SIEMENS

Document Type	Layout specifications
Title	Safety-Related Application Rules
Project	Systems, Products, Portfolio
Reference-ID	SAR

Protection Class
Restricted

	Name Organizational Unit	Date	Sgd. (electronic signature in EDM) Space for Original Signature
Approved by	Lazos Filippidis MO MM RD CP	2016-02-12	Signed FILIPPI_LAZ
Verified by(*)	Lazos Filippidis MO MM SPP PL Frank Wend MO MM ML PE RAMS Andreas Hildebrand MO MM BE PME Stefan Jung MO MM R&D PPD PT 1 Reßlhuber, Wilfried MO MM BE QM Manfred Schieblich MO MM BE DEV		Signed FILIPPI_LAZ Signed WEND_FRA Signed HILDEBR_AND1 Signed JUNG_STE Signed RESSLHU_WIL Signed SCHIEBL_MAN
Prepared by	Ernesto de Stefano MO MM R&D PTS RAMSS 2 Begoña Tiscar Vega MO MM R&D ES SA	2016-01-28 2016-01-28	Signed STEFANO_ERN Signed Begoña Tiscar Vega

(*) Name etc. or reference to review minutes

Validity and Purpose

Scope

This document describes the standardized

- identifiers

- forms and

- minimum content

that application rules and especially safety-related application rules (SARs) must employ in order to ensure consistent handling of content and additional information throughout MO MM.

In doing so it provides input information for Siemens MO MM with the object of standardizing the handling of SARs.

The present document does not cover the processes for the creation and verification of SARs and the different levels to which they are passed (for example development – configuration or sales – customer).

Contents

List of Tables

1 Application rules

1.1 Definition

SARs within Siemens MO MM must be named consistently both in product and project related documents and in the tools used (for example DOORS).

At the development validation/assessment level, the requirements are to be compiled and consolidated on the basis of relevance (only requirements that are applied at this level) in a single document or in one consistent location in the tool used.

The abbreviation "SAR" has been adopted as it is the same for the German (Sicherheitsrelevante Anwendungs-Regel) and English (safety-related application rule).

Application Rules which are not safety-related should follow the same requirements for SARs .

1.2 Requirements for SARs

The requirements to be met when formulating an SAR are set out in the following.

The associated motivation (why is this rule needed), the solution (how is it possible to comply with this requirement) and the result/verification (how can compliance with the requirement be demonstrated) are presented in part.

Each of the requirements has an identifier, to which reference is made elsewhere in the document.

Identifier	#A1#
Requirement	SARs shall have a clear addressee that will subsequently be responsible for compliance with the rule (for example system engineering, configuration, verification (testing), validation, installation, acceptance, maintenance, operator (where applicable distinction between traffic control/management), decommissioning, etc.).[1] The verification that compliance is possible must be confirmed either by the customer project or the PLM of the product line before the rule is assigned.
Motivation	Rules must be clearly allocated and drafted in such a form that compliance is possible before they can advance to release/assessment.
Solution	The originator can/should include the entities in clarification activities.
Result/verification	For example review minutes. If the addressee is an external organizational unit, for example a customer, the verifying internal organizational unit, for example Sales or PLM, acts as its interface.
Proposal	N/A

Table 1: #A1#

[1] These groups must be defined at a higher level

Identifier	#A2#
Requirement	SARs shall at least be formulated in English, If it´s required in the project, the SAR's have to provide under CM administration additional in other languages.
Motivation	Products including their SARs are often used for application in international projects
Solution	N/A
Result/verification	N/A
Proposal	

Table 2: #A2#

Identifier	#A3#
Requirement	Regarding a complete set of SARs, as many SARs as reasonably practicable shall be combined in a single document or collector that is referenced or included in the safety case document.
Motivation	It should be easy to access SARs in their entirety. Nonetheless it may be sensible to include SARs regarding specific issues (e.g. engineering or maintenance) in dedicated documents which provide valuable or necessary contextual information to understand and adhere to the SARs. Redundant SARs increase the effort and cause confusion when demonstrating adherence to them.
Solution	For example in DOORS with exportable documents with a defined baseline
Result/verification	
Proposal	

Table 3: #A3#

Identifier	#A4#
Requirement	The text block of an SAR shall include sufficient information to represent a self-contained rule (i.e. complete in itself).
Motivation	References to figures, tables or other documents which include information to make the SAR complete in itself, increase the effort and margins for errors.
Solution	
Result/verification	
Proposal	

Table 4: #A4#

Identifier	#A8#
Requirement	The source of an SAR shall be referenced and SAR identifier has to be unique.
Motivation	Traceability (important in connection with queries during the verification process)
Solution	See GUIDE “Configuration Management and Maintenance Plan” (GUIDE_CMMainPl) (A6Z08110483622), section “Identification of Application Conditions”.
Result/verification	
Proposal	

Table 5: #A8#

Identifier	#A10#
Requirement	A description or an example (e.g. reference to demonstration in another project) shall be provided on how to practically adhere to the SAR.
Motivation	Comprehensibility, efficient processing of the requirement, avoidance of misinterpretations
Solution	
Result/verification	
Proposal	

Table 6: #A10#

Identifier	#A12#
Requirement	It shall be clearly stated if it’s safety related and what the consequence will be if the SAR is not adhered to
Motivation	Comprehensibility,
Solution	Problem awareness
Result/verification	
Proposal	The consequence may be explained using a formulation like “In order to prevent…”.

Table 7: #A12#

Note: Variations with respect to the requirements set out above must be cleared with the originator.

1.3 Example

Identifier	#Train_Control_System-01#
Trace from	#TSR_OBU-01# (Requirement identifier of source document or hazard log entry)
Safety Related	YES
In order to prevent accidents normally covered by Train Control System, the driver shall assume full safety responsibility for the operation of a train if he / she activates a cab on a vehicle with cut-off switch in “ATP off” position. If the cut-off switch on a cab is in “ATP off” position, the Rolling Stock cut-off-circuitry bypasses all safety related outputs of the Train Control System.	
Example for practical adherence	-
Severity	Catastrophic
Applicability	Driver/Rail Authority

Table 8: #Train_Control_System-01#

Identifier	#Train_Control_System-02#
Trace from	#TSR_OBU-02# (Requirement identifier of source document or hazard log entry)
Safety Related	YES
In order to prevent an unclear state of safety responsibility at start or restart of the Train Control System the driver shall acknowledge his safety responsibility.	
Example for practical adherence	The engineering/commissioning shall configure the parameter OP_ACK_INIT_STATE to “1” requiring the driver to acknowledge his safety responsibility start or restart of the Train Control System while the cab is activated. The parameter OP_ACK_INIT_STATE is only allowed to be configured to “0” after consultation with the development department to define an adequate safety related application condition for the operator / driver.
Severity	Catastrophic
Applicability	Specific Application Engineering

Table 9: #Train_Control_System-02#

Identifier	#TRAIN_2#
Trace from	#HAZARD_2112# (Requirement identifier of source document or hazard log entry)
Safety Related	YES
In order to prevent an inefficiency train braking and overpassed the limited of movement , Train Manufacturer has to guarantee that the train will brake at least with the brake parameters used by the ATP equipment.	
Example for practical adherence	N-A
Severity	Catastrophic
Applicability	Specific Application Customer

Table 10: #CBTC_ONBOARD_1#

2 About This Document

2.1 Terms and Abbreviations

The following terms are used here:

Term	Explanation
Rule	This term is used in the present document to denote a requirement relating to safety, to differentiate with respect to safety requirements in the sense of safety objectives and as a synonym for the abbreviations SEAR, SAV, SRAC, SDAR and probably many others as well. Other names for rules are operating condition, application condition.
safety objective, safety requirement	A safety objective or safety requirement as described in EN 50126ff is a function to be performed by a fail-safe signaling system in order to ensure that railway operation can be realized safely. It is usually defined as a requirement of the target function, with the integrity requirements derived to this end in the form of the tolerable hazard rate (THR) and the safety integrity level (SIL)
safety related	An attribute designating functions or properties whose object it is to ensure that a safety objective can be achieved. The function or property is absolutely essential as defined in order to achieve the safety objective.
severity	Severity of the hazard where this SRAC has been identified. The values could be catastrophic, critical. Marginal or insignificant

Table 11: Terms

The following abbreviations are used here:

Abbreviation	Term
SEAR	safety-related development/application rule -> SRAC Sicherheitstechnische Entwurfs- und Anwendungsregeln
SAV	safety-related application condition -> SRAC Sicherheitsrelevante Anwendungs-Vorschriften
SAR	safety-related application rule ; sicherheitsrelevante Anwendungs-Regel
SRAC	safety-related application condition (term used in standards)
SDAR	safety- and design-related application rules
GUIDE_CMMainPl	Configuration Management and Maintenance Guideline (A6Z08110483622)

Table 12: Abbreviations

2.2 Document History

Version	Date	Author	Sections changed	Reason for change
B	2016-01-28	Ernesto de Stefano	Validity and Purpose 1.1 1.2 1.3	Slightly rephrased for better understanding. Slightly rephrased for better understanding. Merged #A1# and #A9# into #A1# and deleted #A9#. Rephrased #A2#, #A3#, #A4#, #A8# and #A12#. Deleted #A5# and #A6# as already covered by rephrased #A3#. Deleted #A7# as implicitly covered by #A4# and #A10. Renamed #12# to #A12#. Merged #10#, #A11# and #A13# into #A10# and deleted #A11# and #A13#. Changed section including two example instead of providing the structure of the rule.
	2015-12-15	Begoña Tiscar	Validity and purpose Application rules section Section 1.1 Table 2 Table3 Table5 Table7 Section 1.3 Table 12	After revision comments

Table 13: Document History