

Report to the Certificate

U 01 05 20160 006

FSC Fail-Safe Controller System Family
Version 535.x

Manufacturer:

Honeywell Safety Management Systems B.V.
Rietveldenweg 32
NL-5222 AR 's-Hertogenbosch
Netherlands

Report No.: SH99495C
Revision 5.35 of 22. July 2003

Testing and Certification Center
TÜV AUTOMOTIVE GMBH
Automation, Software and Electronics - IQSE
Ridlerstraße 65
80339 München

This Report to the Certificate may not be duplicated **other than in its entirety** without the prior written consent of the TÜV AUTOMOTIVE GMBH, IQSE.

Report to the Certificate on the FSC Fail-Safe Controller System Family

Contents	Page
1 Subject of Certification.....	4
2 Description of the System.....	5
2.1 Extent of Certified System	5
2.1.1 Safety-Related Modules.....	5
2.1.2 Tested, non-interacting Modules.....	7
2.1.3 Mechanical and electrical parts.....	8
2.1.4 Safety-Related Software Functions.....	8
2.1.5 Tested, non-interacting Software Functions.....	8
2.2 Certified System Configurations	8
2.3 Reconfiguration	16
2.4 Mixed Configurations	17
2.5 Possible Wiring Alternatives for Requirements Categories AK1 to AK6.....	17
2.5.1 Inputs.....	17
2.5.2 Outputs.....	18
2.6 Communication.....	18
2.6.1 Safety-Related Communication (FSC Protocol)	19
2.6.2 Safety-Related Communication (RKE 3964R Protocol)	19
2.6.3 Non-Safety-Related Communication.....	20
2.6.4 Access to the FSC safety system by the FSC Navigator	20
2.7 Compiling the Application Program.....	21
2.8 FSC safety checker	21
2.9 Modifying the Application Program during Operation.....	21
2.10 Fire and Gas applications	21
2.11 Release identification	22
3 Basis of Certification.....	22
4 Basis of Tests.....	24

4.1	Functional Safety.....	24
4.2	Application-Related Requirements	24
4.3	Basic Safety	24
4.4	Basic Safety Tests conducted by Underwriters Laboratories	26
4.5	Electromagnetic Compatibility.....	26
4.6	Product-Related Quality Assurance and Certification	26
5	Overall Results	27
5.1	Response Times.....	27
5.2	Response of System to Faults.....	27
5.3	Modifications to the Application Program During Operation.....	28
6	Certificate Number.....	28
7	Conditions of Certification.....	29
7.1	Planning; Non-Product-Related Conditions	29
7.2	Planning; Product-Related Conditions	30
7.3	Programming; Non-Product-Related Conditions	30
7.4	Programming; Product-Related Conditions.....	31
7.5	Communication; Product-Related Conditions	31
7.6	Special Operating Modes; Non-Product-Related Conditions.....	31
7.7	Special Operating Modes; Product-Related Conditions	32
7.8	Fire Detection and Alarm Installations; Non-Product-Related Conditions	32

1 Subject of Certification

The present Certification Report is a compilation of the most important user-related findings of the type approval tests on the FSC Fail-Safe Controller System Family, version 535.x for the system configurations:

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

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

in conjunction with its operating system.

The Certification Report SH99495C revision 5.34 of 10. July 2003 is replaced by this Certification Report.

The FSC Fail-Safe Controller System Family 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).

2 Description of the System

2.1 Extent of Certified System

The certified system encompasses the hardware modules listed below as well as the corresponding operating system with the specified software functions.

2.1.1 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
10001/1/1	Vertical bus driver
10001/R/1	Vertical bus driver (relay)
10002/1/2	Central processing unit (EPROM memory)
10012/1/2	Central processing unit (FLASH memory)
10020/1/1	Quad processor module -QPM- (Flash memory)
10004/./.	Communication module (EPROM memory)
10014/./.	Communication module (EPROM, FLASH memory)
10005/1/1	Watchdog module
10007/1/1	Single bus driver
10024/./.	Enhanced Communication module (EPROM, FLASH memory)
10100/1/1 and 10100/2/1	Horizontal bus driver
10101/1/1 and 10101/2/1	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	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	4 channel analog input module for redundant systems and non-redundant systems
10105/2/1	16 channel high-density analog input module
10106/2/1	16 channel line-monitored digital input module with earth fault monitor
10201/1/1 and 10201/2/1	8 channel digital output module 24 VDC
10205/1/1 and 10205/2/1	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	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	4 channel digital output module 48 VDC
10214/1/2	3 channel digital output module 220 VDC
10215/1/1 and 10215/2/1	4 channel digital output module 24 VDC
10216/1/1 and 10216/2/1	4 channel digital output module 24 VDC with loop-monitoring
10216/2/3	4 channel digital output module 48 VDC with loop-monitoring

Module Number	Module Description
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)
FTA-T-05	Fail-safe digital output FTA (24 VDC, 12 channels)
FTA-T-06	115 / 230 VAC digital input FTA Fail-Safe (potential free input contacts)
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
FTA-T-15	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 AK5/6 applications
FTA-T-18	Fail-safe Gas / Flame detector input
FTA-T-19	Fail-safe Fire detector input FTA with line monitoring
FTA-T-21	Fail-safe digital input FTA (24/48/60 VDC, NAMUR, 16 channels)
FTA-T-23	16 channel digital input FTA 24 VDC (current-limited),
FTA-T-29	Fail safe active/passive digital input FTA 115V VAC/DC, 16 channels
FTA-T-35	FS current limited 24Vdc 8 channel DO FTA
FTA-T-36	FS current limited 24Vdc 4 channel DO FTA
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	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

2.1.2 Tested, non-interacting Modules

The certified version of the operating system supports the following tested, non-safety-related but 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/.	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	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	10 channel relay output module 24 VDC
10209/1/1 and 10209/2/1	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)

2.1.3 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 (FSC) System Hardware Manual".

2.1.4 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 analog input and output signals
- Processing timer and counter data
- Processing the user program in function block mode
- Analog value processing
- Calculation functions including floating point functions
- User-defined function blocks
- Equation blocks
- Communication, see Section 2.6 “
- Safety-Related Communication (FSC Protocol)“ and Section 2.6.2 “Safety-Related Communication (RKE 3964R Protocol)“

2.1.5 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 Section 2.6.3 "Non-Safety-Related Communication"
- Real Time Clock (RTC, DCF)

2.2 Certified System Configurations

For safety-related operation of the FSC Fail-Safe Controller, a configuration in accordance with the Requirements Category as per the following table shall be selected.

Quad processor module 10020/1/1 (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)
Requirements Category	AK 1 – 6	AK 1 - 6	AK 1 - 6
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 fail-safe 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 recognised 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)
Requirements Category	AK 1 – 6	AK 1 - 6	AK 1 - 6
System response in the event of failure of fail-safe output modules (Note 3)	<p>Depending on the locality of the fault, the system responds as follows:</p> <ul style="list-style-type: none"> 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 	<p>Depending on the locality of the fault, the system responds as follows:</p> <ul style="list-style-type: none"> 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 	<p>Depending on the locality of the fault, the system responds as follows:</p> <ul style="list-style-type: none"> 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 <p>Continued operation for unlimited period of time using intact central part</p>

Note 1: Faults in redundant central parts, which are detected and localised by the 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 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).

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)
Requirements Category	AK 1 - 4	AK 1 - 6	AK 1 - 6
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	<p><u>AK 1-4:</u> Shutdown of defective central part and continued operation for unlimited period using intact central part.</p> <p><u>AK5-6:</u> Possible system response:</p> <ul style="list-style-type: none"> • 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. 	<p><u>AK 1-4:</u> Shutdown of defective central part and continued operation for unlimited period using intact central part.</p> <p><u>AK5-6:</u> Possible system response:</p> <ul style="list-style-type: none"> • 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	single CP - single I/O (1oo1D)	redundant CP - single I/O (1oo2D)	redundant CP - redundant I/O (1oo2D)
Requirements Category	AK 1 - 4	AK 1 - 6	AK 1 - 6
System response in the event of I/O comparison errors (non-localisable)		<p>Input comparison:</p> <p>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.</p> <p>The fault response "System shutdown, process group shutdown or alarm" shall be programmed</p> <p>Or if</p> <ul style="list-style-type: none"> • 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. <p>Output comparison:</p> <p>An output comparison error is indicated by a system flag. The fault response "System shutdown, process group shutdown or alarm" shall be programmed.</p>	<p>Input comparison:</p> <p>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.</p> <p>The fault response "System shutdown, process group shutdown or alarm" shall be programmed</p> <p>Or if</p> <ul style="list-style-type: none"> • 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. <p>Output comparison:</p> <p>An output comparison error is indicated by a system flag. The fault response "System shutdown, process group shutdown or alarm" shall be programmed.</p>

System	single CP - single I/O (1oo1D)	redundant CP - single I/O (1oo2D)	redundant CP - redundant I/O (1oo2D)
Requirements Category	AK 1 - 4	AK 1 - 6	AK 1 - 6
		<u>AK5</u> : IF <ul style="list-style-type: none"> 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>AK6</u> : System shutdown	<u>AK5</u> : IF <ul style="list-style-type: none"> 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>AK6</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: <ul style="list-style-type: none"> Shutdown of output signal or Group shutdown or System shutdown 	Depending on the locality of the fault, the system responds as follows: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> Shutdown of output signal of the channel concerned or Group shutdown of the channel concerned or Shutdown of the affected central part <u>AK 5 - 6</u> : Continued operation for a period of time defined by the manufacturers PFD calculation for a specific system; (Note 4)

System	single CP - single I/O (1oo1D)	redundant CP - single I/O (1oo2D)	redundant CP - redundant I/O (1oo2D)
Requirements Category	AK 1 - 4	AK 1 - 6	AK 1 - 6
	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 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 analog 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 analog inputs, the configured minimum limit is adopted. The fault response "System shutdown, process group shutdown or alarm shall be programmed OR if <ul style="list-style-type: none"> • 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.

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: AK 1 - 5: All faults which are only detected by comparing the internal system statuses of the two central parts and can not be localised result in a system alarm

AK6: For central parts and output failures all faults which are only detected by comparing the internal system statuses of the two central parts and can not 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 Requirements Categories, 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 Requirements Categories upto and including AK6.

2.5 Possible Wiring Alternatives for Requirements Categories AK1 to AK6

2.5.1 Inputs

For AK6 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 AK6 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 chapter "Safety-Related Non-Fail-Safe Redundant Inputs" 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 AK6 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 AK6 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 AK 6)	Yes
FSC protocol for communication (multi-drop and point to point) between FSC systems (up to AK 6)	Yes
Modified RKE3964R protocol for communication (point to point) via public telecommunication services (up to AK 5) 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 Plantscape system	No
Communication via PBUS with the ABB Automation Contronic E/S process control system	No

2.6.1 Safety-Related Communication (FSC 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
- 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 AK5.

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 can not 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 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 Bayern Sachsen e. V. / TÜV Product Service GmbH and TÜV Rheinland.

2.7 Compiling the Application Program

The planning, programming and compiling of the application program is 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 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.

2.9 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 chapter "On-Line Modification" in the FSC Software Manual.

2.10 Fire and Gas applications

The FSC system can be used for Fire & Gas applications. The FSC Safety Manual (PM.MAN.8047) and the special Fire and Gas Application Manual (PM.MAN.8160) describe basic F&G applications that are designed according to the requirements of EN-54 part 2.

A wide range of fire and gas field devices can be connected to the special fail-safe FTA's, FTA-T-18 (analog gas and flame detectors) and FTA-T-19 (conventional fire detectors). The connecting and signal handling details for these supported third party devices are detailed in the Fire and Gas Field Devices Interface Manual (PM.MAN.8163).

2.11 Release identification

This report covers the FSC releases 535.x where x indicates the actual (maintenance) release. For the release 535.x the following safety related software components shall be used:

- Central Processing Units, System software version 53.09
- Communication Modules, System software version (safety related) 50.06
- Verify Application 46.0.0.0
- Safety checker 52.0.0.0

All other software parts (not safety related) must have a version-number equal/greater than 44.1.0.0 (FSC Navigator box) or equal/greater than 10.03 (Monitor System/FSC System/Versions) and can be modified by HSMS without new certification by TÜV AUTOMOTIVE GMBH.

The hardware modules are listed in section 2.1.1 and 2.1.2.

3 Basis of Certification

Certification is based on the following test reports:

Test reports for the certification of version 535.x:

- “Report on the Modification Test of the FSC Fail-Safe Controller System Family“
Version 535.x
Report no. HH80659T Revision 1.0 of 22. July 2003
- “Assessment Report about the conformity according IEC 61508 of the FSC Fail-Safe Controller System Family“
Report no. HH80661T Revision 1.0 of 13. May 2003
- “Prüfbericht des FSC Sicherheitssystems
nach DIN EN 54 Teil 2 und DIN VDE 0833 Teil 1“
Report no. SH95395 Revision 1.0 of 9. October 1995
- Declaration of Programmable Systems Conformity
Underwriters Laboratories Inc.
UL File E168580 and UL File 168320
- Audit Report, Honeywell SMS - SIL / reliability calculations
Version 1.2
Report-no. HS7008C Revision 1.2 of 17. December 1999
- Test Report
Senton EMI/EMC-Testcenter
Report no. 56306-80353 for F101R Safety Manager, 27. April 1998

- Test Report
Senton EMI/EMC-Testcenter
Report no. 56306-80546 for Full download Plantscape and Full download Manager,
09. July 1998
- Test Report
Senton EMI/EMC-Testcenter
Report no. 56306-80826 for Full download Plantscape, 07. October 1998
- Test Report
Senton EMI/EMC-Testcenter
Report no. 56306-90646 for FSC 530, 15. November 1999
- Test Report
Senton EMI/EMC-Testcenter
Report no. 56306-00102 for FSC 530-ECM+EPM, 20. March 2000
- Test Report
Senton EMI/EMC-Testcenter
Report no. 56306-10365 for FSC 600, 22. June 2001

Certification report on the most recently tested version:

- "Certification report
FSC Fail-Safe Controller System Family
Version 534.x"
Report no. SH99495C Revision 5.34 of 10. July 2003

The certification of the system family according to the regulations and standards detailed in Section 4, "Basis of Tests", verifies successful completion of the following test components:

1. Functional Safety
 - 1.1 Failure effects analyses of the hardware modules detailed in Section 2.1, "Extent of Certified System" as well as the complete circuitry.
 - 1.2 Software analysis of the operating system
 - 1.3 Guidance notes on safety in the system manuals
2. Basic / Electrical Safety
3. Susceptibility to Environmental Stress
 - 3.1 Climate and Temperature
 - 3.2 Physical Stress
4. EMC
 - 4.1 Susceptibility to Electromagnetic Effects
 - 4.2 Electromagnetic Emission
5. Product-Related Quality Assurance in Manufacture and Product Development

4 Basis of Tests

Due to the broad range of applications of the FSC Fail-Safe Controller System Family, testing of the categories specified in Section 3, “Basis of Certification”, was based on the following guidelines and standards:

4.1 Functional Safety

DIN V 19250 (1/89, 5/94)	Fundamental aspects to be considered for measurement and control equipment
DIN V VDE 0801 (1/90) and Amendment A1 (10/94)	Principles for computers in safety-related systems / AK 6
IEC 61508 Part 1 to 4:2000	Functional Safety of electrical/electronic/programmable electronic safety-related systems / SIL 3 Part 1: General requirements Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems Part 3: Software requirements Part 4: Definitions and abbreviations
UL 1998 (first edition)	Safety-related software
QSH IQSE (Version 1.1)	IQSE quality manual
ANSI/S84.01 (as applicable)	Application of SIS's for the process industries

4.2 Application-Related Requirements

DIN VDE 0116 (10/89) Clause 8.7	Electrical Equipment of furnaces Safety-related requirements of electronic components
DIN EN 54-2 (01/90)	Components of automatic fire detection systems; control and indicating equipment
DIN VDE 0833-1 (01/89)	Alarm systems for fire, intrusion and hold-up; general requirements

4.3 Basic Safety

Testing Standards		Test Severity
DIN VDE 0160 (05/88), DIN VDE 0160 A1 (04/89)	Electronic equipment to be used in electrical power installations and their assembly into electrical power installations	

Testing Standards		Test Severity
DIN VDE 0110 (01/89)	Insulation co-ordination for equipment within low-voltage systems; fundamental requirements Part 1: Basic Specifications Part 2: Measuring Air Clearances and Creepage	Printed circuits; epoxy glass fibre insulating material class IIIa; contamination level 2; rated voltage 50 V; rated surge voltage 0.5 kV
DIN IEC 68	Basic environmental testing procedures	
DIN IEC 68 Part 2-1	Cold' test	0°C; 16 hours; system in operation; reduced power supply voltage (-15%): U=20.4 VDC or (-10%): U=198 VAC
DIN IEC 68 Part 2-1	Cold' test	-5°C ¹ ; 16 hours; system in operation
DIN IEC 68 Part 2-2	Dry Heat test	up to 60°C ¹ as per manufacturer's specifications; 16 hours; system in operation; increased power supply voltage (+15%): U=27.6 VDC or (+10%): U=242 VAC
DIN IEC 68 Part 2-3	Test Ca: damp heat, steady state	21 days at +40°C, 95% rel. humidity; function test after cooling
DIN IEC 68 Part 2-3	Test Ca: damp heat, steady state	96 hours at +40°C, 95% rel. humidity; system in operation
DIN IEC 68 Part 2-6	Environmental testing - Part 2: Tests - Test Fc: Vibration (sinusoidal)	Excitation: sine-shaped with sliding frequency. Frequency range: 10-150 Hz Loads: 10Hz - 57Hz; 0,075mm 57Hz - 150Hz; 1g Duration:10 cycles (20 sweeps) per axis No. of axes: 3 (x;y;z) Traverse rate: 1 oct/min System in operation
DIN IEC 68 Part 2-27	Environmental testing - Part 2: Tests - Test Ea: shock	Half sinus shock 1 shock per direction (6 in total) Maximum acceleration: 15 g Shock duration: 11 ms System in operation

¹ The temperature monitoring system was de-activated for the purposes of the tests. With the temperature monitoring system active, the system is shut down for safety reasons at approx. 0°C / +60°C as measured on the 10006/./ DBM modules.

4.4 Basic Safety Tests conducted by Underwriters Laboratories

Tests according to the following standards were conducted by Underwriters Laboratories and recognised by TÜV AUTOMOTIVE GMBH.

UL 508 (16th edition)	Industrial control equipment
UL 991 (2nd edition)	Tests for safety-related controls employing solid-state devices
IEC 61131-2 (9/92) sections 3, 4.1-4.10, 4.12, 5, 6	Programmable controllers; Part 2: Equipment requirements and tests

4.5 Electromagnetic Compatibility

Testing Standards		Test Severity
EN 55011 (03/91)	Limits and methods of measurement of radio disturbance characteristics of industrial, scientific and medical (ISM) radio-frequency equipment.	Group 1, Class A
EN 50082-2 (1995)	Electromagnetic compatibility - Generic immunity standard; part 2: Industrial environment	
EN 61131-2, 1994	Programmable controllers	
EN 61000-4-5, 03.1995	Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques - Section 5: Surge immunity test	

4.6 Product-Related Quality Assurance and Certification

DIN ISO 9001 (05/90)	Quality systems; Model for quality assurance in design / development, production, installation and servicing
93/465/EEC	Resolution of the Council of 22 July 1993 as to the Modules to be Used in the Technical Harmonisation Directives for the Various Phases of the Conformity Assessment Procedures and the Rules for the Display and Use of the CE Conformity Mark
QSH IQSE (Version 1.1)	IQSE quality manual
EN 45001 (05/90)	General criteria for the operation of testing laboratories
EN 45011 (05/90)	General criteria for certification bodies operating product certification
IEC 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems

5 Overall Results

The tests performed and the quality assurance measures implemented by the manufacturer have shown that the FSC Fail-Safe Controller System Family in conjunction with its operating system version 535.x complies with the testing criteria specified in Section 4, „Basis of Tests“ subject to the conditions set out in Section 7, „Conditions of Certification“ and observing the structures defined in Section 2, „Description of the System“, and is suitable for safety-related use in systems as per Requirements Categories AK 1 to 6 according to DIN V 19250 / 05/94 in intermittent or continuous operation as well as for operation with or without continuous supervision, Safety Integrity Level 3 according to IEC 61508:2000, Part 1 to 4 and according to ANSI/S84.01 and can be used e.g. in applications as Emergency Shut Down (ESD), Fire & Gas detection and Burner Management Systems.

5.1 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 entitled "FSC-FSC Communication").

5.2 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, "FSC-System Fault Detection and Reaction".

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 entitled "FSC System Fault Detection and Reaction").

5.3 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.

6 Certificate Number

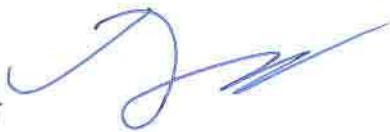
This report adds technical details and implementation conditions required for the application of the FSC Fail-Safe Controller System Family to the certificate:

U 01 05 20160 006

Munich, 22. July 2003

TÜV AUTOMOTIVE GMBH
Automation, Software and Electronics – IQSE

Beer



7 Conditions of Certification

Use of the FSC Fail-Safe Controller System Family 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" of the company Honeywell Safety Management Systems B.V.

In addition, the conditions listed below also apply. 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.

7.1 Planning; Non-Product-Related Conditions

- 7.1.1. Only approved fail-safe hardware modules may be used for safety-related operation. The approved hardware modules are listed in Section 2.1 „Extent of Certified System“.
- 7.1.2. Checking of operating mode (RAM, FLASH or EPROM operation), Requirements Category, version number for the safety related software components defined in Section 2.10 "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).
- 7.1.3. The safety system response to faults and response times shall be taken into consideration and checked as detailed in Section 5, "Overall Results", of this Certification Report.
- 7.1.4. Safety-related responses to faults which only result in an alarm are only permissible in the case of operation with permanent supervision.
- 7.1.5. 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".
- 7.1.6. Non-fail-safe but non-interacting modules may be used for processing non-safety-related signals but not for processing safety-related functions.
- 7.1.7. Planning should include measures for provision of adequate overvoltage protection for the complete system.

- 7.1.8. The conditions of use specified in the FSC Safety Manual shall be observed.
- 7.1.9. 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).
- 7.1.10. The external supply of the output modules is only allowed with power supplies that fulfill IEC 61010 or IEC 60950.

7.2 Planning; Product-Related Conditions

- 7.2.1. 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.
- 7.2.2. 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 requirement class AK 5/6, 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.
- 7.2.3. 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.
- 7.2.4. In an UCN communication link at least two grounded "UCN taps" shall be used, according to the installation guide.
- 7.2.5. 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.
- 7.2.6. The output-voltage of the FTA-T-15 has to be checked by the application program via the module 10105/2/1.
- 7.2.7. The relay on the FTA-T-19 may not be used for safety-related functions

7.3 Programming; Non-Product-Related Conditions

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

7.4 Programming; Product-Related Conditions

- 7.4.1. 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.
- 7.4.2. 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.
- 7.4.3. 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“.

7.5 Communication; Product-Related Conditions

- 7.5.1. Safety-related communication (FSC protocol) is only permitted within the FSC Fail-Safe Controller Product Family.
- 7.5.2. For safety-related communication, the safe condition for transmission data shall be “zero”.
- 7.5.3. 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 AK5 (see also section 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

7.6 Special Operating Modes; Non-Product-Related Conditions

- 7.6.1. Modifications during active operation (on-line modifications) are permissible only after consultation with the inspection and testing centre responsible for approval of the application.
- 7.6.2. 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.
- 7.6.3. 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.

- 7.6.4. The use of "maintenance override" shall comply with the current version of the document "Maintenance Override" published by TÜV Bayern Sachsen e. V. / TÜV Product Service GmbH and TÜV Rheinland.
- 7.6.5. 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.
- 7.6.6. If the user program is stored in RAM or Flash, inadvertent alteration of the user program shall be prevented by means of password protection.

7.7 Special Operating Modes; Product-Related Conditions

None

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

- 7.8.1. 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.
- 7.8.2. The power supply of an alarm installation following DIN VDE 0833 shall be independent of the supply of any other installation.
- 7.8.3. The installation shall provide for an alarm horn of at least 60 dB and for a nuisance alarm of at least 50 dB.