Report

on the

Certificate

Z10 16 11 20160 011

Fail-Safe Controller System Family FSC Version 80x.x

Manufacturer:
Honeywell Safety Management Systems
Burgemeester Burgerslaan 40
5245 NH Rosmalen
Netherlands

Report no. HR90153C
Revision 1.2 of 2018-11-14

Test Body
TÜV SÜD Rail GmbH
Rail Automation
Barthstrasse 16
D-80339 Munich

Certification Body
TÜV SÜD Product Service GmbH
Ridlerstrasse 65
D-80339 Munich

TABLE OF CONTENTS

Revision Log

Revision	Date	HW Rev.	SW Rev.	Author	Status	Modifications
1.0	2016-11-14	R800.2	80.02	M. Braun	Initial	FSC Version 800.2 Project No. 717511398
1.1	2018-01-25	R801.1	80.11	M. Braun	Approved	FSC Version 801.1 Project No. 717515976
1.2	2018-11-14	R801.2	80.12	M. Braun	Approved	FSC Version 801.2 Project No. 717517998

Table 1: Revision

1 Target of Evaluation (ToE)

In 10-Aug-2015 the company Honeywell Safety Management Systems assigned TÜV SÜD for re-certifying of the Fail-Safe Controller System Family FSC Version 80x.x according to SIL 1-3 of IEC 61508: 2010 series and EN 61511.

The Fail-Safe Controller System Family FSC Version 80x.x is a fail-safe programmable controller (PLC) suitable in particular for

- safety-related applications requiring approval and
- applications not requiring approval but with a high risk potential
  (e.g. control or protection systems for chemical processes or fire detection and alarm systems).

The Certification Report HH84623C, revision 1.5 of 10th May 2016 on FSC Version 710.x is the basis for this Certification Report.

Central Part configuration	I/O configuration	CPU type	Architecture	Voting
Single	Single	10020/1/1 or 10020/1/2 (QPM)	DMR	1oo2
		10002/1/2 or 10012/1/2	1oo1D	1oo1D
Redundant	Single, redundant, single and redundant	10020/1/1 or 10020/1/2 (QPM)	QMR	2oo4D
		10002/1/2 or 10012/1/2	1oo2D	1oo2D

(QPM – Quad Processor Module, QMR – Quadruple Modular Redundant, DMR – Dual Modular Redundant)

Table 2: FSC architectures

2 System overview

2.1 Description

The Fail-Safe Controller System Family FSC Version 80x.x is an integrated safety solutions platform, forms the basis for functional safety, securing operations personnel, plant equipment and environment as well as ensuring optimum availability for plant operations.

Based on Quadruple Modular Redundant (QMR) technology, FSC Version 80x.x supports a wide range of high integrity process control and safety functions including:

- High-integrity process control
- Burner/boiler management systems
- Process safeguarding and emergency shutdown
- Turbine and compressor safeguarding
- Fire and gas detection systems
- Pipeline monitoring.

FSC Version 80x.x provides a dual redundant fault tolerant controller for safety and shutdown applications on the TPS system's Universal Control Network (UCN) and the Experion system through the Scada protocol. These safety functions are integrated into the architecture to support unified operations and control, while at the same time providing the ability to isolate emergency shutdown (ESD) functions from process control strategies on a separate safety network.

The Fail Safe Controller can be supplied in a number of architectures, each with its own characteristics and typical applications. Table 2 above provides an overview of the available architectures. The system can be configured in a number of different basic architectures (1oo1D, 1oo2D, QMR) depending on the requirement class of the process, the availability required and the FSC hardware modules used. This also means that field signals can be handled in multiple voting schemes (1oo1, 1oo1D, 1oo2, 1oo2D, 2oo4D).

The certified system encompasses the hardware modules listed below (see chapter 2.1.3 and 2.1.4) as well as the corresponding operating system with the specified software functions.

2.1.1 Test specimen

See Table 2.

2.1.2 Functional block diagram

Single Central Part and Single I/O (1oo1D, DMR) architecture has a single Central Part and single input and output (I/O) modules. No redundancy is present except as built into those modules where redundancy is required for safety (memory and watchdog).

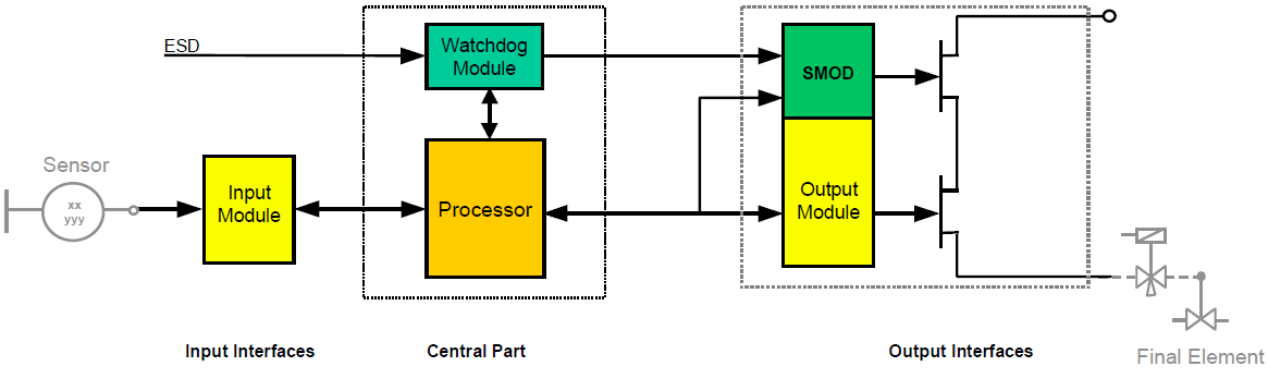

Figure 1: Single Central Part, single I/O

The next FSC architecture has redundant Central Parts and single input and output (I/O) modules. The processor is fully redundant, which allows continuous operation and bump less (zero-delay) transfer in case of a Central Part failure.

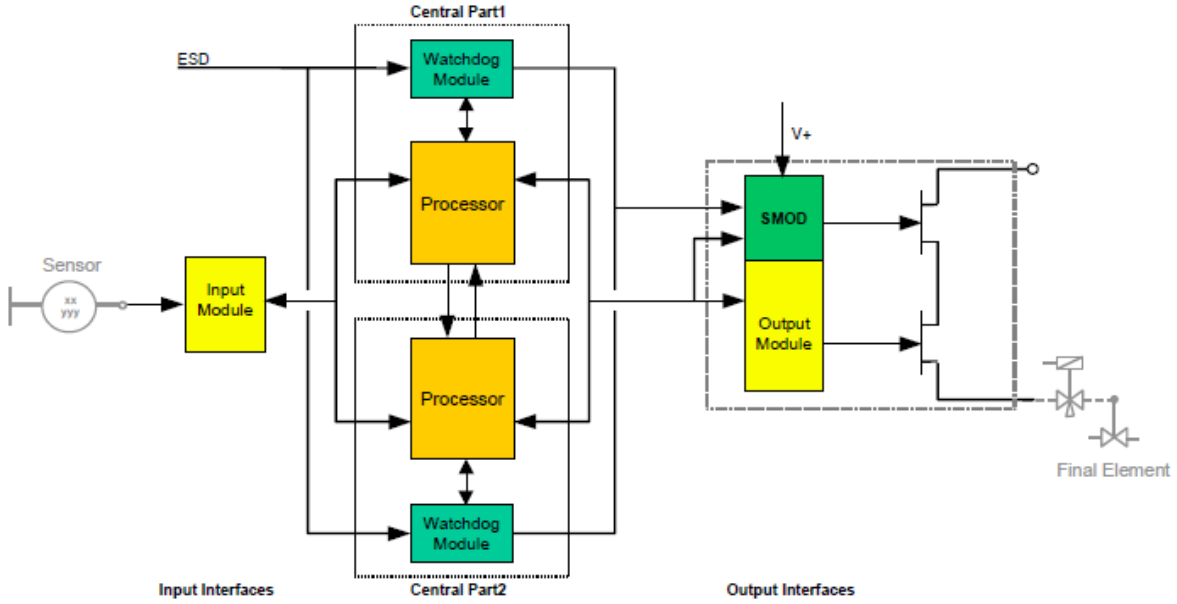

Figure 2: Redundant Central Parts, single I/O

This FSC architecture has redundant Central Parts and redundant input and output (I/O) modules (OR function on outputs). The processor and I/O are fully redundant, which allows continuous operation and bump less (zero-delay) transfer in case of a Central Part or I/O failure.

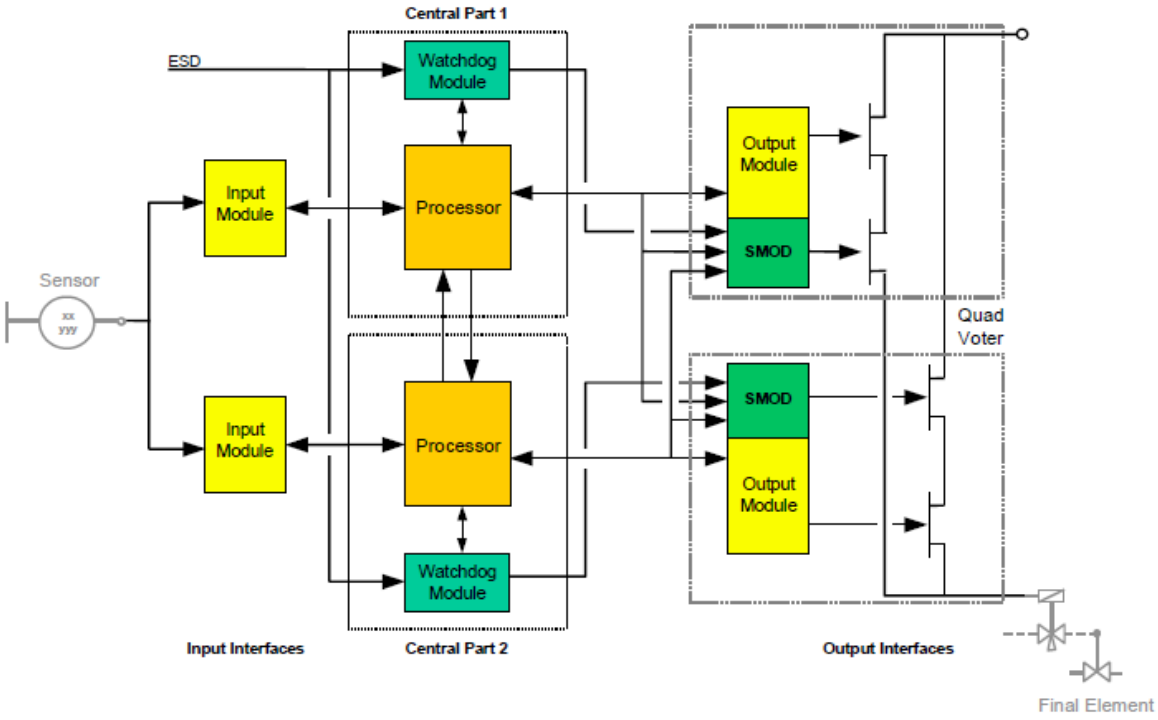

Figure 3: Redundant Central Parts, redundant I/O

The FSC architecture below has redundant Central Parts and redundant input and output (I/O) modules (OR function on outputs) combined with single input and output modules. The processor and I/O are fully redundant, which allows continuous operation and bump less (zero-delay) transfer in case of a Central Part or I/O failure of the redundant I/O modules.

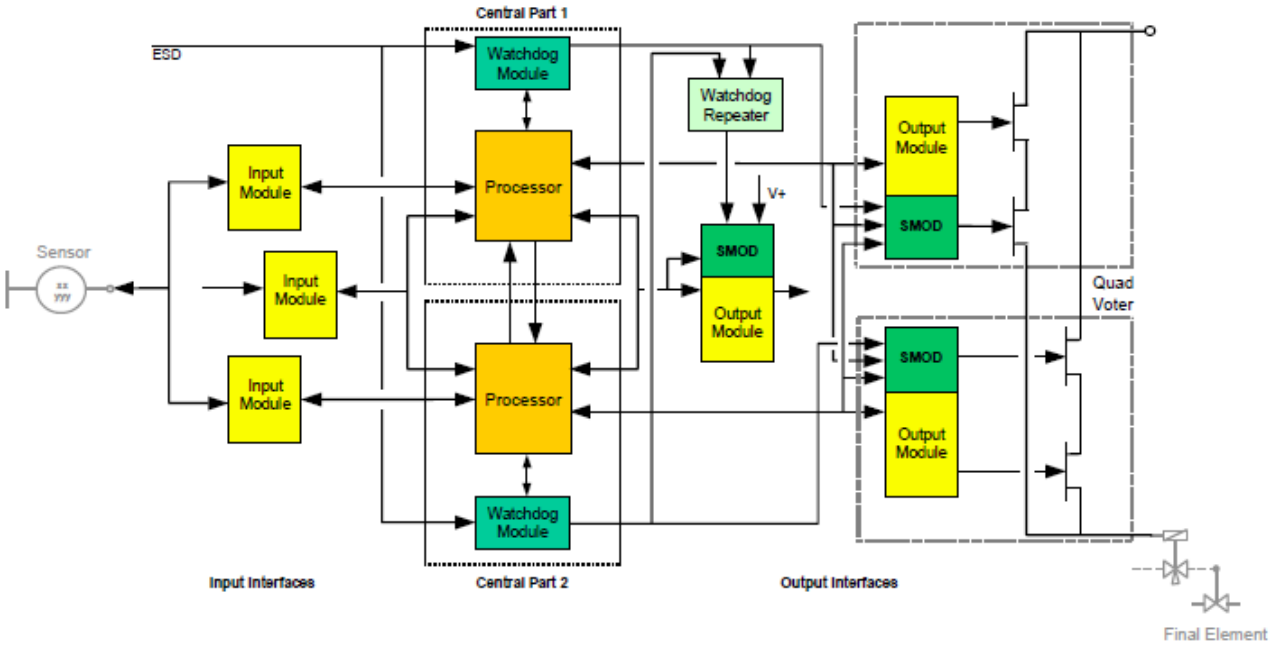

Figure 4: Redundant Central Parts with redundant and single I/O

The Quadruple Modular Redundant (QMR™) architecture with 2oo4D voting is an evolution of the proven 1oo2D concept. The QMR™ architecture with 2oo4D voting is based on dual-processor technology, and is characterized by a high level of diagnostics and fault tolerance.

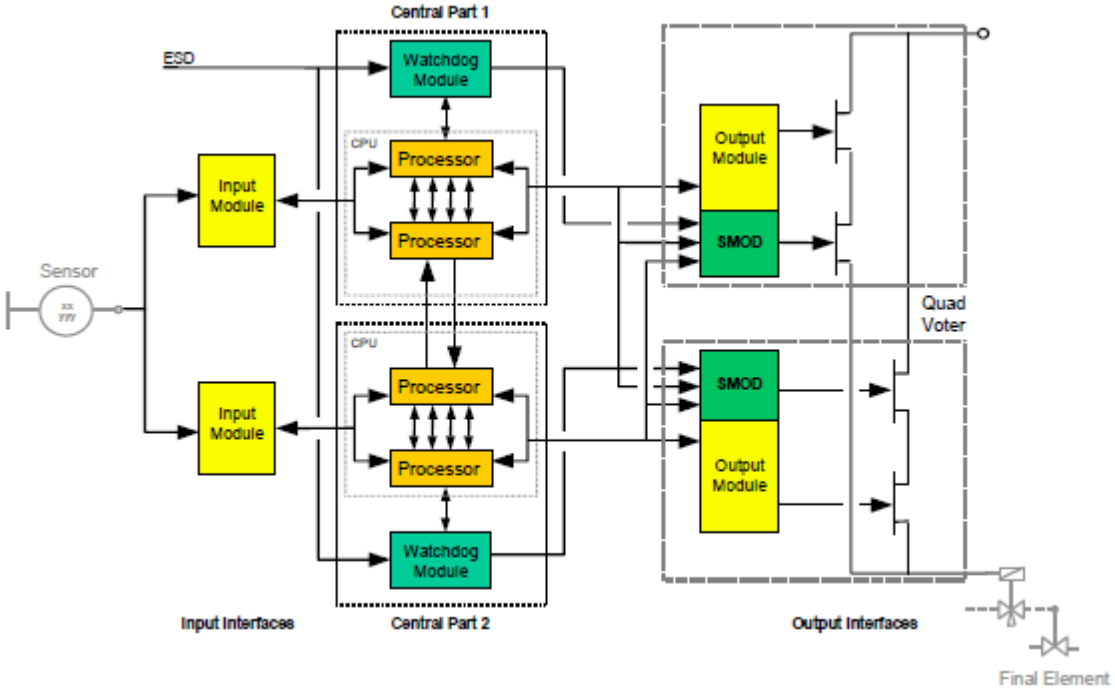

Figure 5: QMR architecture

2.1.3 Safety-Related Modules

The certified version of the operating system supports the following tested modules within the approved configurations in safety-related applications:

Module Number	Module Description
10001/1/1CC	Vertical bus driver
10001/R/1CC	Vertical bus driver (relay)
10002/1/2CC	Central processing unit (EPROM memory)
10012/1/2CC	Central processing unit (FLASH memory)
10020/1/1CC	Quad processor module -QPM- (Flash memory)
10020/1/2CC	Quad processor module -QPM- (Flash memory)
10004/./.CC	Communication module (EPROM memory)
10014/./.CC	Communication module (EPROM, FLASH memory)
10005/1/1CC	Watchdog module
10007/1/1CC	Single bus driver
10024/./.CC	Enhanced Communication module (EPROM, FLASH memory)
10100/1/1 and 10100/2/1 and FC-IO-0001	Horizontal bus driver

Module Number	Module Description
10101/1/1 and 10101/2/1 and FC-SDI-1624	16 channel digital input module 24 VDC
10101/1/2 and 10101/2/2	16 channel digital input module 60 VDC
10101/1/3 and 10101/2/3 and FC-SDI-1648	16 channel digital input module 48 VDC
10102/1/1	4 channel analog input module for non-redundant systems
10102/1/2 and 10102/2/1 and FC-SAI-0410	4 channel analog input module for redundant systems and non-redundant systems
10105/2/1 and FC-SAI-1620m	16 channel high-density analog input module
10106/2/1 and FC-SDIL-1608	16 channel line-monitored digital input module with earth fault monitor
10201/1/1 and 10201/2/1 and FC-SDO-0824	8 channel digital output module 24 VDC
10205/1/1 and 10205/2/1 and FC-SAO-0220m	2 channel analog output module
10212/1/1	8 channel digital output module 24 VDC (4 channel fail-safe, 4 channel non-interacting)
10213/1/1 and 10213/2/1 and FC-SDO-04110	4 channel digital output module 110 VDC
10213/1/2 and 10213/2/2	4 channel digital output module 60 VDC
10213/1/3 and 10213/2/3 and FC-SDO-0448	4 channel digital output module 48 VDC
10214/1/2	3 channel digital output module 220 VDC
10215/1/1 and 10215/2/1 and FC-SDO-0424	4 channel digital output module 24 VDC
10216/1/1 and 10216/2/1 and FC-SDOL-0424	4 channel digital output module 24 VDC with loop-monitoring
10216/2/3 and FC-SDOL-0448	4 channel digital output module 48 VDC with loop-monitoring
10302/1/1 and 10302/2/1	Watchdog repeater
10305/1/1	16 channel analog input converter
10311/2/1	Dual key switch module
FTA-T-02	Fail-safe digital output FTA (24/48/60 VDC, 24 channels)
FC-TSDO-0824	Fail-safe digital output FTA (24 Vdc, 8 channels)
FC-TSAI-0410	Fail-safe analog input FTA (4 channels)
FC-TSHART-1620m	Fail-safe 0(4)-20 mA analog input FTA with HART interface (16 channels)
FC-TSAO-0220m	Fail-safe analog output FTA (0(4)-20 mA, 2 channels)
FTA-T-05	Fail-safe digital output FTA (24 VDC, 12 channels)
FC-TSDO-0424	Fail-safe digital output FTA (24 Vdc, 4 channels)
FTA-T-06	115 / 230 VAC digital input FTA Fail-Safe (potential free input contacts)

Module Number	Module Description
FTA-T-07	115 / 230 VAC digital input FTA Fail-Safe, power supply voltage supplied from FTA
FTA-T-08	4-channel digital output (Relay) FTA Fail Safe, 115/230 VAC
FTA-T-09	8 channel digital input FTA 115 VAC/DC passive Fail Safe
FTA-T-13	16 channel digital input FTA 24 VDC (current-limited),
FTA-T-14	16 channel analog input FTA, 0(4) - 20 mA
FC-TSAI-1620m	Fail-safe 0(4)-20 mA analog input FTA (16 channels)
FTA-T-15	24 VDC to 30 VDC/1 A converter
FC-TPSU-2430	24 Vdc to 30 Vdc/1 A converter
FTA-T-16	16 channel active digital input FTA with line-monitoring
FTA-T-17	4 channel digital output (relay) FTA for SIL 3 applications
FC-TSRO-0824	Safe digital output (relay) FTA for SIL 3 applications (8 channels)
FC-TSRO-08UNI	Safe common external power relay output FTA for SIL3 applications (8 channels)
FTA-T-18	Fail-safe Gas / Flame detector input
FC-TSGAS-1624	Fail-safe Gas -Flame detector input FTA (0 - 20 mA, 16 channels)
FTA-T-19	Fail-safe Fire detector input FTA with line monitoring
FC-TSFIRE-1624	Fail-safe Fire detector input FTA with line monitoring (24 Vdc, 16 channels)
FTA-T-21	Fail-safe digital input FTA (24/48/60 VDC, NAMUR, 16 channels)
FC-TSDI-16UNI	Fail-safe digital input FTA (24/48 Vdc, NAMUR, 16 channels)
FTA-T-23	16 channel digital input FTA 24 VDC (current-limited),
FC-TSDI-1624C	Current-limited digital input FTA (24 Vdc, 16 channels)
FTA-T-29	Fail safe active/passive digital input FTA 115V VAC/DC, 16 channels
FC-TSDI-16115	Fail-safe active/passive digital input FTA (115 Vac/dc, 16 channels)
FTA-T-35	Fail-Safe digital output FTA, current limited (24Vdc, 8 channels)
FC-TSDO-0824C	Fail-safe digital output FTA, current limited (24 Vdc, 8 channels)
FTA-T-36	Fail-Safe digital output FTA, current limited (24Vdc, 4 channels)
FC-TSDOL-0424C	Fail-safe digital output FTA, Current limited (24 Vdc, 4 channels)
M24 - 20 HE	110 VAC / 220 VAC / 234 VAC to 24 VDC power supply unit
M24 - 12 HE	110 VAC / 220 VAC / 234 VAC to 24 VDC power supply unit
M48 - 10 HE	110 VAC / 220 VAC / 234 VAC to 48 VDC power supply unit
M60 - 5 HE	110 VAC / 220 VAC / 234 VAC to 48 / 60 VDC power supply unit
1200 S 24 P067	110 VAC / 220 VAC / 234 VAC to 24 VDC power supply unit
GK 60	24 VDC / 5 VDC power supply unit
10300/1/1	24 VDC / 5 VDC power supply unit
10303/1/1	Power supply distribution module
FC-PSU-UNI2450U	System Power Supply, input 115/230VAC output 24Vdc, 50A, UL508
FA-PSU-UNI2450U	System PSU, input 115/230VAC output 24Vdc, 50A, UL508, ATEX
FC-PSU-UNI4825U	System Power Supply, input 115/230VAC output 48Vdc, 25A, UL508

Module Number	Module Description
FC-PSU-UNI6020U	System Power Supply, input 115/230VAC output 60Vdc, 20A, UL508
FC-PSU-UNI11011U	System PSU, input 115/230VAC output 110Vdc, 11A, UL508
FC-PSU-UNI12010U	System PSU, input 115/230VAC output 120Vdc, 10A, UL508
FC-FDOVP-2450	System Power Supply input 24VDC output 24Vdc, 50A, UL 508

Details on withdrawn modules see current version of the "Fail Safe Control Hardware Manual".

Table 3: Tested safety-related modules

2.1.4 Tested, non-interacting Modules

The certified version of the operating system supports the following tested, non-safety-related and non-interacting modules:

Module Number	Module Description
10006/1/1	Diagnostic and battery module
10006/2/1	Diagnostic and battery module with RTC clock
10006/2/2	Diagnostic and battery module with DCF clock
10008/2/U	FSC-SMM communication module (EPROM memory)
10018/2/U	FSC-SMM communication module (FLASH memory)
10018/E/1 and 10018/E/E	Communication module Ethernet (FLASH memory)
10008/3/P	FSC-PBUS communication module
10103/1/1	4 channel EExi intrinsically-safe input module
10104/1/1 and 10104/2/1	16 channel digital input module 24 VDC
10206/1/1 and 10206/2/1 and FC-DO-1224	12 channel digital output module 24 VDC
10207/1/1	8 channel EExi intrinsically-safe optocoupler output module 24 VDC
10208/1/1	12 channel relay output module 24 VDC
10208/2/1 and FC-RO-1024	10 channel relay output module 24 VDC
10209/1/1 and 10209/2/1 and FC-DO-1624	16 channel digital output module 24 VDC
FTA-T-10	8 channel digital output (relay) FTA- NFS
FTA-T-12	8 channel isolated digital input FTA-NFS (passive)
FTA-T-20	8 channel digital output (relay contact) FTA (NO/NC)
FC-TRO-0824	Digital output (relay contact) FTA (8 channels, NO/NC)

Details on withdrawn modules see current version of the "Fail Safe Control Hardware Manual".

Table 4: Tested non-interacting modules

2.1.5 Mechanical and electrical parts

The mechanical and electrical parts of the FSC Fail-Safe Controller System such as cabinet enclosure, backplanes, buses and system interconnecting cables are described in the current version of the "Fail Safe Control Hardware Manual".

2.1.6 Safety-Related Software Functions

The certified version of the operating system supports the following tested software functions in safety-related applications:

- Reading and generating digital and analogue input and output signals
- Processing timer and counter data
- Processing the user program in function block mode
- Analogue value processing
- Calculation functions including floating point functions
- User-defined function blocks
- Equation blocks
- Communication, see chapter
  2.6.1 Safety-Related Communication (FSC protocol and SafeNet protocol) and
  2.6.2 Safety-Related Communication (RKE 3964R Protocol)

2.1.7 Tested, non-interacting Software Functions

The certified version of the operating system supports the following tested, non-safety-related but non-interacting software functions:

- Processing of multiplexed input / output signals
- Alarm sequences
- PID algorithm
- Sequence of event recording (SER)
- Communication, see chapter 2.6.3 Non-Safety-Related Communication
- Real Time Clock (RTC, DCF)

2.2 Certified System Configurations

For safety-related operation of the FSC Version 80x.x, a configuration in accordance with the Safety Integrity Level as per the following table shall be selected.

Quad processor module 10020/1/1 and 10020/1/2 (dual processor):

System	**single CP - single I/O** (DMR, 1oo2 voting)	**redundant CP - single I/O** (QMR, 2oo4D voting)	**redundant CP - redundant I/O** (QMR, 2oo4D voting)
Safety Integrity Level	SIL 1 – 3	SIL 1 – 3	SIL 1 – 3
Number of central parts	1	2	2
Minimum number of Bus Systems (Note 2, VBD 10001/x/1)	1	1	2
System response in the event of faults, i.e. internal fault conditions attributable to a central part (Note 3)	System shutdown	Shutdown of defective central part and continued operation for unlimited period using intact central part (Note 1).	Shutdown of defective central part and continued operation for unlimited period using intact central part (Note 1).
System response in the event of failure of failsafe input modules (Note 3)	Defective digital inputs are read as “0 signal” and in the case of analog inputs, the configured minimum limit is used. "System shutdown, process group shutdown or alarm” shall be programmed.	Defective digital inputs are read as “0 signal” and in the case of analog inputs, the configured minimum limit is used. "System shutdown, process group shutdown or alarm” shall be programmed.	The input signals recognized as defective (set to "0" for digital inputs and minimum limit for analog inputs) are overwritten by the correct input signals from the other central part and an alarm is generated. "System shutdown, process group shutdown or alarm” shall be programmed.

System	**single CP - single I/O** (DMR, 1oo2 voting)	**redundant CP - single I/O** (QMR, 2oo4D voting)	**redundant CP - redundant I/O** (QMR, 2oo4D voting)
System response in the event of failure of fail-safe output modules (Note 3)	Depending on the locality of the fault, the system responds as follows: • Group shutdown of the channel concerned with continued operation for a period of time defined by the manufacturers PFD calculation for a specific system of the channel concerned or • System shutdown	Depending on the locality of the fault, the system responds as follows: • Group shutdown of the channel concerned with continued operation for a period of time defined by the manufacturers PFD calculation for a specific system or • System shutdown	Depending on the locality of the fault, the system responds as follows: • Group shutdown of the channel concerned with continued operation for a period of time defined by the manufacturers PFD calculation for a specific system or • Shutdown of the affected central part Continued operation for unlimited period of time using intact central part

Table 5: Quad processor module 10020/1/1 and 10020/1/2 (dual processor)

Note 1: Faults in redundant central parts, which are detected and localised by self-tests result in single-central part operation with an unlimited time period. The mode of operation; single or redundant does not influence the coverage of self-tests. The self-test interval is not extended for single-central part operation. The self-test interval shall be less than the fault tolerance period of the process (PST).

Note 2: Multiple VBD Bus systems may be used for expansion and I/O segregation.

Note 3: For detailed Information see the current version of the FSC Safety Manual

Central processing unit 10002/1/2 and 10012/1/2 (single processor):

System	**single CP - single I/O (1oo1D)**	**redundant CP - single I/O (1oo2D)**	**redundant CP - redundant I/O (1oo2D)**
Safety Integrity Level	SIL 1 - 3	SIL 1 - 2	SIL 1 - 3
Number of central parts	1	2	2
Minimum number of Bus Systems (Note 6) (VBD 10001/x/1)	1	1	2
System response in the event of localisable faults, i.e. internal fault conditions attributable to a central part (Note 5)	System shutdown	<u>SIL 1 - 2:</u> Shutdown of defective central part and continued operation for unlimited period using intact central part. <u>SIL 3:</u> Possible system response: • Shutdown of defective central part and single-channel operation for a period of time defined by the manufacturers PFD calculation for a specific system. (Note 4) System shutdown can be programmed by means of user program.	
System response in the event of I/O comparison errors (non-localisable) Input comparison		In the event of input signals recognised as inconsistent by comparison, the system switches to the safe condition of the affected input and indicates this by a system flag. The fault response "System shutdown, process group shutdown or alarm" shall be programmed. Or if • the process is continuously monitored by an operator AND • the process safety time is sufficiently long to insure manual shutdown AND • the operator has sufficient means to monitor and shutdown the process independent of the FSC system AND • the fault is annunciated by fail-safe means manual reaction and shutdown is permissible.	

System	single CP - single I/O (1oo1D)	redundant CP - single I/O (1oo2D)	redundant CP - redundant I/O (1oo2D)
System response in the event of I/O comparison errors (non-localisable) Output comparison		An output comparison error is indicated by a system flag. The fault response “System shutdown, process group shutdown or alarm” shall be programmed. <u>SIL2</u>: IF • the process is continuously monitored by an operator AND • the process safety time is sufficiently long to insure manual shutdown AND • the operator has sufficient means to monitor and shutdown the process independent of the FSC system AND • the fault is annunciated by fail-safe means manual reaction and shutdown is permissible. <u>SIL3</u>: System shutdown	
System response in the event of failure of fail-safe output modules (localisable fault)	Depending on the locality of the fault, the system responds as follows: • Shutdown of output signal or • Group shutdown or • System shutdown	Depending on the locality of the fault, the system responds as follows: • Shutdown of output signal of the channel concerned or • Group shutdown of the channel concerned • System shutdown	Depending on the locality of the fault, the system responds as follows: • Shutdown of output signal of the channel concerned or • Group shutdown of the channel concerned or • Shutdown of the affected central part • <u>SIL 3</u>: Continued operation for a period of time defined by the manufacturers PFD calculation for a specific system. (Note 4)
	Process group shutdown or system shutdown shall be programmed.	Process group shutdown or system shutdown shall be programmed.	Process group shutdown or system shutdown shall be programmed.

System	single CP - single I/O (1oo1D)	redundant CP - single I/O (1oo2D)	redundant CP - redundant I/O (1oo2D)
System response in the event of failure of fail-safe input modules (localisable faults)	Defective digital inputs are read as “0 signal” and in the case of analogue inputs, the configured minimum limit is adopted. "System shutdown, process group shutdown or alarm” shall be programmed.	Defective digital inputs are read as “0 signal” and in the case of analogue inputs, the configured minimum limit is adopted. The fault response "System shutdown, process group shutdown or alarm shall be programmed OR if • the process is continuously monitored by an operator AND • the process safety time is sufficiently long to insure manual shutdown AND • the operator has sufficient means to monitor and shutdown the process independent of the FSC system AND • the fault is annunciated by fail-safe means manual reaction and shutdown is permissible.	The input signals recognised as defective are overwritten by the correct input signals from the other channel and an error message is generated. The fault response "Process group shutdown or alarm” with continued operation for a period of time defined by the manufacturers PFD calculation for a specific system (Note 4) or "System shutdown" shall be programmed.

Table 6: Central processing unit 10002/1/2 and 10012/1/2 (single processor)

Note 4: Faults in redundant central parts which are detected and localised by the self-tests result in single-central part operation for a limited time period. The mode of operation; single or redundant does not influence the coverage of the self-tests. The self-test interval is not extended for single-central part operation. The self-test interval shall be less than the fault tolerance period of the process (PST).
The fail-to-danger-rate of an application including sensors and positioners at the controller’s ascertained MTBF figures and fault coverage rates are not significantly increased by single-channel operation for a limited period. This period has to be defined by the manufacturers PFD calculation for a specific system
The calculated maximum duration for single-central part operation depends on the specific process concerned and must be specified individually for each application. On the FSC system, this is specified by means of the system parameter "Interval time between faults".

Note 5: SIL 1- 2: All faults which are only detected by comparing the internal system statuses of the two central parts and cannot be localised result in a system alarm

SIL 3: For central parts and output failures all faults which are only detected by comparing the internal system statuses of the two central parts and cannot be localised result in immediate shutdown of the system.

Note 6: Multiple VBD Bus systems may be used for expansion and I/O segregation.

2.3 Reconfiguration

The reconfiguration options possible and permissible depend on the safety classification applicable in each case and the system configuration.

In the event of faults on a safety-related input module, the input signal concerned is masked out (input signal set to zero, error flag set). In the event of faults on a safety-related output module, a sub-process shutdown is performed if a sub-process has been configured to which the output concerned belongs.

The following table illustrates the relationship between the defined system configuration and the permissible reconfiguration in the event of faults, which are not covered by the above fault responses to peripheral faults. In particular, this includes central part faults and faults on the vertical and horizontal busses as well as faults on safety-related output modules if no sub-processes have been configured.

System Configuration	Reconfiguration	Action After Elimination of Fault
single CP - single I/O	System shutdown	Restart after clearance from the operator
redundant CP - single I/O	single CP - single I/O in the event of faults on the central part. System shutdown or process group shutdown in the event of faults on a safety-related output module	redundant CP - single I/O Restart after clearance from the operator
redundant CP – redundant I/O	single CP - single I/O	redundant CP - redundant I/O

Re-activation of subsystems after repair is possible while the system is running. In such cases, the restarted central part copies the data from the running system. The operator should treat all error messages on start-up with particular caution.

2.4 Mixed Configurations

In order to provide greater capability of process-specific risk analysis and allocation of process signals to specific Safety Integrity Level, the FSC system offers the facility of mixed configuration. The mixed configuration "redundant CP - redundant I/O" / "redundant CP - single I/O)" allow processing signals of the Safety Integrity Level up to and including SIL 3.

2.5 Possible Wiring Alternatives for Safety Integrity Level SIL 1 to SIL 3

2.5.1 Inputs

For SIL 3 with redundant inputs, the input modules of both channels shall be used. Safety-related process variables shall be read from both busses.

If fail-safe sensors are used for SIL 3 with single I/O, one controller input for each safety-related process signal is sufficient. Programming and connection of inputs for non fail-safe sensors is explained in detail in the Appendix C "Safety-Related Inputs with Non-Fail-Safe Sensors" of the current FSC Software Manual.

2.5.2 Outputs

The shutdown circuits in safety-related applications shall always take the form of dual independent circuits. In single I/O configurations up to and including SIL 3 this is provided by connection of the output signal in series with the integrated secondary means of deenergization (group shutdown or total shutdown via watchdog) on the safety related output modules.

In order to increase availability, in the system configuration "redundant CP - redundant I/O", the outputs of both channels are connected in parallel.

In accordance with the application-specific standards, it is assumed that for SIL 3 applications, redundant actuators will normally be used, each of which is capable of bringing the process to a safe condition.

2.6 Communication

The certified version of the operating system supports the following communication protocols:

Data Transmission Protocol	**Transmission of Safety-Related Data Permissible?**
FSC protocol for communication between two redundant central parts (up to SIL 3)	Yes
FSC protocol for communication (multi-drop and point to point) between FSC systems where one of the peers is running on a FSC release **< R800.x** (up to SIL 3)	Yes
SafeNet protocol for communication (multi-drop only) between FSC systems that are running on a FSC release **>= R800.2** (up to SIL 3)	Yes
SafeNet protocol for communication (multi-drop only) between FSC systems that are running on a FSC release **>= R801.1** and Safety Manager systems that are running on a Safety Manager release **>= R161.1** (up to SIL 3), restriction on compatibility see 5.5.2	Yes
Modified RKE3964R protocol for communication (point to point) via public telecommunication services (up to SIL 2) with extra measures for data integrity in the application program via the FLD modules: MASTER_1, FIRST ISSUE, 07-26-1998 SLAVE_62, FIRST ISSUE, 07-26-1998	Yes
Communication via standard RKE3964R protocol	No
Communication with FSC Navigator	No
Transmission of data from and to peripheral systems (printer, process control system, etc.)	No
Communication via Modbus (RTU)	No
Communication via Universal Control Network (UCN) with the HONEYWELL Total Plant Solution System	No
Communication via Ethernet with the HONEYWELL Experion PKS system and Plantscape system	No
Communication via PBUS with the ABB Automation Contronic E/S process control system	No

Table 7: Supported communication protocols

2.6.1 Safety-Related Communication (FSC protocol and SafeNet protocol)

The FSC system permits distributed configuration of safety-related systems. In such cases, two basically different communications structures between the individual FSC systems can be constructed:

- point to point links (on FSC-FSC protocol, only)
- multi-drop links

Both communications structures can be used within the same system configuration. To assist communication in such a network, one system can be configured as a communications server.

The complete communications route including non-safety-related transmission components such as modems or fibre-optic cable links are covered by the safety procedures used.

The safety-related data (marker bytes and register bytes) to be transmitted between the FSC systems shall be identified as such during the parameterisation process.

The transmission times inherent in communication have the effect of lengthening the fault response times of the relevant FSC systems. The increased fault response time must be taken into account and shall not exceed the process safety time of the application concerned.

Additional important information on FSC communication is given in the FSC Safety Manual.

2.6.2 Safety-Related Communication (RKE 3964R Protocol)

To establish communication via public telecommunication services the modified RKE 3964R protocol together with extra measures for data integrity in the application program can be used to exchange safety related data up to SIL 2.

The extra measures must be programmed via the FSC logic functions and must fulfil following requirements:

- Timing integrity
- Address integrity
- Data integrity
- Wrong sequence of telegrams

Unlike the regular FSC protocol, these requirements are not implicitly covered with the standard RKE 3964R communication protocol, but must be programmed via the FSC logic functions realised with the modules MASTER_1 and SLAVE_62.

The RKE protocol is a Point to Point protocol, and cannot be used for multi-drop communications.

The complete communications route including non-safety-related transmission components such as modems or fiber-optic cable links are covered by the safety procedures used.

The safety-related data (marker bytes and register bytes) to be transmitted between the FSC systems shall be identified as such during the parameterisation process.

The transmission times inherent in communication have the effect of lengthening the fault response times of the relevant FSC systems. The increased fault response time must be taken into account and shall not exceed the process safety time of the application concerned.

Additional important information on RKE 3964R communication is given in the FSC Safety Manual.

Note: If safety relevant communication is used the FSC-FSC protocol is preferred because all safety checks are implemented in the system software.

2.6.3 Non-Safety-Related Communication

Use of the other transmission protocols provided by the FSC system - in particular the Universal Control Network (UCN) to the Honeywell TotalPlant Solution System, the Ethernet protocol to the Honeywell Experion PKS system and Plantscape system and the PBUS to the ABB Automation Contronic E/S process control system - will not impair the safety-related performance of the FSC system or an FSC network, assuming that parameterisation and application programming have been correctly performed.

The data sent and received by the non-safety-related protocols shall normally be considered as not relevant to safety and shall be processed on that basis. The data exchange between FSC system and the mentioned process control systems can be configured to be:

- read only
- read and write
  (write only for non-safety related variables in predefined memory areas)

2.6.4 Access to the FSC safety system by the FSC Navigator

During active operation of the safety functions, the following modes of access to the FSC safety system by the PC operated application development package „FSC Navigator“ are permitted:

Read access:

- Reading of process statuses and FSC safety system statuses
- Diagnostic status of the FSC safety system

Read access by maintenance functions of the FSC Navigator

- „On-line rebuild“ of the FSC database on the FSC Navigator
- Reading back and checking the running application program

Limited Write access is also permitted for the following functions subject to clearance from the operator. The responsibility for both functions lies with the operator.

- Forcing of "enabled" FSC variables.
  Forcing may only be authorised by way of a key-operated switch. Checking of which signals may be forced can be performed with the aid of a printout of the FSC variables.
- "Maintenance Override"
  Use of the “maintenance override” function must comply with the requirements set out in the current version of the document “Maintenance Override” published by TÜV SÜD and TÜV Rheinland.

2.7 Compiling the Application Program

The planning, programming and compiling of the application program are carried out with the aid of the “FSC Navigator“. Since the hardware environment of the FSC user station must be viewed as non-safety-related, additional facilities have been implemented in the FSC programming system in order to enable straightforward checking of correct compilation of the application for the user. The functions referred to below are described in detail in the FSC Safety Manual.

Compilation of the application is checked by an independent and diversely developed decompiler and comparator (“Verify FSC Application Software“ function). The project engineer shall perform a consistency check of the messages of that function on site and the CRC signature of the application software shall be compared with the CRC signature of the application work files.
The function “Verify FSC Application Software“ can also be employed as a revision comparator. In such situations, the modified application is compared with the original application. Based on the

expectation that all modifications must appear in the log file, it can be demonstrated that all modifications have been correctly incorporated in the new application.

2.8 Migrating an Application Program

The 'Verify Application' option of FSC Navigator can also be used to verify that the migration and download of an FSC application to a Safety Manager controller has been completed.

The customer shall execute 'Verify Application' on 2 separate PCs and compare the reported differences which should be identical.

The customer shall carry out a functional test on application level for at least one channel of each safety related input and output module.

2.9 FSC safety checker

The FSC safety checker is used to verify the safety consistency of any engineered FSC application created with the FSC Navigator software.
The principle of the FSC safety checker is, that any output which is used for safety critical applications (e.g. for shutdown purposes) should be set to safety related, and the path (inputs, logic) which results in this output should be safety related as well. Any inconsistency with this rule will be reported by the safety checker.

2.10 Modifying the Application Program during Operation

In the case of the redundant systems "redundant CP - single I/O", "redundant CP - redundant I/O" and mixed configuration "redundant CP - redundant I/O" / "redundant CP - single I/O", applications allow modifications to the application software to be carried out during active operation. A detailed description of the procedure involved is given in the Appendix D "On-Line Modification" in the FSC Software Manual.

2.11 Machinery Safety applications

The FSC system can be used for Machinery Safety applications. The FSC Machine Safety manual (PM.MAN.8172) describes basic machinery safety functions.
The connecting and signal handling details for these supported solutions are specified in the FSC Machine Safety Manual.

2.12 Release identification

This report covers the FSC Version 80x.x where x indicates the actual (maintenance) release.

For release 80x.x the following safety related software components shall be used:

Release	CPU System software version (safety related) / System Software CRC	Communication Modules, System software version (safety related)	Verify Application
800.2	80.02 / 0xA9FFB37F	80.02	60.1.0.0
801.1	80.11 / 0x9BD0C08F	80.11	60.2.0.0
801.2	80.12 / 0xE2FFE285	80.12	60.3.0.0

For details see individual release letters of R80x.x.
The hardware modules are listed in section 2.1.3 and 2.1.4.

3 Certification Requirements

3.1 Basis of Certification

The certification of the FSC Version 80x.x will be according to the regulations and standards listed in clause 3.3 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

Following test reports were issued by TÜV SÜD Rail GmbH or other accredited test laboratories.

No.	Title	Document-No./ File identifier	Revision	Date
[R1]	Report Fail-Safe Controller System Family, Version 710.x	SH99495C	7.10	2011-03-14
[R2]	Technical Report by TÜV SÜD Rail GmbH Assessment Report about the conformity according IEC 61508 of the FSC Fail-Safe Controller System Family	HH80661T	1.0	2003-05-13
[R3]	Technical Report Fail-Safe Controller System Family, FSC Version 710.x	HH84624T	1.0	2013-02-05
[R4]	Technical Report Fail-Safe Controller System Family, FSC Version 800.x	HR90152T	1.0	2016-11-11
[R5]	Test Report about the approval of the Safety Manager 160.2 TÜV Rheinland	968/EZ 195.38/16		2016-09-01

No.	Title	Document-No./ File identifier	Revision	Date
[R6]	Inspection Report FSM Assessment for product development according IEC 61508 TÜV NORD	SEBS-A.171939_13IR	1.0	2014-07-07
[R7]	EMC Test Report	BICON Report HON-20160603-E1-2.pdf		2016-07-19
[R8]	Technical Report of Modifications FSC Version R801.1	HR92047T	1.0	2018-01-25
[R9]	Technical Report of Modifications FSC Version R801.2	HR93212T	1.0	2018-11-14

Further certification documentation:

[1] FSC R800 Safety Manual (FS90-800) by Honeywell Safety Management Systems and reviewed by TÜV SÜD Rail GmbH.

Certification report on the most recently tested version:

[2] Report on the Certificate
FSC Fail-Safe Controller System Family
Version 710.x
HH84623C, revision 1.5 of 10th May 2016 on FSC Version 710.x

Based on the specified purpose of use of the FSC Version 80x.x 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:

No.	Standard	Title
[N1]	IEC 61508-1: 2010 (SIL 1 - 3)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 1: General requirements
[N2]	IEC 61508-2: 2010 (SIL 1-3)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 2: Requirements for electrical/electronic/ programmable electronic safety-related systems
[N3]	IEC 61508-3: 2010 (SIL 1-3)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 3: Software requirements
[N4]	IEC 61508-4: 2010 (SIL 1-3)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 4: Definitions and abbreviations
[N5]	EN 61511-1: 2004 (SIL 1-3)	Functional safety – Safety instrumented systems for the process industry sector Part 1: Framework, definition, system hardware and software requirements

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:

No.	Standard	Title
[N6]	EN 60068-2-1: 2007	Environmental testing Part 2: Tests; Tests A: Cold
[N7]	EN 60068-2-2: 2007	Basic environmental testing procedures Part 2: Tests; Tests B: Dry Heat
[N8]	EN 60068-2-6: 2008	Environmental testing Part 2: Tests; Tests Fc: Vibration (sinusoidal)
[N9]	EN 60068-2-27: 2009	Environmental testing Part 2: Tests; Tests Ea: Shock

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:

No.	Standard	Title
[N10]	EN 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

4 Results

4.1 Functional Safety

The tests performed and quality assurance measures implemented by the manufacturer have shown that the FSC Version 80x.x 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 1-3 in accordance with IEC 61508: 2010 and EN 61511 and can be used e.g. in applications as Emergency Shut Down (ESD), Fire & Gas detection and Burner Management Systems.

4.1.1 Fault Reaction and Timing

Fault detection in the FSC Version 80x.x is assured by means of following basic techniques:

- self test at power up and during operation
- two channel control logic with cross check
- redundancy
- dynamic signals
- de - energizing in case of over – and under-voltage
- de - energizing by watch dog monitoring

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.

Response Times:
The response time to external requests applied directly to the FSC system is no more than twice the cycle time of the automation system.
In the case of single-channel system configuration, individual faults capable of bringing about a dangerous operating condition are detected within the projected test cycle time (configured process safety time) by the self-test and external test facilities. In the case of redundant system configurations, additional to the selftests, individual faults are detected within the period of two cycles of the automation system by comparing the two channels.
In the case of distributed safety-related system configurations, additional fault response times must be taken into consideration (see FSC Safety Manual, chapter 5.3, entitled "FSC Networks").

Response of System to Faults:
The response of the FSC system to detected faults can be broadly determined by means of the application program. The responsibility for programming the system's response to faults lies with the application program developer. The standard system responses or system messages are detailed in the FSC Safety Manual in the chapter 6, "FSC System Fault Detection and Response".

Individual faults which can be definitely attributed to a particular central part by the highly effective self-tests result in reconfiguration in the case of the FSC systems "redundant CP - single I/O" and "redundant CP - redundant I/O" due to the dual-channel configuration and an error message is sent to the application program.

In the case of operation with continuous supervision, i.e. if the operator can observe the process and can react quickly enough to bring the process to a safe condition, a fail-safe alarm can be programmed instead of the system shutdown (see FSC Safety Manual, chapter 6 entitled "FSC System Fault Detection and Response").

4.1.4 Modifications to the Application Program during Operation

On-line modifications presuppose applications programs that have been subjected to particularly thorough testing beforehand, e.g. at simulators. In the case of such thoroughly tested application programs, it is sufficient for all modifications made to be subjected to a full function test in order to demonstrate correct functioning of the program. If non-safety-related modifications are made, they shall be subjected to suitable function tests in order to demonstrate absence of interaction.

In general, responsibility for monitoring the process during the period of on-line modification lies entirely with the person responsible for the on-line modification. Since on-line modifications are generally associated with an increased level of risk, the approval of on-line modifications is at the discretion of the testing and inspection center responsible for approval of the system.

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. No changes, compare [R1] for old references.

4.2.2 Environnemental Testing

The environmental stress tests are documented by the certificates of an accredited test centre. No changes, compare [R1] for old references.

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. Compare [R1] for old references and [R7] for additional required type tests.
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 quality assurance and control system.

As part of the certification process TÜV SÜD 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

Use of the Fail-Safe Controller System Family FSC Version 80x.x shall comply with the current version of the "Fail Safe Control (FSC) System Safety Manual" and the "Fail Safe Control (FSC) System Hardware Manual" and the "Fail Safe Control (FSC) Software Manual" and the “Fire and Gas Application Manual” and the “Fire and Gas Field Devices Interface Manual” and the “Fail Safe Control Machine Safety Manual” of the company Honeywell Safety Management Systems.

The following implementation and installation requirements have to be followed if the FSC Version 80x.x is used in safety-related installations. The conditions are arranged according to the major stages of engineering a programmable electronic system for safety-related instrumentation and protective equipment. The conditions are further subdivided into

- non-product-related conditions which are not determined by the characteristics of the certified system but by the fundamental nature of safety-related programmable electronic systems, and
- product-related conditions which arise from the characteristics of the certified system.

5.1 Planning; Non-Product-Related Conditions

5.1.1. The FSC Version 80x.x can be used in applications up to SIL 1-3 according to IEC 61508: 2010 and EN 61511.

5.1.2. Only approved fail-safe hardware modules may be used for safety-related operation. The approved hardware modules are listed in chapter 2.1.

5.1.3. Checking of operating mode (RAM, FLASH or EPROM operation), Safety Integrity Level, version number for the safety related software components defined in chapter 2.12 "Release identification" and important system times such as test cycle time, second fault occurrence time, minimum and maximum program running time shall be performed by means of the "View FSC System and process status" program on the FSC Navigator (option parameters).

In general, correct parameterisation of system characteristics affecting safety should be checked for all safety-related applications (e.g. with the aid of the FSC diagnostic system and fault simulation).

5.1.4. The safety system response to faults and response times shall be taken into consideration and checked as detailed in chapter 4, “Results“, of this report.

5.1.5. Safety-related responses to faults which only result in an alarm are only permissible in the case of operation with permanent supervision.

5.1.6. Except for fire detection and alarm applications, the closed circuit principle shall be applied to all external electrical safety circuits connected to the system. This means that for both digital and analog signals, the safe condition is defined as the “zero condition”.

5.1.7. Non-fail-safe but non-interacting modules may be used for processing non-safety-related signals but not for processing safety-related functions.

5.1.8. Planning should include measures for provision of adequate overvoltage protection for the complete system.

5.1.9. The conditions of use specified in the FSC Safety Manual shall be observed. The guidelines, operating conditions and the instructions for commissioning, described in the instruction manuals, have to be followed.

5.1.10. Administrative measures shall be implemented by the operator in order to ensure that the buffer batteries for preventing data loss from the volatile memory are checked and replaced at regular intervals (see FSC Operation and Maintenance Manual).

5.1.11. The external supply of the output modules is only allowed with power supplies that fulfill IEC 61010 or IEC 60950.

5.2 Planning; Product-Related Conditions

5.2.1. In the case of the redundant system "redundant CP - redundant I/O", the total output load shall not exceed the specified output load of a single output module because in the event of a fault, the output modules are no longer redundant.

5.2.2. When using the 4-channel digital output module FTA-T-08, the contact position of the relays shall be monitored via safety-related input modules of the FSC Fail-Safe-Controller. In applications for SIL 3, two channels of the FTA-T-08 relay output module for each safety relevant output shall be used with the relay contacts in series.

Because of the different requirements for relays in application standards, it might be necessary to check the suitability of the relay (type of design, mechanical/electrical live etc.) for the particular application.

5.2.3. The output signal of the undervoltage alarm circuit P366 of M24-12 and M24-20 shall only be processed by a safety-related input module of the FSC Fail-Safe Controller.

5.2.4. In an UCN communication link at least two grounded "UCN taps" shall be used, according to the installation guide.

5.2.5. If the FSC Fail-Safe Controller is mounted in a cabinet separate from the ABB Automation Contronic E/S control system cabinet then the PBUS connection shall be via an optical link.

5.2.6. The output-voltage of the FTA-T-15 has to be checked by the application program via the module 10105/2/1.

5.2.7. The relay on the FTA-T-19 may not be used for safety-related functions.

5.3 Programming; Non-Product-Related Conditions

5.3.1. The printed function block diagrams shall be compared with the previously prepared function block diagrams.

5.4 Programming; Product-Related Conditions

5.4.1. The response of the system to faults on the hardware modules shall be specified by the application program in accordance with the particular safety-related circumstances of the system. The default configured response is an automatic safe action.

5.4.2. In the event of a sub-process shutdown on the system "redundant CP - redundant I/O"; i.e. a fault on the fail safe output modules, a timer shall instigate reconfiguration of the system after expiry of a second-fault occurrence time defined according to the demands of the individual application.

5.4.3. The use of safety-related Counter Functionality is suitable for processes in which the counter signal is changing within the second-fault occurrence time. The planning and programming of the counter functionality shall comply with the manual „Fail Safe Control, Technical Note, FSC Safety-Related Counter Functionality“.

5.5 Communication; Product-Related Conditions

5.5.1. Safety-related communication (FSC protocol) is only permitted within the Fail-Safe Controller System Family.

5.5.2. Safety-related communication (SafeNet protocol) is only permitted within the Fail-Safe Controller System Family (>=R801.1) and Safety Manager Product Family (>=R161.1). Compatibility between Fail-Safe Controller System Family and Safety Manager shall comply with the current Release Letter of FSC Version 80x.x.

5.5.3. For safety-related communication, the safe condition for transmission data shall be “zero”.

5.5.4. To establish safety related communication via public telecommunication services the modified RKE 3964R protocol may be used also but extra measures for data integrity must be programmed via FSC logic functions and must fulfill the requirements according SIL 2 (see also chapter 2.6.2). This is realised with the following modules which must be used for the safety relevant communication:
- MASTER_1, FIRST ISSUE, 07-26-1998
- SLAVE_62, FIRST ISSUE, 07-26-1998

5.6 Special Operating Modes; Non-Product-Related Conditions

5.6.1. Modifications during active operation (on-line modifications) are permissible only after consultation with the inspection and testing centre responsible for approval of the application.

5.6.2. Responsibility for monitoring the process while on-line modifications are being carried out is that of the person responsible for the on-line modifications. All system messages received while carrying out on-line modifications are to be treated with the utmost caution.

5.6.3. On-line modifications presuppose applications programs that have been subjected to particularly thorough testing beforehand, e.g. at simulators. In the case of such thoroughly tested application programs, as part of the on-line modification process, at least all functions reported by the function “Verify FSC Application Software“ of the FSC Navigator as having been modified shall be subjected to a full function test.

The operator shall compare all changes reported during the process of on-line modification with the modifications he/she has made and investigate any discrepancies (i.e. apparently unmodified application sheet reported as having been modified) and document the causes.

5.6.4. The use of "maintenance override" shall comply with the current version of the document "Maintenance Override" published by TÜV SÜD and TÜV Rheinland.

5.6.5. Forcing of signals shall only be possible allowed under the supervision of a key-operated switch and is the responsibility of the operator alone. Checking of which signals may be forced can be performed with the aid of a printout of the FSC variables.

5.6.6. If the user program is stored in RAM or Flash, inadvertent alteration of the user program shall be prevented by means of password protection.

5.7 Special Operating Modes; Product-Related Conditions

None

5.8 Fire Detection and Alarm Installations; Non-Product-Related Conditions

5.8.1. The energy shall be provided by an un-interruptable power supply (UPS). The bridge-over duration and the alarm duration will be determined by the application and by the effective national requirements.

5.8.2. The power supply of an alarm installation following DIN VDE 0833 shall be independent of the supply of any other installation.

5.8.3. The installation shall provide for an alarm horn of at least 60 dB and for a nuisance alarm of at least 50 dB.

6 Certificate Number

This report specifies technical details and implementation conditions required for the application of FSC Version 80x.x to the certificate:

Z10 16 11 20160 011

Munich, 2018-11-14

TÜV SÜD Rail GmbH
Rail Automation

Digital
unterschrieben von
Johannes Blum
Datum: 2018.11.16
12:46:04 +01'00'

J. Blum
(Technical Certifier)