Choose certainty.
Add value.

Report

on the

Certificate

Z10 14 03 78846 002

Safety-Related Programmable System

800xA Safety

Manufacturer:
Ansaldo Energia S.p.A.
Via Nicola Lorenzi 8
Genova, GE, 16152
ITALY

Report No.: AG85521C

Revision 1.0 dated 2014-03-10

Testing Body:
TÜV SÜD Rail GmbH
Rail Automation

Certification Body:
TÜV SÜD Product Service GmbH
Ridlerstraße 65
D-80339 München

Revision

Version	Name	Date	Changes/History
1.0	P. Weiß	2014-03-10	Initial version based on report AV84798C, version 1.1 dated 2013-08-16

1 Target of Evaluation (ToE)

TÜV Süd Rail GmbH has been contracted by Ansaldo Energia S.p.A. to certify the safety-related programmable system 800xA Safety according to Category 4 PL e according to ISO 13849-1 and SIL 3 according to IEC 61508 series and IEC 62061.

This report summarizes the user related results of the tests and inspections performed on the relevant parts of the system 800xA Safety, based on the certification requirements outlined under clause 3.1 and reported by the documentation listed under clause 2.5.

1.1 Definition of Terms

The following terms are used in this report with a meaning defined as follows:

CBM	Control Builder M is the certified engineering tool for the AC 800M controller
Common cause failure	Failure, which is the result of one or more events, causing coincident failures of two or more separate channels in a multiple channel system, leading to system failure
Controller	Refers to the standard AC 800M process controller
Controller configuration	HW configuration or setup of a controller, including configuration of I/O, communication, access variables, resources/tasks (cycle-time, priority, etc) in addition to the I/O connection.
Demand response time	Time from a demand to a sub-system and until the correct state on this sub-system output, is achieved.
Diversity	Different means of performing a required function.
Failure	The termination of the ability of a functional unit to perform a required function.
Fault	Abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function.
Fault avoidance	Use of techniques and procedures, which aim to avoid the introduction of faults during any phase of the safety lifecycle of the safety-related system.
Fault detection and reaction time	Time from occurrence of a fault and until it is found and reported as an output of this sub-system.

Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors (NOTE: Assuming safety functions, not process availability issues).
Hot replacement	Replacement of HW that may be done with power connected to the unit.
On-line replacement	Replacement of HW/SW part that does not affect the process in control.
Process safety time	The maximum time a process is allowed to run with a faulty safety critical output.
PM	Processor Module as specified in the related annexes
Random hardware failure	Failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware.
Redundancy	Existence of means, in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information.
Safety Controller	Specifies the AC 800M HI, comprising the Processor Module with safety firmware and the Safety Module, as one unit (I/O sub-system excl.).
Safety I/O	Certified I/O module for safety related field instruments.
SM	Safety module as specified in the related annexes
Safety system	Safety system specifies the Safety controller and the I/O sub-system.
Sub-system	Part of a system (e.g. component as I/O module, I/O system or SW "package").
800xA Safety	Comprehensive safety and process automation system, which consist of safety critical and non-interference products/modules. This includes for example the AC 800M High Integrity controller, S800 High Integrity I/O, Control Builder M engineering environment and the 800xA Operator Workplace.
1oo1D	One channel hardware architecture, with external diagnostic
1oo2D	Two channel hardware architecture, with mutual diagnostic

2 System overview

2.1 Architecture

The safety-related programmable system AC 800M High Integrity is suitable for safety-related applications with a high level of potential danger, e.g. machinery applications, chemical processes and offshore processes.

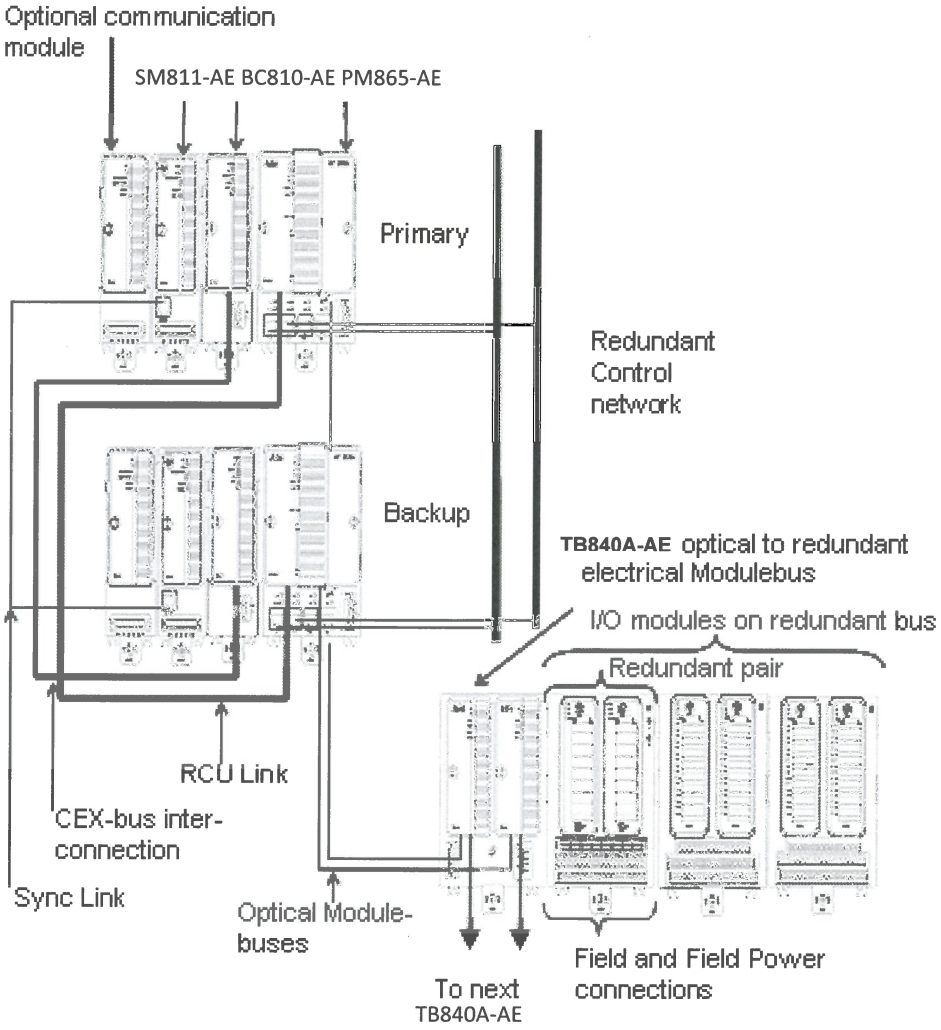

Figure of safety-related programmable system AC 800M High Integrity

The AC 800M High Integrity system consists mainly of a Processor Module, a Safety Module and I/O modules suitable for safety-related applications.

Safety critical input signals are read from the process with the safety-related I/O modules or read from other AC 800M High Integrity systems via safety-related application communication.

Safety critical output signals are sent from the AC 800M High Integrity controller to the safety-related I/O or to other AC 800M High Integrity systems via safety-related application communication. The safety-related I/O is responsible for the safety-related output to the process.

2.1.1 Processor Module and Safety Module

2.1.1.1 Architecture 1oo1D for SIL 1-2, CAT 3, PL e
The "single-channel" process controller AC 800M is combined with a Safety Module in a 1oo1D architecture. Internal self-diagnostics have been realized in the Processor Module, PM, and in the Safety Module, SM. The program flow of the application execution and the I/O scanning in the PM is supervised by diagnostics running in the SM.

Additional fault monitoring of the safety controller is realized by the safety-related I/O, checking the CRC from the SM and the safety-related data from the PM.

2.1.1.2 Architecture 1oo2D for SIL 1-3, CAT 4, PL e
The 1oo2D architecture is realized with the PM and SM, whereas the application program is executed in parallel within both modules. Verification of the two results is implemented in the PM and independently in the I/O via comparison of the inverted CRC (from SM) and the related data (from PM).
All safety integrity measures roughly described in the chapter above for the 1oo1D architecture are additionally in place.

2.1.2 Control Builder M

The Control Builder M is enhanced with safety functions in order to support its use as an engineering environment for safety applications. Additional software packages are included in order to perform the necessary diagnostics and to support execution-environment for safety-related applications.

For the user, this includes e.g.:

- Standard library items classified in order to show their usability in safety application building
- Standard Safety libraries
- Possibility for SIL classification of user-defined libraries and applications

The Control Builder M is used as a configuration and programming environment of the safety-related applications.

2.1.3 AC 800M High Integrity I/O modules

The S800 High Integrity I/O modules are designed with a "hidden" 1oo2 structure with diverse execution and internal mutual supervision. Fault detection and control is implemented by the combination or comparison of the results calculated by the diverse hardware channels.

The modules can be located in central or decentralized DIN rail assemblies.

2.1.4 Safety configuration

Safety configuration is necessary for installation and modification of the safety-related programmable system AC 800M High Integrity using the Control Builder M tool.

2.2 Hardware Components under Certification

The safety-related system components belonging to this certification are listed in the current revision of the Annex A to this report. This allows the components to be used to process safety critical signals and functions.

For details on architectural, configuration and implementation requirements please refer to the user manuals and the Safety Manual for the safety-related programmable system AC 800M High Integrity.

2.3 Software Components under Certification

A list of the software components with the valid version numbers is shown in the current revision of the Annex A to this report.

2.4 Communication

A safety-related communication between the AC 800M High Integrity controller and the S800 High Integrity I/O modules has been realized, using the standard ModuleBus telegram with an included safety layer.

To exchange safety critical process signals and results calculated in 1131-applications, a peer-to-peer communication, including a safety layer, between AC 800M High Integrity systems could be configured and used. Safe peer-to-peer communication is realized by either using dedicated library modules (MMS) or Communication Variables (IAC).

2.5 Safety Manual

The conditions and rules for safe use of the safety-related programmable system AC 800M High Integrity are laid down within the user documentation "AC 800M High Integrity – Safety Manual", "AC 800M Controller Hardware", "800xA Safety, Reliability and Availability Data", "S800 I/O, Modules and Termination Units" and "S800 I/O, Getting started".

In addition to the components documented in the Annex A their corresponding MTUs, ModuleBus and CEX-Bus inlets, outlets and termination units, cables etc. are listed in the relevant ABB user manuals, possible to connect to and to use in the safety system.

2.6 Redundancy

Redundancy for the safety-related programmable system AC 800M High Integrity 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.

The AC 800M High Integrity controller and the S800 High Integrity I/O modules need no redundancy to fulfil the requirements of the intended safety.

2.7 Availability

AC 800M High Integrity controller is certified up to SIL 3 in a single configuration which from CPU point of view contains one PM and one SM unit working in a functional pair. Redundancy of these units is not required for achieving or maintaining the safety integrity. Redundancy of AC 800M High Integrity can however be arranged by using two PM and two SM units in a quad(ruple) structure (i.e. four CPUs) to achieve better system availability. Redundancy increases system availability using the SIL 2 or SIL 3 system configuration. Adding redundancy does not affect safety integrity, it only increases availability. Details can be found in the document "800xA Safety, Reliability and Availability Data".

Availability calculations are not in the scope of this certification and therefore are not regarded by TÜV SÜD Rail GmbH during the functional safety assessment.

3 Certification Requirements

3.1 Basis of Certification

The certification of the safety-related programmable system AC 800M High Integrity will be according to the regulations and standards listed in clause 3.3 to 3.5 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

Documentation of this certification is based on the following reports:

- Technical Report, No.: AG85520T (on system level)
- Modification Reports related to minor system modifications

- Technical Reports of new system components using a technical safety concept of already certified components
- AnsaldoEnergia System 800xA Safety AC 800M High Integrity – Safety Manual
- AC 800M High Integrity – Reliability and Availability

Additional information regarding installation and use of the AC 800M High Integrity controller and the S800 High Integrity I/O modules can be found in:

- S800 I/O, Modules and Termination Units
- S800 I/O, Getting Started
- AC 800M – Controller Hardware

Based on the specified purpose of use of the safety-related programmable system AC 800M High Integrity 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.

Some of these standards have been updated during system development and modifications. Therefore component or module specific information about the compliance to the standards is given in the current revision of the Annex A.

3.3 Functional Safety

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

IEC 61508-1: 2010	Functional Safety of electrical/electronic/programmable electronic safety-related systems Part 1: General requirements
IEC 61508-2: 2010	Functional Safety of electrical/electronic/programmable electronic safety-related systems Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems
IEC 61508-3: 2010	Functional Safety of electrical/electronic/programmable electronic safety-related systems Part 3: Software requirements
IEC 61508-4: 2010	Functional Safety of electrical/electronic/programmable electronic safety-related systems Part 4: Definitions and abbreviations

IEC 61508-5: 2010	Functional Safety of electrical/electronic/programmable electronic safety-related systems Part 5: Examples of methods for the determination of safety integrity levels
IEC 61508-6: 2010	Functional Safety of electrical/electronic/programmable electronic safety-related systems Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
IEC 61508-7: 2010	Functional Safety of electrical/electronic/programmable electronic safety-related systems Part 7: Overview of techniques and measures
IEC 62061: 2005	Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
EN ISO 13849-1: 2008	Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design
EN ISO 13849-2: 2008	Safety of machinery - Safety-related parts of control systems - Part 2: Validation
IEC 61511-1: 2003	Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and software requirements
EN 61131-6: 2012	Programmable controllers – Part 6: Functional safety
UL 1998: 2010	Software in Programmable Components

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 covering the following standards:

IEC 61131-2: 2007	Programmable controllers - equipment requirements and tests
EN 50178: 1997	Electronic equipment for use in power installations
UL 508: 2010	Industrial Control Equipment

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 covering the following standards:

EN 61131-2: 2007	Programmable controllers – Part 2: Equipment requirements and tests
IEC 61000-6-2: 2005	Electromagnetic compatibility (EMC) – Part 6-2: Generic standards – Immunity for industrial environments
IEC 61000-6-4: 2010	Generic standard - Emission for industrial environments
IEC 61326-3-1: 2008	Electrical equipment for measurement, control and laboratory use - EMC requirements - Part 3-1: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) - General industrial applications
IEC 61326-3-2: 2008	Electrical equipment for measurement, control and laboratory use - EMC requirements - Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – Industrial applications with specific electromagnetic environment

3.6 Application Standards

Because of the expected applications of the system following additional standards and regulations were considered:

Machinery Applications	
EN 60204-1: 2010	Safety of machinery – Electrical equipment of machines
NFPA 79: 2012	Electrical Standard for Industrial Machinery
EN 1037: 2008	Safety of machinery - Prevention of unexpected start-up
EN ISO 13850: 2008	Safety of machinery - Emergency stop - Principles for design
Process Industry	
ISA S84.01: 1996	Application of safety instrumented system for the Process Industry
EN 54-2: 1997 EN 54-2 A1: 2007	Fire detection and fire alarm systems - Part 2: Control and indicating equipment
NFPA 72: 2012	National Fire Alarm and Signaling Code
Burner Systems	
EN 298: 2012	Automatic burner control systems for burners and appliances burning gaseous or liquid fuels
EN 50156-1: 2004	Electrical equipment for furnaces and ancillary equipment - Part 1: Requirements for application design and installation
NFPA 85: 2012	Boiler and Combustion Systems Hazard Code
FM 7605: 1999	Programmable Logic Control based Burner Management Systems

4 Results

The Ansaldo Energia 800xA Safety system is identical to the ABB AB Control Technologies 800xA Safety system. Therefore the results documented in Report No. AV84798C are valid.

5 Implementation Conditions and Restrictions

The use of the AC 800M High Integrity system and the S800 High Integrity I/O modules shall comply with the current version of the Safety parts of the manuals:

- AC 800M High Integrity – Safety Manual
- AC 800M High Integrity – Reliability and Availability
- S800 I/O, Modules and Termination Units
- S800 I/O, Getting Started
- AC 800M, Controller Hardware

The relevant implementation and installation requirements have to be followed if the AC 800M High Integrity system is used in safety-related installations.

The recommendations and installation requirements, based on the experience and judgement of Ansaldo Energia S.p.A. and documented in the manuals, shall therefore be carefully followed. The information, recommendations, specifications and safety instructions given in the belonging manuals shall be read and understood.

5.1 General application conditions

5.1.1. Only modules certified for safety-related operation, as shown in the current revision of the Annex A to this report shall be used for safety-critical signals.

5.1.2. The fault tolerance period (process safety time) of the process controlled by the system shall be greater than the worst-case response time of the system.

5.1.3. A well-defined shutdown procedure shall be specified.

5.1.4. Operator alarms as exclusive means of shutdown are only permitted under supervised operation and if the fault tolerance time of the controlled process is sufficiently long to ensure a safe manual reaction and shutdown and the operator has sufficient independent means to supervise the process. Installations that must react to shutdown conditions quicker than achievable with manual intervention or installations running unsupervised shall incorporate an automatic fault reaction procedure.

5.1.5. The S800 High Integrity I/O shall be used in safety-related applications only in combination with the AC 800M High Integrity controller (including safety-related communication via CEX-bus and ModuleBus) and the Control Builder M.

5.1.6. The operating conditions as specified in the user manuals shall be met.

5.1.7. The timing requirements of the application standards must be approved for the safety-related peer-to-peer communication.

5.1.8. The components of the system versions belonging to the certificate Z10 11 11 78846 001 can be combined with the components of system versions related to this certification report (as stated in the Annex A). As a result, the safety functions build up using these combined system versions shall be used in the certification scope of Z10 11 11 78846 001 only.

5.2 General commissioning conditions

5.2.1. Prior to commissioning, a complete functional test of all safety-relevant programmed application functions shall be performed.

5.2.2. All timing requirements shall be validated.

5.2.3. Any application software modification after commissioning shall result in a complete re-validation of the changed parts of the programmed safety function. The Difference Report identifies the changed part of the programmed safety function, and it shall be verified that this report complies with the intended changes.

5.2.4. 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

5.3.1. 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 for AC 800M High Integrity controller and the S800 High Integrity I/O modules are documented in the AC 800M High Integrity Reliability and Availability.

5.3.2. Application program modification during run-time should only be permitted under end-user responsibility.

5.3.3. The procedure described in the user manuals has to be followed.

5.3.4. The application program modifications shall be limited and simple to verify and validate.

5.3.5. The modifications and their interaction with existing program sections shall be thoroughly tested, e.g. using simulation.

5.3.6. The modification shall be granted by the approval authority for the plant assessment.

5.3.7. Maintenance override is to be limited (time-restriction and number) of logical points according to the relevant application standards. The full responsibility of maintenance overrides lies with the user of the system. The TÜV guidelines for maintenance overrides are to be followed.

6 Certificate Number

This report specifies technical details and implementation conditions required for the application of the safety-related programmable system 800xA Safety by Ansaldo Energia S.p.A. on the certificate:

Z10 14 03 78846 002

M6A 14 03 78846 003

Munich, 2014-03-10

P. Weiß

Technical Certifier