
Alias	Technical safety requirements specification
Status	Proposed
App. Domain	Automotive
Type	Safety Product
Priority	High
Description	Specification of the technical safety requirements in accordance with the functional safety concept, the preliminary architectural assumptions of the item and the following system properties
Derived from	ISO 26262 Part 4

<CRF> 0026: <Boundary definition >	
Alias	Technical safety concept
Status	Proposed
App. Domain	Automotive
Type	Safety Product
Priority	High
Description	Implementation of the technical safety requirements at system design level
Derived from	ISO 26262 Part 4

<CRF> 0027: <Boundary definition >	
Alias	System design specification
Status	Proposed
App. Domain	Automotive
Type	Safety Product
Priority	High
Description	The system design shall be based on the functional concept, the preliminary architectural assumptions and the technical safety requirements
Derived from	ISO 26262 Part 4

<CRF> 0028: <Boundary definition >	
Alias	HW-SW Interface specification (HSI)
Status	Proposed
App. Domain	Automotive
Type	Safety Product
Priority	High
Description	Specification of the hardware and software interaction that must be consistent with the technical safety concept. This includes the component's hardware devices, that are controlled by software and hardware resources that support the execution of software
Derived from	ISO 26262 Part 4

<CRF> 0029: <Boundary definition >	
Alias	Specification of requirements for production, operation, service and decommissioning
Status	Proposed
App. Domain	Automotive
Type	Safety Product
Priority	High
Description	Diagnostic features shall be specified to provide the required data that enables field monitoring for the item or its elements during production, operation, service and decommissioning, assuring the compliance with the results of the safety analyses and the implemented safety mechanisms
Derived from	ISO 26262 Part 4

<CRF> 0013: <Hazard analysis and risk assessment >	
Alias	Hazard analysis and risk assessment
Status	Proposed
App. Domain	Automotive
Type	Safety Product
Priority	High
Description	To identify and to categorise the hazards in the item under development and to formulate the safety goals related to the prevention or mitigation of the hazardous events
Derived from	ISO 26262 Part 3

<CRF> 0006: <Safety Case>	
Alias	Safety Case
Status	Proposed
App. Domain	Automotive
Type	Safety Product
Priority	High
Description	Progressive compilation of the work products that are generated during the safety lifecycle
Derived from	ISO 26262 Part 2

<CRF> 0015: <Verification and validation review of the results >	
Alias	Verification review report of the hazard analysis and risk assessment and the safety goals
Status	Proposed
App. Domain	Automotive
Type	Safety Product
Priority	High
Description	The hazard analysis, risk assessment and the safety goals shall be verified in accordance with the reference standard showing the evidence of: a)completeness with regard to situations and hazards b) compliance with the item definition c) consistency with related hazard analyses and risk assessments d) completeness of the coverage of the hazardous events e) consistency of the assigned ASILs with the corresponding hazardous events
Derived from	ISO 26262 Part 3

<CRF> 0017: <Verification and validation review of the results >	
Alias	Verification report of the functional safety concept
Status	Proposed
App. Domain	Automotive
Type	Safety Product
Priority	High
Description	The functional safety concept shall be verified to show: a) its consistency and compliance with the safety goals b) its ability to mitigate or avoid the hazardous events The ability to mitigate or to avoid a hazardous event can be evaluated by tests, trials or expert judgement, prototypes, studies, subject tests, simulations
Derived from	ISO 26262 Part 3

<CRF> 0024: <Verification and validation review of the results >	
Alias	System safety verification report
Status	Proposed
App. Domain	Automotive
Type	Safety Product
Priority	High
Description	Technical safety requirements verification providing evidence for their: a) compliance and consistency with the functional safety concept b) compliance with the preliminary architectural design assumptions
Derived from	ISO 26262 Part 4

<CRF> 0030: <Verification and validation review of the results >	
Alias	System safety verification report (refined)
Status	Proposed
App. Domain	Automotive
Type	Safety Product
Priority	High
Description	The system design shall be verified for compliance and completeness with regard to the technical safety concept through inspection, simulation, prototyping, testing and analyses
Derived from	ISO 26262 Part 4

<CRF> 0031: <Verification and validation review of the results >	
Alias	Safety analysis reports (system level as resulting from requirement)
Status	Proposed
App. Domain	Automotive
Type	Safety Product
Priority	High
Description	Safety analyses (qualitative/quantitative) on the system level design to identify the causes of systematic failures and the effects of systematic faults shall be applied in accordance with reference standard (for example: deductive analysis methods including FTA, reliability block diagrams, Ishikawa diagram; inductive analysis methods including FMEA, ETA, Markov modelling)
Derived from	ISO 26262 Part 4

4.2 System testing/validation level

The proposed automotive requirements which constitute “Safety Product” according to the reference standard in relation to System level testing validation, from ISO 26262 – Part 4, continue in a brief summary in the following:

BOUNDARY DEFINITION

83	Integration testing specification(s)

SAFETY MEASURES REVIEW

86	Validation of system concerning torque monitoring on vehicle level – For electric vehicles
87	Validation of system concerning HV (High Voltage) on vehicle level – For hybrid/electric vehicles
88	Real-life validation (effectiveness of safety measures)

VERIFICATION AND VALIDATION REVIEW OF THE RESULTS

89	Validation report (at vehicle level about: a) the controllability b) the effectiveness of safety measures for controlling random and systematic failures c) the effectiveness of the external measures d) the effectiveness of the elements of other technologies)
90	Release of components (supplier's release)

And as final certification assessment:

<CRF> 0091: <Verification and validation review of the results >	
Alias	Functional safety assessment report
Status	Proposed
App. Domain	Automotive
Type	Safety Product
Priority	High
Description	For each step of the safety lifecycle, as defined in the reference standard, the specific topics to be addressed by the functional safety assessment shall be identified, producing the final Functional safety assessment report based on : – safety case – safety plan (refined) – confirmation review reports – audit reports (if available) – functional safety assessment plan (refined)
Derived from	ISO 26262 Part 4

<CRF> 0092: <Verification and validation review of the results >	
Alias	Release for production report
Status	Proposed
App. Domain	Automotive
Type	Safety Product
Priority	High
Description	Provided the prerequisites: – functional safety assessment report – safety case This report is the complete documentation of functional safety for release for production and shall include the following information: a) the name and signature of the person responsible for release b) the version(s) of the released item c) the configuration of the released item d) references to associated documents e) the release date
Derived from	ISO 26262 Part 4

4.3 Hardware level

The proposed automotive requirements which constitute “Safety Product” at Hardware level for production development, from ISO 26262 – Part 5, are listed more briefly resumed for Sub-Type in the following:

BOUNDARY DEFINITION

33	Hardware safety requirements specification (including test and qualification criteria)
34	HW-SW Interface specification (HSI refined)
36	Hardware design specification
39	Specification of requirements related to production, operation, service and decommissioning

43	Specification of dedicated measures for hardware, if needed, including the rationale regarding the effectiveness of the dedicated measures

HAZARD ANALYSIS AND RISK ASSESSMENT REVIEW

42	Analysis of safety goal violations due to random hardware failures

SAFETY CASE

40	Analysis of the effectiveness of the architecture of the item to cope with the random hardware failures

SAFETY MEASURES REVIEW

41	Review report of evaluation of the effectiveness of the architecture of the item to cope with the random hardware failures
44	Review report of evaluation of safety goal violations due to random hardware failures

VERIFICATION AND VALIDATION REVIEW OF THE RESULTS

35	Hardware safety requirements verification report
37	Hardware safety analysis report
38	Hardware design verification report
45	Hardware integration and testing report

4.4 Software level

The proposed automotive requirements which constitute “Safety Product” at Software level for production development, from ISO 26262 – Part 6, are listed more briefly resumed for Sub-Type in the following:

BOUNDARY DEFINITION

49	Design and coding guidelines for modeling and programming languages
50	Tool application guidelines
51	Software safety requirements specification
52	HW-SW Interface specification (refined)
55	Software architectural design specification
57	Software safety requirements specification (refined - as a result of the allocation of the requirements with the highest ASIL to each software component)
61	Software unit design specification
62	Software unit implementation (Summary of design principles for software unit design and implementation at the source code level to be applied to achieve general quality standards and robustness)
65	Software verification specification
68	Software verification specification (refined – after integration)
69	Embedded software (SW integration)
72	Software verification specification (refined – SW embedded)
74	Configuration data specification
75	Calibration data specification
77	Configuration data
78	Calibration data
80	Verification specification (of configuration and calibration data)

HAZARD ANALYSIS AND RISK ASSESSMENT REVIEW

59	Dependent failures analysis report

SAFETY MEASURES REVIEW

54	Software verification report (Verification of software safety requirements and the refined hardware-software interface requirements to show their: a) compliance and consistency with the technical safety requirements b) compliance with the system design c) consistency with the hardware-software interface)
58	Software safety analysis report (identify/confirm the safety-related parts of the software; support the specification and verify the efficiency of the safety mechanisms)
60	Software verification report (refined – at architectural level)
63	Software verification report (refined – at unit implementation level)
66	Software verification report (refined – at functionality level – units functional testing)
70	Software verification report (refined – at elements integration level – architectural testing)
73	Software verification report (refined – at safety level)

VERIFICATION AND VALIDATION REVIEW OF THE RESULTS

81	Verification report (with configuration and calibration data – Capability of enabling controlled changes in the behaviour of the software for different applications)

4.5 Production and Operation

The proposed automotive requirements which constitute “Safety Product” according to the reference standard in relation to Production and Operation level, from ISO 26262 – Part 7, is listed in a brief summary as following:

BOUNDARY DEFINITION

93	Safety-related content of the production plan
94	Safety-related content of the production control plan including the test plan, resulting from requirements
96	If applicable, requirements specification on the producibility at system, hardware or software development level and appended to the relevant documentation of the corresponding phases
98	Safety-related content of the maintenance plan
99	Repair instructions resulting
100	Safety-related content of the information made available to the user
101	Instructions regarding field observations resulting from requirement
102	Safety-related content of the instructions for decommissioning
103	If applicable, requirements specification relating to operation, service and decommissioning at system hardware or software development level

SAFETY MEASURES REVIEW

95	Control measures report (control date, identification of controlled object and control results)

VERIFICATION AND VALIDATION REVIEW OF THE RESULTS

97	Assessment report for capability of the production process

4.6 ASIL oriented & safety oriented analyses

The proposed automotive requirements which constitute “Safety Product” at ASIL and Safety oriented analyses level, from ISO 26262 – Part 9, are detailed in the following:

<CRF> 0131: <Boundary definition >	
Alias	Update of architectural information
Status	Proposed
App. Domain	Automotive
Type	Safety Product
Priority	High
Description	Update of architectural information
Derived from	ISO 26262 Part 9

<CRF> 0132: <Boundary definition >	
Alias	Update of ASIL as attribute of safety requirements and elements
Status	Proposed
App. Domain	Automotive
Type	Safety Product
Priority	High
Description	Update of ASIL as attribute of safety requirements and elements
Derived from	ISO 26262 Part 9

<CRF> 0133: <Boundary definition >	
Alias	Update of ASIL as attribute of sub-elements of elements
Status	Proposed
App. Domain	Automotive
Type	Safety Product
Priority	High
Description	Update of ASIL as attribute of sub-elements of elements
Derived from	ISO 26262 Part 9

<CRF> 0134: <Boundary definition >	
Alias	Results of analysis of dependent failures
Status	Proposed
App. Domain	Automotive
Type	Safety Product
Priority	High
Description	Results of analysis of dependent failures
Derived from	ISO 26262 Part 9

<CRF> 0135: <Boundary definition >	
Alias	Results of safety analyses
Status	Proposed
App. Domain	Automotive
Type	Safety Product
Priority	High
Description	Results of safety analyses
Derived from	ISO 26262 Part 9