Report

on the

Certificate

Z10 14 02 60643 007

RTP3000 TAS

Manufacturer:

RTP Corporation
2832 Center Port Circle
Pompano Beach
Florida 33064
USA

Report no. RP85295C
Revision 1.3 of 2014-03-31

Test Body
TÜV SÜD Rail GmbH
Generic Safety Systems
D-80339 Munich

Certification Body
TÜV SÜD Product Service GmbH

D-80339 Munich

TABLE OF CONTENTS

Revision

Version	Status	Date	Author	Changed chapters	Reason of change
1.0	initial	2013-12-17	J. Dong		Initial
1.1		2013-12-20	K. Leupold		corrections
1.2		2014-02-07	K. Leupold		NFPA 72, 85 added
1.3		2014-03-31	J. Dong		certificate number updated

Table 1: Revision

1 Target of Evaluation (ToE)

In March 2013 the company RTP Corporation assigned TÜV SÜD Rail GmbH for testing and certifying of the RTP3000 TAS according to SIL 3 according to IEC 61508 series.

2 System overview

2.1 Description

The RTP3000 TAS systems is a safety-related programmable system suitable for safety-related applications with a high level of potential danger e. g. Emergency Shutdown Systems (ESD), Burner Management Systems (BMS), Fire and Gas Detection Systems (F&G), Turbine Control Systems, etc.

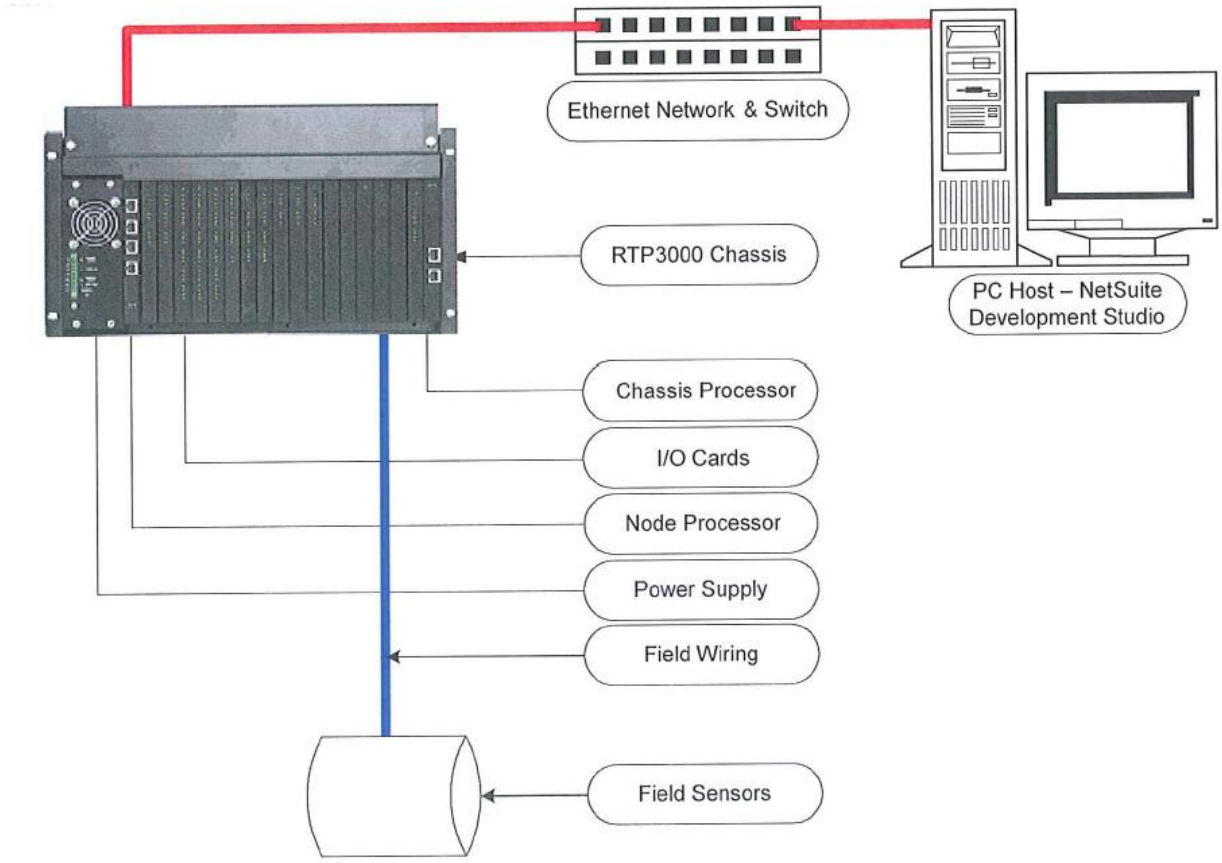

Figure of RTP3000 System

The basic RTP3000 TAS system consists of a hardware chassis, a power supply, a node processor card, a chassis processor card and any optional input/output cards.

2.2 Test specimen

2.2.1 Processor

The processor node could include safety related and non safety related library modules in an application, whereas the safety instrumented functions should be built up in a user application program while using the certified subset of the graphical languages.

Each node processor executes two copies of the user application program (PGM). I/O scanning of the processor is performed at the same point during program execution, using the same input data for both application programs. The outputs of each of the PGM are compared before sending them to the Chassis Processor.

The node processor of the RTP3000 TAS system is configurable in simplex (RTP3000S), dual redundant (RTP3000D), TMR architecture (RTP3000T) and quad redundant architecture (RTP3000Q).

2.2.2 I/O Modules / Components

An I/O card is the component that provides basic I/O capabilities between the RTP system and field sensors/signals. The I/O itself will be performed asynchronously. All safety rated input cards and safety rated analog output cards shall satisfy SIL 2 requirements, some of them satisfy SIL 3 requirements. SIL 3 requirement for SIL 2 modules shall be accomplished by means of redundant architectures.
The I/O racks, and their installed I/O cards, can be organized as common (non-redundant) I/O racks, redundant I/O rack pairs, or redundant I/O triplets to match the required availability.

2.2.3 Safety configuration

The safety application programming software “NetArrays Developer Studio” is able to configure safety related PES nodes and safety I/O modules as well as non-safety PES nodes and non-interfering I/O modules.

2.2.4 Safety application programming

The application programming software “NetArrays Developer Studio” contains a SIL-certified subset of the graphical languages as previously implemented by RTP Corp. to give the opportunity for users to build up their PGM. The safety application programming environment compiles the application project and checks for errors and mistakes.
The conditions and rules for safe use of the RTP3000 TAS series are laid down within the user documentation.

2.2.5 Communication Component Relationships

1. I/O data is transferred between I/O cards and the RTP 3000 Node Processor card: In an RTP3000 SIS, I/O data is passed between an I/O card and the chassis processor via the chassis back-plane bus. The chassis processor card communicates I/O data with the RTP3000 Node Processor card via Ethernet messages which can either be wired port to port or through a separate Ethernet network. This network can be configured redundantly.

2. Intercommunication data is managed between redundant RTP3000 Node Processor cards: In an RTP3000SIS, intercommunication data is passed between RTP3000 Node Processor cards via Ethernet messages which can either be wired port to port (a dual redundant scenario) or through a separate Ethernet network (a triple redundant scenario). This network cannot be redundantly configured.
3. Peer-to-peer communication data is managed between RTP2300, RTP2300M, RTP2500, RTP2500M and RTP3000 Node Processor cards via an Ethernet network using TCP/IP messages.
4. Host communication data is managed between an RTP3000 Node Processor card and a host PC via an Ethernet network using TCP/IP messages. Host PC applications can be either RTP NetSuite or a 3rd party HMI software package communication via RTP communications protocol or an OPC interface utilizing the RTP communications protocol.

2.2.6 Basis System Availability and Redundancy

Triple and quad redundancy for the safety-related programmable system RTP3000 TAS increases availability without having influence onto the safety of the system. Techniques and measures are included to allow switching from a faulty module to the standby module within a time that allows carrying on the process in a safe manner without interruption. An overview of the reachable safety integrity levels in redundant and non-redundant mode can be seen in the related manuals.

	RTP3000S RTP3000M (Non-redundant I/O)	RTP3000D, RTP 3000T RTP 3000Q (Non-redundant I/O)	RTP3000D, RTP3000T RTP3000Q (Redundant I/O)
Availability	Normal	High	Very High
Controller Module	Mono	Redundant	Redundant
I/O Module	Mono	Mono	Redundant
I/O Bus	Mono	Mono	Redundant

2.2.7 Hardware Components under Certification

Beside the above mentioned certified hardware modules the systems consist of non safety-related hardware. These non-interfering I/O cards shall be able to be inserted into the same chassis as with the safety-certified I/O cards. These non-interfering hardware modules may only be used for the processing of signals not relevant to safety and not for the processing of safety-related tasks.

2.2.8 Fault Reactions of the System

System behavior in all possible architectures of all component types, like Processor Nodes, Chassis Processors (including communication) and I/O Modules is described in the Architectural Design Specification. See also Annex of the report to the certificate RP85295C in the current version.

3 Certification Requirements

3.1 Basis of Certification

The certification of the RTP3000 TAS will be according to the regulations and standards listed in clause 3.3 to 3.6 of this document. This will certify the successful completion of the following test segments:

I. Functional safety
   - Analysis of the system structure (FMEA system)
   - Analysis of the hardware (FMEA component, quantitative analysis)
   - Analysis of the software
   - Fault simulations and software tests
   - Test of the fault prevention measures
   - Functional test

II. Electrical safety

III. Susceptibility to environmental errors
   - Climate and temperature
   - Mechanical effects

IV. Electromagnetic compatibility

V. Safety information in the product documentation (safety manual, operating instructions)

VI. Product-related Quality Management in manufacturing and product care.

Certification is dependent on successful completion of all above listed test segments. The testing follows the basic certification scheme for Safety Components of TÜV SÜD Rail GMBH.

3.2 Certification Documentation

- Technical Report by TÜV SÜD Rail GmbH
  Report No. RP85294T
- Safety Manual - 3000 Series – Safety Instrumented Systems
- Reference Manual – NetArrays I/O Card Configuration Properties
- User Guide - RTP NetSuite Safety Instrumented System Development SoftwareUser
- Technical Manuals (provided for each component)

Based on the specified purpose of use of the RTP3000 TAS in safety critical process applications, the certification is based on the following set of standards. The issuance of the certificate states compliance with these references unless specifically noted otherwise.

3.3 Functional Safety

The testing for functional safety is to be performed using the following standards and guidelines:

IEC 61508/ EN 61508 part 1 –4: 2010 (SIL3)	Functional safety of electrical/electronic/programmable electronic safety-related systems
IEC 61131 –6: 2012 (SIL3)	Functional safety

3.4 Basic Safety and Environmental Safety

To complete and to specify the technical requirements resulting from the essential requirements of the directives listed above the testing of Basic Safety is to cover the following standards:

EN 61131-2: 2007	Programmable controllers – equipment requirements and tests

3.5 Electromagnetic Compatibility

To complete and to specify the technical requirements resulting from the essential requirements of the directives listed above, the testing of Electromagnetic Compatibility is to cover the following standards:

EN 61131-2: 2007	Programmable controllers – equipment requirements and tests

3.6 Application

EN 54-2: 1997	Fire detection and fire alarm systems - Part 2: Control and indicating equipment
IEC 61511-1: 2003	Functional Safety: Safety Instrumented Systems for the process industry sector
NFPA 72: 2013	National fire alarm and signalling code
NFPA 85: 2011	Boiler and combustion systems hazards code

4 Results

4.1 Functional Safety

The tests performed and quality assurance measures implemented by the manufacturer have shown that the RTP3000 TAS complies with the testing criteria specified in clause 3 subject to the conditions defined in clause 5 and its subsections, and is suitable for safety-related use in applications up to SIL 3 in accordance with EN/IEC 61508.

4.1.1 Fault Reaction and Timing

Fault detection in the RTP3000 TAS is assured by means of following basic techniques:

- self test at power up and during operation
- two channel control logic with cross check
- redundancy
- normal and inverted signal processing within the I/O cards

4.1.2 Evaluation of fault prevention measures

For the avoidance of failures the following techniques and measures were used:

- Project management
- Documentation
- Structured specification
- Inspection of the specification or walk-through of the specification
- Observance of relevant guidelines and standards
- Structured design
- Modularization
- Use of well tried components
- Inspection of the hardware
- Functional testing (also under environmental conditions)
- Operational and maintenance instructions
- User- and maintenance friendliness

The individual measures for the avoidance of failures provide the required degree of effectiveness and are specified in the relevant documents

4.1.3 Analysis of the hardware safety integrity and hardware fault simulations (FIT)

The Failure Mode Effect and Diagnostic Analysis (FMEDA) showed that the occurrence of a single fault do not lead to loss of the safe functioning. The individual architectural constrains are sufficient and their corresponding degree of fault detection provide the required degree of effectiveness.
The response time to safety critical faults shall be determined application specific in accordance to the safety manual.

4.2 Basic Safety and Electromagnetic Compatibility

4.2.1 Electrical Safety

The results about the electrical safety are documented by the certificates and test reports of an accredited test centre. The documentation of the tests has been reviewed for completeness.
These certificates show that the standards specified in clause 3 are covered.

4.2.2 Environnemental Testing

The environmental stress tests are documented by the certificates of an accredited test centre.
The above mentioned certificates and tests and the quality assurance measures implemented by the manufacturer have shown that the RTP3000 TAS comply with the testing criteria specified in clause 3 subject to the conditions defined in clause 5 and its subsections.

4.2.3 Electromagnetic Compatibility

The tests of the electromagnetic compatibility are documented by the certificates and test reports of an accredited test centre. The documentation of the tests has been reviewed for completeness.
These certificates show that the standards specified in clause 3 are covered.

4.3 Product Specific Quality Assurance and Control

The software and hardware components developed and manufactured in course of the safety evaluation are governed by RTP Corp. quality assurance and control system.
As part of the certification process TÜV Product Service also performs a procedure that is tailored to the assessed product in order to assess the consistency of product quality while accounting for product modifications and their identifiability (follow-up service).

5 Implementation Conditions and Restrictions

The use of the RTP3000 TAS shall comply with the current version of the safety parts of the user manual, and the following implementation and installation requirements have to be followed if the RTP3000 TAS is used in safety-related installations.

5.1 General Application Conditions

- The guidelines specified in the instruction manuals shall be followed.
- Only modules certified for safety-related operation, as shown in the annex shall be used for safety-critical functions.

  Not certified standard modules (defined as non-interfering) may be used for non-safety-critical signals only.
- The fault tolerance period of the process controlled by the system shall be greater than the worst-case response time of the system.

- A well-defined shutdown procedure shall be specified.
- Non-safety-related blocks in the application program shall not control or affect data used by any safety-critical block unless in case of plausibility checks in the safety-related program.

5.2 General Commissioning Conditions

- The guidelines and the instructions for commissioning, described in the instruction manual, have to be followed.
- Prior to commissioning, a complete functional test of all safety-relevant programmed application functions shall be performed.
- All timing requirements shall be validated.
- Any application software modification after commissioning shall result in a re-validation of the entire application software. The commissioning can be reduced if the change can be shown by use of a revision checker to be limited to a specific area of program.
- The proper fail-safe configuration of all safety-critical fail-safe I/O shall be verified. Only configurations covered by the Safety Manual are covered by the certification.

5.3 General Run-time Conditions

- The operating conditions as specified in the instruction manuals shall be met.
- The procedures of modification of safety related data and components described in the user manual have to be followed.
- The maintenance and repair instructions described in the instruction manual of the RTP3000 TAS have to be followed.
- Failed modules that are safety-related should be replaced as quickly as practical to minimize the probability of multiple fault accumulation and potential (safe) nuisance shutdown. As a maximum, failed modules should be replaced within the multiple fault occurrence time. The calculations of the Probability-of-Failure-on-Demand of the safety-related RTP3000 series system are documented in the report “Markov Model Analysis”.

6 Certificate Number

This report specifies technical details and implementation conditions required for the application of RTP3000 TAS to the certificate:

Z10 14 02 60643 007

Munich, 2014-03-31

TÜV SÜD Rail GmbH
Rail Automation

Peter Weiß
(Technical Certifier)