

REPORT

to the

CERTIFICATE

Z2 01 06 44254 001

Fail-Safe Programmable Logic Controller

Advant Controller 31-S

Manufacturer

ABB

STOTZ-KONTAKT GmbH

Eppelheimer Straße 82

69123 Heidelberg

Germany

Report No.: 10032339

Version 2.0 dated 15 May 2001

Certification Body:

TÜV Product Service GmbH

Institute for Quality and Safety in Electronics -IQSE

Ridlerstraße 65

D-80339 München

Germany

This Certification Report may **not** be duplicated **in extract form** without the written consent of the IQSE.

Certification Report on the Fail-Safe Programmable Logic Controller Advant Controller 31-S

Contents

1	SUBJECT OF THE CERTIFICATION	4
2	BASIS OF THE CERTIFICATION	4
3	TEST BASIS	5
3.1	European Directives and national laws and regulations	5
3.2	Application-specific requirements	6
3.3	Functional safety	6
3.4	Electrical safety and susceptibility to environmental interference	6
3.5	Electromagnetic compatibility	7
3.6	Quality management in testing	7
4	SCOPE OF THE CERTIFIED SYSTEM	7
4.1	Safety related I/O modules	7
4.2	Non safety related I/O modules	7
4.3	Programming tools	7
5	SYSTEM SAFETY CONCEPT	8
5.1	Safety related I/O components	8
5.2	Non-safety related I/O components	8
5.3	Central Processing Unit	9
5.4	Non-safety related communication	9
5.5	Non-safety related I/Os of the 07 KT 93-S and 07 KT 94-S	9

5.6	Development environment	9
6	ELECTRICAL SAFETY, SUSCEPTIBILITY TO ENVIRONMENTAL INFLUENCE, EMC	10
6.1	Safety related modules	10
6.2	Non-safety related modules	10
7	PRODUCT-RELATED QUALITY ASSURANCE AND CERTIFICATION	11
8	OVERALL RESULT	11
8.1	European Directives	11
8.2	Functional safety	11
8.2.1	Response times	12
8.2.2	Fault behaviour	12
9	CONDITIONS	12
9.1	Conditions relating to safety related project planning	12
9.2	Conditions applicable to safety related application programming	13
9.3	Conditions regarding maintenance and service	13
9.4	Conditions regarding environmental conditions to be complied with	13
9.5	Conditions for use in road traffic signal installations	14
10	SAFETY CERTIFICATE NUMBER	14
11	ANNEX	15

1 Subject of the certification

The subject of the certification is the fail-safe programmable logic controller Advant Controller 31-S manufactured by ABB STOTZ-KONTAKT GmbH with the modules and software components specified in section 4.

The Advant Controller 31-S system has been developed from the T 200-S system by using the CPU 07 KT 93 in place of the previously used CPU 07 ZE 6x R302. With this version of the certification report the CPU 07 KT 94-S is included in the scope of certification.

2 Basis of the Certification

Certification of a fail-safe programmable logic controller in accordance with the Directives and Standards stated in section 3 "Test basis" requires that the following test segments be carried out successfully:

1. Functional safety
 - 1.1 Failure mode and effect analysis of the hardware modules and the overall interconnection
 - 1.2 Software analysis of the central and I/O modules
 - 1.3 Assessment of the safety characteristics of the development environment
2. Electrical safety
3. Susceptibility to environmental interference
 - 3.1 Climate and temperature
 - 3.2 Mechanical interference
4. EMC
 - 4.1 Electromagnetic immunity
 - 4.2 Electromagnetic emission
5. Product related quality assurance regarding manufacture and product maintenance

The following test reports summarise the procedure for these test segments and the immediate results:

- Certification report 10032339 dated 26 June 2000 to certificate ZZ 00 12 20206 003 of 26 February 2000
- Report to certificate
ABB Procontric T200-S
Report No. AH70595C Revision 2.1 of 3 May 1996
- Test report on type test
ABB PROCONTIC T200-S
Report No. AH70494B, Revision 1.0 dated 13 July 1994
- Report on modification test
ABB Procontic T200-S
- Report No.: AH101895, Revision 1.0 dated 30 October 1995
Report No.: AH101895B, Revision 1.0 dated 24 August 1995
Report No.: AH116196, Revision 1.0 dated 6 December 1996
- Technical report on modification test 970170670, Revision 1.0 dated 21 July 1999
- Technical report on modification test ah010515 dated 15 May 2001

3 Test Basis

The test was conducted on the basis of the following Laws and Directives owing to the application of the Advant Controller 31-S:

3.1 European Directives and national laws and regulations

89/392/EEC ¹	Council Directive on Machinery
89/336/EEC ²	Council Directive on Electromagnetic Compatibility

(Note: The Council Directive 73/23/EEC concerning electrical equipment for use within certain voltage limits does not apply as the equipment is solely supplied from 24VDC SELV or PELV).

¹ TÜV PRODUCT SERVICE GMBH is a notified body according to the Machinery Directive No. 89/392/EEC, notified by publication in the Official Journal of the EC, Identification No. 0123.

² TÜV Product Service GmbH is a competent body according to the Electromagnetic Compatibility Directive No.: 89/336/EEC (BMPT VFG. 91/1992).

The test was conducted on the basis of the following other Standards and technical regulations in addition to and as a more precise basis for the legal requirements and the "Fundamental Health and Safety Requirements" specified in the Directives.

3.2 Application-specific requirements

DIN VDE 0116: 1989 Clause 8.7	Electrical Equipment for Furnaces; 10.89
EN 954-1: 1997	Safety of Machinery: Safety Related Parts of Control Systems; Category 3
EN 60204-1: 1998	Safety of Machinery– Electrical Equipment of Machines, Part 1
DIN EN 298: 1993 Clause 8, 9, 10	Automatic Gas Burner Control Systems for Gas Burners and Gas Burning Appliances with and without Fans
NE31: 1993	Plant Safety with Process Control and Instrumentation, Class AI
DIN VDE 0832: 1990	Road Traffic Signal Systems
NFPA 8502	Furnace Explosions/Implosions in Multiple Burner Boilers, chapter 4.3
NFPA 8501	Single Boiler Operation, chapter 4.5

3.3 Functional safety

DIN V 19250: 1994	Basic Safety Evaluations of Process Measurement and Control Protection Devices, Requirements Class 4
DIN V VDE 0801: 1990 and A1: 1994	Principles for computers in safety-related systems

3.4 Electrical safety and susceptibility to environmental interference

EN 61131-2:1994 /A11:1998 IEC 1131-2: 1992	Programmable controllers - Equipment requirements and tests
DIN EN 50178:1998	Electronic equipment for use in power installations
DIN VDE 0832: 1990	Road Traffic Signal Systems
DIN VDE 0110-1: 1997	Insulation co-ordination for electrical equipment within low-voltage systems Principles, requirements and tests

3.5 Electromagnetic compatibility

EN 61131-2: 1994 /A11:1998	Programmable Controllers - Equipment Requirements and Tests
EN 50082-2: 1996	Electromagnetic Compatibility (EMC) - Generic Standards - Immunity for Industrial Environments
EN 50081-2: 1994	Electromagnetic Compatibility (EMC) - Generic emission standards - Residential, commercial and light industry

3.6 Quality management in testing

QSH	TÜV Product Service GmbH Quality Assurance Handbook
QSH IQSE (Version 1.4)	IQSE Quality Assurance Handbook

4 Scope of the certified system

The certified system comprises the hardware modules, I/O modules and the software components as listed in the annex.

The presently valid revisions of the products are to be taken from the list of certified products which is held jointly by the manufacturer and the testing body.

4.1 Safety related I/O modules

The list of the safety-related modules for follow-up of the revisions is to be taken from the annex.

4.2 Non safety related I/O modules

For the non safety-related I/O components the properties as described in section 5.2 apply.

4.3 Programming tools

For the production of safety-related applications the tools 07PC331, 907PC338 and 907PC339 shall be used as required by the Safety Manual.

5 System Safety Concept

The existing system Advant Controller CS 31-S has been supplemented with the CPU 07 KT 94-S. The CPU 07 KT 94-S can be used as an alternative to the CPU 07 KT 93-S. If the safety-related I/O modules are used together with these CPUs, this produces the Advant Controller 31-S system.

The safety-related I/O modules have a two-channel 1oo2D-structure and, as decentralised modules, communicate using a safety protocol via the CS31 Bus (AC31 Safety Fieldbus) with the central unit.

As the safety concept relies solely on the safety-related data protocol also media such as e.g. optical fibre, radio link can be applied for transmission instead of 2-wire line.

The user program of the central unit is subdivided into program modules for safety related functions and program modules for non-safety related functions. Only safety related logic elements (S-VE) safeguarded by high-effective software measures are used in the program module for safety related functions.

5.1 Safety related I/O components

Safety related modules are used to perform fail-safe input/outputs (digital and analogue). They have an internal two-channel structure and achieve the safety related response by:

- comparison test between the two channels
- supplementary self-tests (power-on and background test) and
- plausibility tests (assertions).

Safety related input/output modules send respectively receive messages via the CS31 bus in secure data format. Safety related communication between the central unit and the fail-safe I/O components is performed cyclically and is time-monitored.

5.2 Non-safety related I/O components

Interference freeness of the not safety related I/O modules for the CS31 bus is covered by a multi-stage procedure.

Component failures on a standard module do not influence the technical safety behaviour of the overall system owing to fail-safe CS31 bus protocol or failure effects are detected by the self-tests implemented on the central units.

Electrical safety and compliance with the EMC requirements are guaranteed by quality assurance methods of ABB STOTZ-KONTAKT GmbH in Development and Quality Assurance. ABB STOTZ-KONTAKT GmbH maintains a certified and monitored Quality Management System according to ISO 9001.

5.3 Central Processing Unit

The central unit has been supplemented with safety related function units in order to support the safety applications and has been renamed to the new type designation 07 KT 94-S re. 07 KT 93-S. The extensions are implemented purely by software and cover:

- Extension of the development software for separate acquisition of safety related program modules in the user program
- Configuration of the safety related system functions within the safety related program modules
- Presetting of exclusive use of safety related logic elements (S-VE) with high safety standard (diversity) within the safety related program modules
- Introduction of supplementary self-tests as initialisation and background tests.

Central units 07 KT 93-S and 07 KT 94-S feature equivalent functionalities:

- The firmware of the central units have been supplemented with the safety logic elements adopted from the T200-S.
- As on the T200-S, the S-VE elements are subjected to a program flow monitoring. The safety related part of the program is thus monitored during the runtime.
- The S-VE elements perform the safety related function in diversitary manner. The operations are also safeguarded by means of supplementary self-tests.
- Supplementary self-tests are run in the background.

5.4 Non-safety related communication

For communication with the programming system, central units feature non-safety related communication interfaces. The interfaces are interference free and may be used for programming and commissioning.

In addition, non-safety related communication is supported by interference free interface modules. The data received and sent may be used only for non-safety related processing.

5.5 Non-safety related I/Os of the 07 KT 93-S and 07 KT 94-S

The central units feature digital inputs/outputs located on the unit itself. These I/Os may not be used for safety-related tasks. Only decentralized safety-related I/O-devices are permitted to perform safety-related tying of the I/Os.

5.6 Development environment

Programming environment 907 PC331 with the 907 PC338 extension is used for the AC31-S system in together with the central unit 07 KT 93-S. Programming environment 907 PC331

with the 907 PC339 extension is used for the AC31-S system in connection with the central unit 07 KT 94-S.

Development of the fail-safe user program module is based in both environments on a default project preconfigured with the basic safety related components.

Only the safety related logic elements listed in the Annex shall be used for development of safety- related applications.

None of the two programming environments feature a special, fail-safe structure or special measures to avoid or to control failures.

Consequently, a complete functional test of the application as stipulated in the Safety Manual shall always be conducted if a new program is written or if programs are modified.

For modifications of the non-safety related program part verification shall be produced that the modifications do not have effects on the safety part.

6 Electrical safety, susceptibility to environmental influence, EMC

The practical tests were conducted by the manufacturer within the framework of his quality assurance measures. The procedure and the test results have been audited by TÜV Product Service IQSE.

6.1 Safety related modules

The safety related I/O modules (see revision list in the Annex) comply with the requirements of the following test segments:

- Electrical safety according to IEC 61131-2
- Electromagnetic interference immunity according to IEC 61131-2 and EN 50082-2
- Radiated electromagnetic emission according to EN 55011
- Susceptibility to environmental influence according to IEC 61131-2 and DIN IEC 68

The applied standards are shown under point 3.

6.2 Non-safety related modules

The non-safety related modules comply with the requirements of the following test segments pursuant to the targets and tests for quality assurance of Messrs. ABB STOTZ-KONTAKT GmbH:

- Electrical safety according to IEC 61131-2
- Electromagnetic susceptibility pursuant to IEC 61131-2 and EN 50082-2
- Susceptibility to environmental influences pursuant to IEC 61131-2

7 Product-related quality assurance and certification

The European procedures for conformity verification (93/465/EEC „Council Directive of 22 July 1993 concerning the modules for the various phases of the conformity assessment procedures and the rules for the affixing and use of the CE conformity marking, which are intended to be used in the technical harmonisation directives“) attach similar importance both to the prototype test and to quality assurance on the part of the manufacturer in production and product maintenance. Messrs. ABB STOTZ-KONTAKT GmbH meet these requirements by a certified and monitored Quality Management System to DIN ISO 9001.

In addition, the certification body of TÜV Product Service GmbH IQSE will conduct a procedure, matched to the assessed product, for surveillance of the uniformity of product quality considering product modifications and their identification (follow-up service) as a part of the certification process.

8 Overall result

8.1 European Directives

The tests conducted voluntarily and the quality assurance measures on the part of the manufacturer have demonstrated that the product type complies with the related safety requirements to the Council Directive No. 89/392/EEC for Machinery, Annex IV; Article 8, Para. 4a, if the user maintains User Manual and the conditions specified in Clause 9.

The essential safety requirements of the Council Directive No. 73/23/EEC on electrical equipment for use within specific voltage limits are complied if considering the User Manuals and the conditions specified in Clause 7. In particular, the requirements of the standard for primary resp. electrical safety, listed in Clause 3.4 Primary Safety and Susceptibility to Environmental Interference, are complied with.

The test reports listed under Clause 3 test basis indicate that the essential protection requirements of Council Directive No. 89/336/EEC on electromagnetic compatibility are complied with, allowing for the User Manuals and the conditions specified in Clause 6. The requirements of the Basic EMC Publications EN 50081-1 and EN 61000-6-2 as well as the applicable product-specific standards were complied with during the test.

8.2 Functional safety

The ABB Advant Controller 31-S controller is suitable for safety related use in applications of requirement categories 1 to 4 according to DIN V 19250, allowing for the application-specific standards specified in Clause 3 "Test basis". The ABB Advant Controller 31-S controllers comply with the requirements of the test basis specified in Clause 3 inasmuch as the conditions according to Clause 9 of this certification report are complied with.

The modules classified as "interference free" can be used in safety related installations for processing non-safety-related signals.

8.2.1 Response times

The maximum response time (worst case) is 200 ms. The fault tolerance time of the process must thus be less than 200 ms.

8.2.2 Fault behaviour

The I/O of the controller is switched off in the case of safety-related faults.

9 Conditions

On the basis of the test results, the following conditions are specified for fail-safe operation of the Advant Controller 31-S programmable logic controller:

9.1 Conditions relating to safety related project planning

Product independent conditions

- The idle-circuit current principle shall be complied with in the case of all safety circuits connected externally to the system. This means, both for digital signals and for analogue signals, that the "de-energised state" is defined as the safe state.
- The defined LOW level of the output modules (current and voltage) must be considered, specific to the application.
- During project planning, it must be ensured that non-safety related functions/components are not able to block safety relevant functions/components.
- The relevant regulations and provisions (e.g. VDE 0116, EN 60204, EN 298) must be complied with for the external cabling.
- If the sensors are supplied from external sources this supply must be monitored.
- The approved modules are specified in the current list of certified modules which is managed and signed jointly by TÜV Product Service and the manufacturer.
- Further requirements are included in the Safety Manual.

Product dependent conditions

- As the control system does not provide any technical measures for the safety of access except for a protection by pass-word the safety of access shall be ensured by administrative means. The cubicle which houses the control system shall be lockable with a key.
- Safety related networking or communication with other systems is not allowed in safety related applications. The various bus couplers shall not be used for transmission of safety-related signals.

- The application-specific requirements concerning special operation modes, e.g. restricted safety mode or grouping/group shut-down shall be considered and coordinated with the expert performing the inspection of the plant installation.
- If the CPU 07 KT 93-S /07 KT 94-S is used, the digital inputs/outputs located on the CPU shall not be used for safety relevant applications.

9.2 Conditions applicable to safety related application programming

Product independent conditions

- Application programming shall be performed in accordance with the provisions in the Safety Manual of the manufacturer.
- Safety related configuration and application programming shall be checked by the expert in accordance with the provisions in the checklist in the Safety Manual.

Product dependent conditions

- The safety related application program shall be subjected to a complete functional test.
- Responsibility for programming the fault reaction lies with the application program.
- The reaction to external faults shall be programmed by the user and lies within his responsibility.

9.3 Conditions regarding maintenance and service

- Overvoltage protection elements shall be inspected in case of demand or fault within the plant maintenance and exchanged if necessary.
- The requirements of the Safety Manual shall be respected.

9.4 Conditions regarding environmental conditions to be complied with

Product dependent conditions

- The specified operating conditions (EMC, mechanical, chemical, climatic influences) shall be complied with.
- The requirements applicable to a special power pack shall be followed for operation of the controller in the extended temperature range of 55...60°C. Otherwise, the temperature ranges defined in the Safety Manual shall apply.

- The safety related AC31 units and all the process voltages shall be powered from power packs which meet the requirements for safety extra-low voltage (SELV).
- To meet the increased EMC requirements of EN 298 the additional EMC measures according to the Safety Manual are to be applied (filter for the supply voltage).

9.5 Conditions for use in road traffic signal installations

Product independent conditions

- The procedures for configuring a road traffic signal installation with the AC31-S programmable logic controller, described in the Safety Manual, shall be followed.

Product dependent conditions

- Only personnel familiar with road traffic signal installations may perform configuration and programming of the AC31-S programmable logic controller if used in road traffic signal installations.
- All components of the PLC system and all process voltages shall be powered from power packs which meet the requirements for overvoltage category III and pollution degree 3 and which supply SELV.
- The standard VDE 0832, on which the application in road traffic installations is based, requires an extended temperature range of -25°C to 75°C (short term 80°C). In this case compliance with the specified operating ambient temperatures of the products shall be maintained by means of heating / cooling of the control cubicle.

10 Safety certificate number

The manufacturer is authorised, subject to the conditions specified in the certificate, to provide the products complying with the tested prototype with the following safety certificate number for verification of safety:

Z2 01 06 44254 001

Munich, 15 May 2001

TÜV PRODUCT SERVICE GMBH
Automation, Software and Electronics, IQSE



Peter Müller
Specialist Certifier

11 Annex

List of the modules / safety-related modules of the “Fail-safe Programmable Logic Controller Advant Controller 31-S”

Module	Identification
CPU modules	GJR5 251 384 R0001 07 KT 93 -S R2171
	07 KT 94 -S R2101
	07 KT 94 -S R2161
binary input modules	07 DI 90-S R 0202
	07 EB 90-S R 0101
binary output modules	07 DO 90-S R 0202
	07 AB 90-S R 0101
analogue input modules	07 AI 90-S R 0202
	07 EA 90-S R 0101

List of software to develop applications

Module	Identification
The safety related logic elements and functional modules within the library of the programming software 907PC338	907 PC 338
The safety related logic elements and functional modules within the library of the programming software 907PC339	907 PC 339

List of the interference free modules / couplers

AC 31 -Modules	Identification
RCOM coupler	07 KP 90
MODBUS coupler	07 KP 93
Master-Field-Bus coupler	07 KP 94
Advant-Field-Bus coupler	07 KP 95
Advant-Field Bus coupler	07 KP 99