Choose certainty.
Add value.

Review Report

of the

Partition OS Safety Concept

Applicant

Witz Incorporation

Shirakawa 2nd Bldg. 2F, 7F, 13-1
Sakae 2-Chome
Naka-ku
460-0008 Nagoya

Japan

Manufacturer

Witz Incorporation

Same as above

Report no. WN84129T

Revision: 2.1, Date 15.04.2013

Test and Certification body

TÜV SÜD Rail GmbH
Generic Safety Systems

Barthstraße 16
D-80339 Munich

Revision history

Revision	Date	Author	Status	Modifications
0.1	2011-03-02	H. Hauff	released	-
0.2	2011-12-26	H. Hauff / G. Neumann	Draft	Totally revised. Changes of all reviewed documents regarding ParOS considered.
1.0	2012-02-10	G. Neumann	released	Updated documents considered
2.0	2013-01-18	G. Neumann	released	Updated documents considered; new documents [D6] to [D8]
2.1	2013-04-15	G. Neumann	released	minor corrections and clarifications chapter 5.2 • BCC+ added • Footnote 2 5.4 Footnote 3

Table 1: Revision history

Content

List of Tables

List of Figures

1 Target of Evaluation (TOE)

Witz Incorporation requested TÜV SÜD to assess the concept for the operating system “Partition OS”. The Project No. related to this Technical Report was as follows: 717504876 and 717506059.

The TOE is the “Safety Concept” and all safety relevant documentation of the concept phase regarding the Partition OS according to IEC 61508 [N1] route 1_S.

2 Scope of Testing

2.1 Test specimen

Witz Inc. aims to provide a virtualization environment based on the Partition OS (ParOS). The ParOS will be the virtual machine monitor managing different applications running on different partitions. Each partition has its own context with respect to the OS (SafeOS Instance), libraries and application. The SafeOS itself is shared between the partitions. Each application can be a set of tasks. Partition OS offers an API for the management of partitions. This includes the functional API (e.g. systems calls) and the API with integrity functions with diagnoses for the

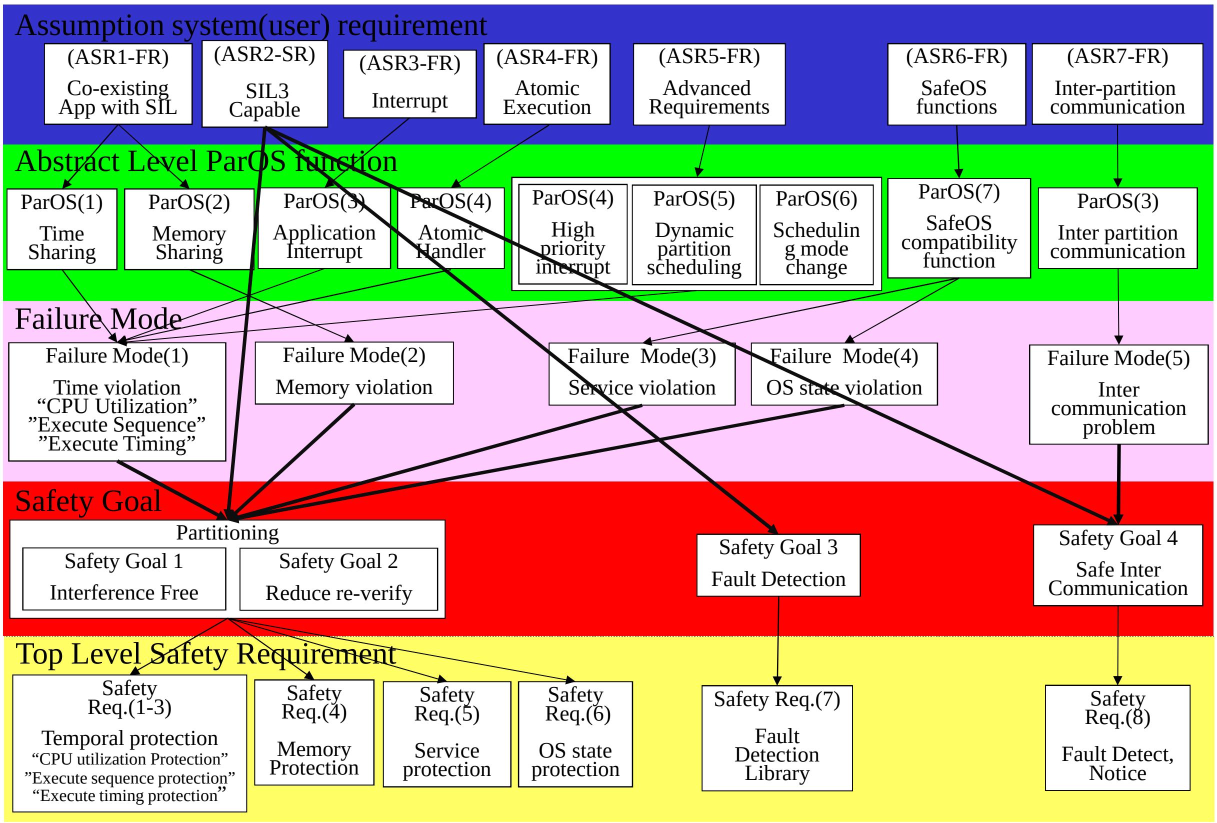
Assumption system(user) requirement
(ASR1-FR) Co-existing App with SIL
(ASR2-SR) SIL3 Capable
(ASR3-FR) Interrupt
(ASR4-FR) Atomic Execution
(ASR5-FR) Advanced Requirements
(ASR6-FR) SafeOS functions
(ASR7-FR) Inter-partition communication
Abstract Level ParOS function
ParOS(1) Time Sharing
ParOS(2) Memory Sharing
ParOS(3) Application Interrupt
ParOS(4) Atomic Handler
ParOS(4) High priority interrupt
ParOS(5) Dynamic partition scheduling
ParOS(6) Schedulin g mode change
ParOS(7) SafeOS compatibility function
ParOS(3) Inter partition communication
Failure Mode
Failure Mode(1) Time violation “CPU Utilization” ”Execute Sequence” ”Execute Timing”
Failure Mode(2) Memory violation
Failure Mode(3) Service violation
Failure Mode(4) OS state violation
Failure Mode(5) Inter communication problem
Safety Goal
Partitioning
Safety Goal 1 Interference Free
Safety Goal 2 Reduce re-verify
Safety Goal 3 Fault Detection
Safety Goal 4 Safe Inter Communication
Top Level Safety Requirement
Safety Req.(1-3) Temporal protection “CPU utilization Protection” ”Execute sequence protection” “Execute timing protection”
Safety Req.(4) Memory Protection
Safety Req.(5) Service protection
Safety Req.(6) OS state protection
Safety Req.(7) Fault Detection Library
Safety Req.(8) Fault Detect, Notice

Figure 1 TOE overview

application and/or partition. Figure 1 shows an overview about the target of evaluation

Figure 2 shows the partitioning principle and the application of partitioning to a safety related system with respect to different SIL applications.

The Executive(OS) is the ParOS providing the partitioning by an partition scheduler, kernel and a failure detection library. Each partition shares the SafeOS with kernel, API, task scheduler but has its own context with respect to the OS and its own failure detection library on partition/application level.

Target of evaluation (TOE) is the safety concept of the Partition OS according to SIL 3 regarding IEC 61508 2nd Edition, which is specified in [D1].

The intended application areas are moving assistance robots, care robots and avionic.

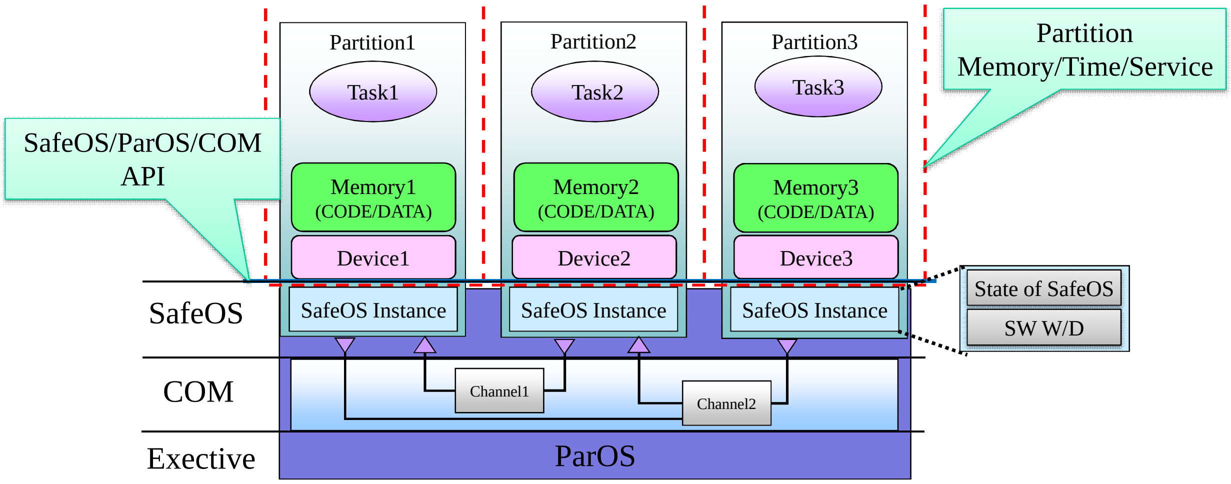

Figure 2 Partitioning with ParOS

2.2 Tests

For each document under test a separate paragraph contains the test results in chapter 5. Five documents were delivered by Witz Inc. containing the information about the safety concept of Partition OS. The overview and summery of the safety concept is shown in [D1], the safety requirements are specified in [D2], safety relevant information, which will be given to users, is given in [D3] and the results of safety analysis are given in [D4] and [D5]. [R1] contains additional information about interpretation of the content given in the preliminary documentation of [D1] to [D4], which was the result of the meeting in January 2011, and [R2] contains information about the interpretation of the documentation [D1] to [D4] based on the meeting in September 2011. Updated documents were delivered to TÜV SÜD Rail GmbH in January 2012. An additional audit was performed in September 2012. The results were incorporated in the latest revisions of the documentation and the new documents [D6] to [D8].

3 Basis of Testing

The regulations and guidelines which form the basis of the type testing are listed below.

3.1 Functional safety

No.	Standard	Title
[N1]	IEC 61508-1: 2010 (SIL 3)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 1: General requirements
[N2]	IEC 61508-3: 2010 (SIL 3)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 3: Software requirements - as far as applicable -
[N3]	IEC 61508-4: 2010 (SIL 3)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 4: Definitions and abbreviations

Table 2: Functional safety

4 Documents provided for testing

Following documents were provided by Witz Inc. to be checked and evaluated by the test house.

No.	Title	Document-No./ File identifier	Revision	Date
[D1]	Partition OS Safety Concept	SafetyConcept_E.doc	1.0	2012-July-03
[D2]	Partition OS Software Safety Requirement Specification	Software Safety Requirement Specification_E.doc	1.0	2013-Dec-25
[D3]	Partition OS Safety Manual (E)	SafetyManual_E.doc	1.0	2013-Dec-25
[D4]	Safety Analysis result report to OS[1]	ParOS_SafetyAnalysis_to_OS_function.xls	0.02	31.10.2011
[D5]	Safety analysis result report to system [1]	ParOS_SafetyAnalysis_to_System.pdf	0.01	28.06.2011
[D6]	Partition OS Safety Requirements Analysis Plan and Results Report	PartOS_SafetyRequirementsAnalysisPlanAndResults Report.doc	1.0	2013-Dec-25
[D7]	Partition OS Safety Requirement Analysis Result Report(detail)	ParOS-SW-00-PJS_ProjectSafetyPlan(EG).xls	1.0	2013-Dec-25
[D8]	FSMP Partition OS Project Safety Plan	ParOS-SW-00-PJS_ProjectSafetyPlan(EG).xls	1.0	2013-Dec-25

Table 3: Documentation

[1] Replaced by [D6]

5 Performance and result of tests

5.1 Test reports

Following test reports were issued by TÜV SÜD Rail GmbH or other accredited test laboratories which must be considered.

No.	Title	Document-No./ File identifier	Revision	Date
[R1]	MEMO	20110110 mom WitzCorp TUEV Rail Memo-hh.docx	---	2011-01-10 to 14
[R2]	Minutes of Meeting	MoM-Witz-ParOS-110912-16.docx MOM-Witz-Process-Audit-2012_01_11-13.docx	---	2011-09-16 2012-01-13
[R3]	Review Report document updates	Review_UpdatedDocuments_Status_20120120.docx	---	2012-02-03
[R4]	ParOS TUEV Rail Memo Meeting Sept. 2012	201209xx WITZ ParOS TUEV Rail Memo.pdf	-	2012-09-21
[R5]	Review Report WitzCorp ParOS	Review Report WitzCorp ParOS 2012 rev1_4_draft_20121210_gn.docx	1.4	2013-01-18

Table 4: Test results

5.2 Partition OS (ParOS) Software Safety Requirement Specification [D2]

The Software Safety Requirement Specification (SW-SRS) gives a definition of the intended application levels (APPReqLv0 to APPReqLv3) and makes an allocation between the application levels to the partition levels (ParLv1 to ParLv4) of ParOS and specifies different conformance classes.

The TOE is restricted to hardware supporting following three constraints:

1. The possession of a mode (non-privilege mode) having access restrictions on the memory.
2. Access to a permitted device is possible even in non-privilege mode.
3. Permission and prohibition of interrupt is possible individually by low overhead.

The constraints and additional requirements related to hardware are given in detail in chapter 4

The conformance classes are specified in chapter 5:

1. BCC/BCC+ (Basic Conformance Class)
2. ECC (Enhanced Conformance Class)
3. DCC (Development Conformance Class)

The conformance class BCC is stricter about partitioning than ECC and ECC is stricter about partitioning than DCC.

BCC has the strictest partitioning.

BCC+ is based on BCC. BCC+ supports all functions supported by BCC. In addition it supports the "functionally-limited system interrupt".

The conformance class ECC allows features which have the potential to violate safety goals but can be used with known restrictions for the application.

The conformance class DCC shall only be used for development but not for safety critical applications.

The SW-SRS defines 5 system states in chapter 8.3 of [D2]

- Undefined state
- System initialization state
- System shutdown processing state
- System stop state
- System normal state

In Figure 2 in [D2] the state transition diagram is given and how the transition between the states can be triggered. In the subsequent paragraphs of chapter 8 the description of the routines and the API as well as the behavior is given in natural language.

Chapter 9.2 in [D2] gives the definition of states of the partition and the related functions to change the state (transition between states). Figure 3 in [D2] shows the state transition diagram for the partition. Subsequent paragraphs describe the API and behavior in a brief manner in natural language. Figure 4 in [D2] shows the system timing (time slices for applications/partitions). Chapter 10 and subsequent paragraphs describe the scheduling of partitions, chapter 21 and 19 the usage and handling of interrupts (system or application). In chapter 17 the Check Hook and the related API is described. The Time Event Handler and the related API is described in chapter 20, the Atomic Handler and the API in chapter 16 and exception handling in chapter 18. Chapter 22 describes the system time event handler. The Time Window Handler and the related API is described in chapter 20. Chapter 15 describes the partition intercommunication and the related API. Task Protection and Stack usage is described in chapter 23 and 24, partition memory protection in chapter 13. All chapters contain a full description of the related API in a systematic manner. Every API function is given with his parameters and return values including error handling. Each requirement is tagged with a unique identifier.

Result:

The SW-SRS describes all requirements and makes each requirement identifiable by a unique identifier. Restrictions by using API functions which have the potential to violate a safety goal are visible.

Some functionality has the potential to violate safety goals, e.g. system interrupts[2] as well as the idle attribution for an application which can produce time jitter and time shift violating the process safety time of an application. In this case time deadlines of individual applications or tasks can be violated. Statement under which conditions/constraints such techniques shall be allowed in a safety application or not are given in the safety manual. The effect of the use of these functions is described and shown in timing diagrams.

[2] There is a separation between interrupts on system level and interrupts on application level. The term “application interrupts” refers to interrupts in one partition. The interrupts on application level cannot cause jitter for other partitions. System interrupt will be treated with higher priority than the application interrupt, so it can cause a jitter in the safety partition.

5.3 Testing of Safety Concept of ParOS ([D1])

The Safety Concept of ParOS references the standards IEC 61508 2nd Ed. part 1-7 and the ISO/DIS 26262 part 10, Software Safety Requirement Specification, the Safety Manual, the Safety Analysis of Safe OS and the Software Safety Requirement Specification and Safety Analysis and Manual of ParOS.

Chapter 2 gives some information about the objectives regarding functional safety. The objective is mainly to separate different applications with different SIL levels by virtualization (partitions) to keep other applications running if one application fails. Also assumptions are made regarding SIL decomposition for combining multiple channels with or without fault tolerance. Failure modes of ParOS are described in an abstract manner in paragraph 2.3 while paragraph 2.2 gives an overview about the functionality of ParOS. The Safety Concept is described in chapter 5 to 7. Figure 5.10 shows the ParOS composition and the relation between ParOS (executive(OS)) and Safe OS and the hardware for all conformance classes (BCC/BCC+, ECC, DCC).

The total approach (system) has 5 components, the OS, the com layer for inter-partition communication, the partitions, the monitoring system and the watchdog/timer.

Paragraph 3 describes the 4 safety goals:

1. Safety goal 1: Software partitions shall be free from interference between each other
2. Safety goal 2: Changes/modifications made on the software of a partition shall not require re-verification of software of other partitions
3. Safety goal 3: A fault detection library to detect random hardware faults shall be provided with a diagnostic coverage (DC) of at least 90% or higher to fulfil SIL2 with a fault tolerance of 0 and SIL3 with a fault tolerance of 1 and higher.
4. Safety goal 4: ParOS shall provide a safe inter-process communication with fault detection and error handling

Chapter 4 describes the architecture of ParOS (Partition layer, COM layer, SafeOS layer and Executive layer). Chapter 5 gives an overview about the temporal and spatial partitioning. Paragraph 5.1 describes the 4 partition levels. The highest level will be ParLv4 with the strictest protection for safety reasons. The partitioning has 4 main protection levels which are shown in [D1] table 5.3:

1. Service protection
2. Memory protection
3. CPU utilization, execution sequence and execution time protection
4. System (OS) state protection

Time and execution protection between partitions is described in paragraph 5.2.1. Each partition (application) will get a static time slice duration and the sequence of running the applications is fixed at link time. The approach is to get a deterministic scheduling. Paragraph 5.2.2 describes spatial partitioning, paragraph 5.2.3 service protection and system state protection.

Paragraph 5.5 describes the conformance classes and gives the relation to the Partition Level (ParLv1-4) requirements.

Paragraph 5.6 specifies the operation modes of ParOS and the partitions.

The ParOS function composition is given in paragraph 5.7.

Paragraph 5.8 gives an overview about functions that have the potential to violate safety goals.

Counter measures to protect against violation of safety goal 1 and 2 will be given in SafeOS Software Safety Requirement Specification and Safe OS Safety Manual.

The description of the functionality of the safety integrity functions provided by the fault detection library is referenced by the documents of Safe OS.

Result:

The safety concept shows how the safety goals will be fulfilled by the top level safety requirements or safety integrity requirements. Each requirement has a unique tag.

- The safety goals, safety requirements and safety integrity requirements are consistent and traceable to each other.
- If safety goals can be violated by ParOS functions the required information is given and the effect is shown.

5.4 Testing of Safety Manual [D3]

The safety manual Chapter 3 gives an overview about ParOS and using ParOS based systems with fault tolerance for SIL3 applications. The given information is repeated out of the Software Safety Requirement Specification and the Safety Concept of ParOS.

Chapter 4 gives introductions and preconditions related to the safety life cycle. The requirements about the software safety life cycle depend on the way, how ParOS/SafeOS will be delivered to the user, either as source files or compiled and linked as object. There are several marks “T.B.D.”; TÜV SÜD assumes it means the content has to be agreed on in a specific project between customers and manufacturer or shall be completed depending on the progress in the project ParOS (e.g. after implementation or verification).

Chapter 5 gives an introduction to the System Development Requirements for the system that uses ParOS.

Chapter 6 gives a description about hardware requirements and restrictions.

Chapter 7 gives an overview how safety goals can be violated by functions of SafeOS and/or ParOS and what the user has to do. It contains small examples in source code for faulty or correct usage, so the user gets deeper information how to deal with safety critical functions of ParOS/SafeOS and how to deal with errors and make correct error handling in the application. Examples for valid or invalid parameters shall be given, depending on a specific platform example with I/O and memory map.

Chapter 8 gives resource and performance data related to ParOS/SafeOS to the user. It gives a description about the delivered files and documents. There are several marks “T.B.D.”; TÜV SÜD assumes it means the content has to be agreed on in a specific project between customers and manufacturer.

Chapter 9 gives information on compatibility between versions of ParOS.

A test suite from the manufacturer is mentioned (undefined content or requirements for the content) and use cases for what a OEM has to do to verify/validate after building ParOS and his application. Rough information is given on how to get the ParOS running.

Results:

The safety manual has to be completed in the detailed phases of a specific project. Completeness of the safety manual is depending on the project specific regulation of deliverables by Witz Inc. This includes:

- responsibilities of the user,
- specific agreements on testing and/or
- validation responsibilities.
- The relation between Partition OS and the interface to the hardware support package. The description of the hardware interface (board support package) is mentioned only on a high level. This emerges from the fact that Witz Inc. makes it mandatory to order the Board Support package development to Witz Inc.[3]
- A requirement to cross-check the result of the tool classification (chapter 4) at time of product release. This can only be defined precisely during the detailed phase with knowledge of the deliverables/responsibilities etc.

There are several imprecise wording issues in the English version of the manual. Wording can cause misunderstandings or some text is not understandable.

For several text sections it is not uniquely identifiable for the user of ParOS if he shall

- select something
- specify something
- describe/document something
- notice something

Due to the nature of chapter 8 a project specific adaption of the safety manual is necessary in any case. The resulting "final" safety manual shall be reviewed and checked to achieve precise and accurate instructions for the user of ParOS. Depending on the chosen language for the specific project this shall include a correct translation. A text version from TÜV was provided that contains some highlighted examples.

SRS or manual to be enhanced with a requirement to cross-check the result of the tool classification to this chapter of the manual at time of product release.

[3] Chapter 3.3 of the manual mentions T2 and T3 tools for the OS integration into a user system, chapter 4 mentions a board support package. For both activities the list of used tools can only be completed and analyzed with knowledge of the specific user system and BSP.

5.5 Testing of Safety Analysis [D4] - [D8]

The Safety Analysis in [D4] and [D5] were replaced by the updated documents [D6] and [D7]. They contain the planning and results of the Safety Analysis including an FMEA and a compliance matrix. Register one contains the cover, register 2 the history, register 3 the index and register 4 gives an overview about groups of functions which can be causes for failures or errors. Registers 5 to 12 give a classification of function groups which have impact regarding the safety goals. Register 13 shows types of violation of safety goals regarding processing with timing diagrams. Register 14 to 21 contain the safety analysis regarding the function groups specified in register 5 to 12. The register 22 gives an overview about the safety measures regarding safety integrity and gives a statement about the claimed diagnostic coverage. Register 23 makes the allocation of requirements to the relevant counter measures.

Both documents seem to be exports and translated files from original documents not available at TÜV SÜD.

The Functional safety management plan (FSMP) for Partition OS [D8] contains information on the team which performs the safety analysis, the qualification and the basic procedures for performing it.

Results:

The analysis follows the principles of a FMEA (cause, failure mode, consequence, prevention measures, detection measures). Measures and techniques are allocated to detect or prevent systematic faults in the phases of the safety life cycle. The process how the analysis was done is defined and referenced. Compliance and completeness is shown in the related matrix sheets.

6 Summary

The available documentation of Witz Inc. is complete with respect to the concept of the TOE as defined in chapter 1.

The safety manual has to be completed in the detailed phases of a specific project depending on the project specific regulation of deliverables by Witz Inc. to the user of ParOS. This includes requirements resulting from the fact that Witz Inc. makes it mandatory to order the Board Support package development by Witz Inc. The resulting “final” safety manual shall be reviewed and checked to achieve precise and accurate instructions for the user of ParOS in accordance with the assessment regulations for the specific application.

The requirements of IEC 61508 2nd Edition are met. The results and recommendations can be used to execute the detailed development phase and documentation for PartitionOS.

i.V. Guido Neumann
Technical Certifier

i.A. Sylvia Waldhausen
Expert Functional Safety