A
Pilz Ges.m.b.H.
Modecenterstraße 14
1030 Wien
Austria
Telephone (01) 7 98 62 63-0
Telefax (01) 7 98 62 64
E-Mail: pilz@pilz.at

AUS
Pilz Australia
Industrial Automation LP
9/475 Blackburn Road
Mt. Waverley, Melbourne VIC 3149
Australia
Telephone (03) 95 44 63 00
Telefax (03) 95 44 63 11
E-Mail: safety@pilz.com.au

B
Pilz Belgium
BC Building
L
Industriezone III
Industrielaan 4
9320 Erembodegem
Belgium
Telephone (0 53) 83 66 70
Telefax (0 53) 83 89 58
E-Mail: info@pilz.be

BR
Pilz do Brasil Sistemas Eletrônicos
Industriais Ltda.
Rua Ártico, 123 - Jd. do Mar
09726-300
São Bernardo do Campo - SP
Brazil
Telephone (11) 43 37-12 41
Telefax (11) 43 37-12 42
E-Mail: pilz@pilzbr.com.br

CH
Pilz Industrieelektronik GmbH
Gewerbepark Hintermättli
Postfach 6
5506 Mägenwil
Switzerland
Telephone (0 62) 8 89 79 30
Telefax (0 62) 8 89 79 40
E-Mail: pilz@pilz.ch

D
Headquarters:
Pilz GmbH & Co.
Felix-Wankel-Straße 2
73760 Ostfildern
Germany
Telephone (07 11) 34 09-0
Telefax (07 11) 34 09-1 33
E-Mail: pilz.gmbh@pilz.de

DK
Pilz Skandinavien KS
Ellegaardvej 25 L
6400 Sonderborg
Denmark
Telephone 74 43 63 32
Telefax 74 43 63 42
E-Mail: pilz@pilz.dk

E
Pilz Industrieelektronik S.L.
Edificio Tilma
Avda. Sant Julià 1
08400 Granollers
Spain
Telephone (93) 8 49 74 33
Telefax (93) 8 49 75 44
E-Mail: central@pilzspain.com

F
Pilz France Electronic
1, rue Jacob Mayer
BP 12
67037 Strasbourg Cedex
France
Telephone 03 88 10 40 00
Telefax 03 88 10 80 00
E-Mail: siege@pilz-france.fr

FIN
Pilz Skandinavien KS
Pakilantie 61
00660 Helsinki
Finland
Telephone (09) 27 09 37 00
Telefax (09) 27 09 37 09
E-Mail: pilz.sk@kolumbus.fi

GB
Pilz Automation Technology
Willow House, Medlicott Close
Oakley Hay Business Park
Corby
Northants NN18 9NF
United Kingdom
Telephone (0 15 36) 46 07 66
Telefax (0 15 36) 46 08 66
E-Mail: sales@pilz.co.uk

I
Pilz Italia Srl
Via Meda 2/A
22060 Novedrate (CO)
Italy
Telephone (0 31) 78 95 11
Telefax (0 31) 78 95 55
E-Mail: info@pilz.it

IRL
Pilz Ireland Industrial Automation
Cork Business and Technology Park
Model Farm Road
Cork
Ireland
Telephone (0 21) 4 34 65 35
Telefax (0 21) 4 80 49 94
E-Mail: sales@pilz.ie

J
Pilz Japan Co., Ltd.
Three One Building 701
3-20-5 Shin-Yokohama
Kohoku-ku
Yokohama 222-0033
Japan
Telephone (0 45) 4 71-22 81
Telefax (0 45) 4 71-22 83
E-Mail: pilz@pilz.co.jp

MEX
Pilz de Mexico S. de R.L. de C.V.
Av. San Ignacio 1079
Col. Jardines de San Ignacio
C.P. 45000
Guadalajara, Jalisco
Mexico
Telephone (0 13) 1 22 16 81
Telefax (0 13) 6 47 81 85
E-Mail: pilz_msolis@infosel.net.mx

NL
Pilz Nederland
Postbus 186
4130 ED Vianen
Netherlands
Telephone (03 47) 32 04 77
Telefax (03 47) 32 04 85
E-Mail: info@pilz.nl

P
Pilz Industrieelektronik S.L.
Apartado 2028
2706-909 Colares
Portugal
Telephone (21) 9 28 91 09
Telefax (21) 9 28 91 13
E-Mail: pilz@esoterica.pt

PRC
Pilz China Representative Office
Flat F9/F Huijing Building
134 Siyou Xin Malu
Dongshan District
Guangzhou 510600
China
Telephone (0 20) 87 37 16 18
Telefax (0 20) 87 37 35 55
E-Mail: pilzchn@public.guangzhou.gd.cn

ROK
Pilz Korea Liaison Office
102-1402 Ilsung apt
767, Kyomun-Dong, Kuri-Si
Kyungki-Do 417-715
Korea
Telephone (31) 5 54 12 80
Telefax (31) 5 54 12 80
E-Mail: pilzkr@hotmail.com

S
Pilz Skandinavien KS
Energigatan 10 B
43437 Kungsbacka
Sweden
Telephone (03 00) 1 39 90
Telefax (03 00) 3 07 40
E-Mail: pilz@tripnet.se

SGP
Pilz Industrial Automation Pte Ltd.
61, Kaki Bukit Ave 1, #05-01
Shun Li Industrial Park
Singapore 417943
Singapore
Telephone 8 44 44 40
Telefax 8 44 44 41
E-Mail: sales@pilz.com.sg

USA
Pilz LP
7150 Commerce Boulevard
Canton
Michigan 48187
USA
Telephone (7 34) 3 54-02 72
Telefax (7 34) 3 54-33 55
E-Mail: info@pilzusa.com

... In many countries we are represented by sales partners. Please refer to our Homepage for further details or contact our headquarters.

www www.pilz.com

Internet enquiries and orders: www.pilz.com

Pilz GmbH & Co.
Felix-Wankel-Straße 2, 73760 Ostfildern, Germany
Telephone +49 (7 11) 34 09-0, Telefax +49 (7 11) 34 09-1 33

18 648-10/01 Printed in Germany

Programmable Safety Systems
PSS-Range

PSS-Range
Safety Manual
Item No. 18 648

The spirit of safety.

V, 09/01

Contents

Contents

Introduction

WARNING!
Read this manual before installing the safety controllers of the PSS 3000 series, the PSS SB 3006 series, PSS 3032, PSS 3046, the PSS 3056 series and the PSS 3100 series. It is essential that you comply with all of the safety regulations contained herein.

This manual describes how to safely use the safety controllers of the PSS 3000 series, the PSS SB 3006 series, PSS 3032, PSS 3046, the PSS 3056 series and the PSS 3100 series. It helps you with respect to the planning/configuration, installation, commissioning, decommissioning and with possible problems.
After an introduction in the controller's safety philosophy, we explain the measures required to safely design a process in which the controller is used.

The process configuration is categorised into stages and the associated safety requirements are described in chapter 3 "Configuration of a process". Chapter 4, "Realisation of the application" explains the installation and commissioning procedure. Chapter 5 "Modification, maintenance and decommissioning" must be reviewed before attempting to modify a process.

Chapter 6, "Dealing with errors" describes possible fault conditions, and the respective measures which should be taken to rectify them. This chapter is predominantly aimed for the service engineers.

Chapter 7, "Remote diagnostics, remote maintenance" describes how to perform the remote diagnostics and remote maintenance and the requirements for this.

Chapter 8, "Checklist" describes the procedure for using the safety system with the help of a checklist.

INFORMATION
This safety manual refers to the modular safety systems of the PSS 3000 series and the PSS 3100 series, and the compact systems of the PSS SB 3006 series, PSS 3032, PSS 3046 and the PSS 3056 series.
For simplicity, the term "safety system" or just "system" will be used in this manual to refer to all these units.

This safety manual, edition V, 09/01 has been TÜV certified.

Introduction

Definition of symbols

Information in this manual that is of particular importance can be identified as follows:

DANGER!

This warning must be heeded! It warns of a **hazardous situation that poses an immediate threat of serious injury and death**, and indicates preventive measures that can be taken.

WARNING!

This warning must be heeded! It warns of a **hazardous situation that could lead to serious injury and death** and indicates preventive measures that can be taken.

CAUTION!

This refers to a hazard that can lead to a less serious or minor injury plus material damage, and also provides information on preventive measures that can be taken.

NOTICE

This describes a situation in which the product or devices in its immediate environment could be damaged. It also provides information on preventive measures that can be taken.

INFORMATION

This gives advice on applications and provides information on special features, as well as highlighting areas within the text that are of particular importance.

Safety applications

Safety philosophy

Areas of application

The programmable safety systems of the PSS-Range are suitable for application in safety electrical circuits of machines and other installations. A few examples are listed below:

- Presses
- Transfer lines
- Tank installations
- Emergency OFF-switches
- Incineration controllers
- Cable cars/vehicle operation
- Platform technology
- Process technology

General safety considerations

Before the implementation of the safety controller, a safety analysis in accordance with the machine guidelines is necessary. The programmable safety system as an individual component is compliant with all safety regulations. It guarantees functional safety e.g. against hardware and software errors. It does not however guarantee the safety of the process as a whole, nor the configuration, nor the application program.
The user is responsible for the safety of the application program.
When programming, please be very thorough and observe all of the norms and regulations. Faulty programming can nullify the safety of the entire process! Define the safety requirements for the installation in its entirety and how it should be realised in technical and organisational terms. Belonging to the technical issues are for instance, the use of the system and the safety compliant implementation of the peripheral components, as well as the configuration and application programming of the controller. Organisational measures are for example, determination of the responsible personnel, the documentation of all working procedures involved with the commissioning and the determination of the responsibilities and access permissions.

Safety applications

The safety requirements concern the function of the installation and the potentially resulting dangers. All possible defective functions and faulty operations.

Safety inspection

The safety system is split into two parts: A fail-safe section and a standard section. Only the fail-safe section may be used for safety relevant tasks.

The fail-safe section of the CPU is structured in a diverse 3 channel arrangement. All input and output signals are processed separately from each channel. Every channel compares the results with both of its neighbours. The input and output signals are only valid when all channels yield identical results.
For the modular safety systems, the modules (e.g. input/output modules) are also categorised into fail-safe modules (yellow) and standard modules (grey). Diverse redundancy for the fail-safe modules guarantees high safety. One exception: Input modules and single pole output modules in the power section are not diversified.

Like for the hardware, the software is also split into a fail-safe section and a standard section. A user program, which was created by the fail-safe section, must be link edited, before the transfer. This procedure recognises various program errors and generates a link protocol with error messages and warnings. The linked program is stored in a file. This is secured against changes and can be transferred to the controller, error free.

The fail-safe and the standard program use separate hardware resources (memory, modules etc.). The standard section is isolated, i.e. it has only read access to the fail-safe resources, like fail-safe inputs and outputs.

The three channel diversified structure of the controller provides a high degree of safety. When configuring and programming, it must be observed that this safety margin is not destroyed by errors and lack of attention. Please observe that the application interface may not be used for safety relevant communication.

Managing a safe application

Safety must be guaranteed during the entire lifetime of an installation or process. The lifetime can be divided into the following phases:

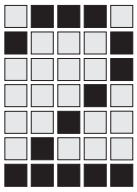
- Planning / configuration
- Installation
- Commissioning
- Operation
- Maintenance
- Decommissioning
- Modification: Only when necessary

A stand-alone safety strategy should be developed and documented for every individual phase, as part of a comprehensive safety plan. This safety plan should contain among other things:

- Technical and organisational measures necessary to ensure safety for each phase
- Responsible parties for the different phases
- Documents which are important for the respective phases
- Measures to ensure the required safety
- Applied technology and measurement procedures
- Analysis and minimisation of possible errors
- Audits to check the functional safety
- Modification procedures
- List of all relevant documents

A significant safety aspect is the responsibility of the personnel. For every phase, qualified personnel must be used. They must have the necessary qualification, the technical expertise and experience. A few examples are given below:

- Configuration
  Process engineer: Requirements: Understanding of the process and the associated safety requirements, thorough familiarisation of the "System manual" of the safety system and the operating instructions of the applied modules.



- Programming
  Programmer: Requirements: Understanding of the configuration plans, knowledge about the safety technology, SPS programming experience and safety-relevant programming, thorough familiarisation of the "System manual" of the safety system.
- Installation
  E.g. Electrician: Requirements: Understandig of the configuration plans, thorough familiarisation of the "Installation guidelines" of the safety system and operating instructions of the modules, knowledge of the accident prevention regulations.
- Commissioning
  Requirements: Knowledge of the process, thorough familiarisation of the "System manual" of the safety system.

Documentation for a safe application

Good documentation is necessary for all safety applications. It should describe every phase (see page 2-3) and the functions of an installation (of a process). A simple, easy-to-follow, accurate and complete description is sufficient for this purpose. Complete means in this case for example, that all functions, signals, events and run-time procedures and associated tests can be followed.
Depending on the extent, the documentation can consist of one or more sections. Each document must be identifiable with a name and a version number.
Further documentation is necessary for the communication between the phases. For instance, the programmer requires information about the necessary configuration functions or the installer requires a wiring diagram from the configurer etc.

Configuration of a process

Define area of application

Before configuration, you must determine

- The exact purpose of the application
- The limits of the application
- The purpose for the use of the safety system

In order to carry out a project, it is necessary to have accurate knowledge about the process.

Determine functions

After defining the area of application, the following questions must be clarified:

- Which safety relevant functions must be fulfilled ?
- Which safety relevant operating conditions can occur ?
- What interfaces and inputs/outputs (safety relevant and non-safety relevant) are necessary ?

Specify the exact definitions of the functions, operating conditions and the applied interface. Use a logic diagram to clarify the functions and operating conditions.

Example: EMERGENCY OFF switch (also see examples in the "Programming guide" of the safety system).

- Function: Switch off the process / installation after pressing the EMERGENCY OFF-button.
- Operating conditions can be defined in a logic diagram by the status of the EMERGENCY OFF-button.
- Define inputs and outputs which are to be connected to the EMERGENCY OFF button, by means of a wiring diagram.

Configuration of a process

Define safety requirements

The first two paragraphs in this chapter describe "what must be done". The following paragraphs describe "how it is done". Firstly define the safety requirements for the controller:

- Define the tasks that the system must perform in order to satisfy the required safety.
  Example: What must the system do in order to monitor the safe operating conditions of the process.
- Determine how the system should react in the case of a fault condition.
  Example: On error, the system must force the process into a safe condition
- Define the input and output signals.
  Example: Number of safety relevant inputs.
- Define the timing requirements of the safety oriented tasks.
  Example: Consideration of the delay times, processing times etc.
  Determination of the process error tolerance (time period for which the process tolerates an error without allowing a dangerous condition arise)
- Define the risk and the required safety norms e.g. DIN V 19250.

We recommend that you have the safety aspects tested and approved.

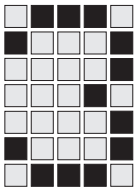
Plan operation and installation

No special measures are necessary to ensure safe operation for the system itself. Should any error occur, e.g. an internal error or short-circuit on a 2 pole output, or external interference like EMC influences, the controller is immediately forced into a safe condition.
Please observe the installation guidelines. They also contain important information concerning electromagnetic compatibility (EMC), the planning, wiring and connection of the inputs and outputs. Further information and installation support can be obtained by calling our hotline (0049 (0)711 / 3409-751).

INFORMATION

If there is an interruption in the power supply for the modules, the system is forced into a safe condition and registers a module error. A restart is only possible via the selector switch "FS" or by switching the CPU's power supply off and on again.

We therefore recommend that you connect the CPU and the peripheral modules to a common switch.



Notes

Realisation of the application

Assign safety requirement classes

After you have defined the required safety and the necessary safety relevant functions, you must assign every safety function a safety requirements class:

- Determine the requirements class with the help of DIN V 19250.
- Ascertain the safety relevant reaction times.

  Check whether there are regulations for the maximum reaction time. The reaction time must be smaller than the maximum value.
- Allocate every safety function the necessary hardware, software and documentation.

Safety in the application program

The application program must be split into two sections - a safety relevant section and a non-safety relevant section. The safety relevant program processes the safety functions and the non-safety relevant program deals with all functions that have no influence on the safety of the process. The inputs to the program are separate: The safety relevant program section are entered with the fail-safe part of the programming device and the non-safety relevant program section is dealt with by the standard part of the programming device. Only the safety relevant part of the program is linked together and checked for errors before transferring to the system. After linking, the executable program is clearly separate from the edited program and thus protected against modification.

Please beware: Errors introduced upon entering the user program and improbable editing errors must be covered by means of comprehensive functional tests.

Safety in the communication procedure

Fail-safe parts and standard parts use separate hardware resources, e.g. peripheral bus, process images, flag etc. The fail-safe part has only access to the communication flags of the standard part. The standard part has only read access to process data of the fail-safe part.

Realisation of the application

WARNING!

- Data from the standard part are **not** secure. They may only be used as a **supplementary** criteria for an action (e.g. start or stop) and **not** inhibit safety actions (e.g. an inactivated stop signal or a continuously activated start signal in the standard part, may not endanger the safety of the process)
- The user interface may only be used for non-safety relevant communication.

Safety requirements for sensors and actuators

achieved by means of: In safety relevant functions, analogue or static binary sensors must recognise a sensor which goes defective whilst indicating a "good condition" status. This is achieved by:

- Using tested sensor samples
- Diversified sensors or actuators with regular checks
- Redundancy sensors or actuators with regular checks
- Self tests or external tests for automatic error detection
- Sensor/actuator construction which excludes physical errors (product certificate with respect to common production)
- Measuring and regularly monitoring diversified process data

Examples for activating actuators and sensors are described in the "installation guidelines".
Some actuators must be controlled via auxiliary contacters. Information about auxiliary contacters can be found in the "installation guidelines". When using auxiliary contacters, additional safety measures must be taken.

Configuration and application programming

The programming can only begin after the modular safety system has been configured, i.e. when the slots have been occupied. Remember which modules are inserted into what slots. With the compact safety system, the layout with inputs and outputs are pre-determined. Allocate the inputs and outputs to the safety functions. Then generate a structured program flow procedure. In this program flow procedure, general errors like voltage supply interruption, short-circuits and peripheral errors must be taken into consideration.

For many applications, a plausibility study is necessary (also see "installation guidelines").
The application program is split into safety relevant and non-safety relevant sections. Only the safety relevant program can carry out the required safety functions. This part is created by the PSS 3000/PSS 3056 programming device. All rules and regulations specified in the "Programming guide" of the safety system, must be complied with when programming.

To avoid errors and to enable simple tests, the application program should be categorised into program blocks. Every program block is responsible for an elementary task. These program blocks of the safety system are called program modules. The following program modules are available for the program structure:

- Organisation modules
  Call up program and function modules, OB101 activates the application program
- Program modules
  Contain elementary functions; When sub-dividing programs, every machine function should reside in a separate program module, e.g. PB10 for feed function, PB20 for configuration etc.; can call up function modules
- Function modules
  Contain concrete individual tasks, e.g. FB10 multiplication, FB20 Adding etc.; can be parameterised.
- Data modules
  Contain data; can be called up by any other module

NOTICE
Always program the safety relevant and non-safety relevant functions in separate modules! Whenever possible, program non-safety relevant functions in the standard part.

The use of modules is a prerequisite for safe programming, as the program becomes:

- Easy to understand and follow
- Logically categorised
- Easy to test

- Modules can be used more than once

After programming, print out the application program and check for errors, e.g. exceeding the permissible parameter range, requests for values outside the parameter range etc. Checking by means of a print out also discovers possible errors of the programming device.

NOTICE

- Zero-voltage data: Data can only be stored in the standard part in a special zero-voltage proof data module.
- Flags and data words must be initialised before application.
- Check the program carefully for programming errors like unwanted overwriting of flags in a data module, number of loops etc.

A further aid to programming are the standard function modules. Standard function modules process standard functions and can be generated by the user or obtained from the company Pilz. A few standard function modules are tested and encoded from certain bodies (e.g. BG, TÜV). These modules cannot be modified and are secure against manipulation. The programs contained therein do not need to be tested further, even for installations that are subject to inspection and monitoring.

Planning the installation

The installation of the system must be carried out in accordance with the "installation guidelines". They contain regulations, notes and measures which should be taken to ensure safe assembly and wiring of the system.

A report should be compiled concerning the installation, in which all activities, reactions and problem solutions are included.

Planning the commissioning process

The commissioning process should be analysed and noted step by step. Compile an accurate description of

- Necessary commissioning activities (actions, responsibilities, solutions to problems)
- Acceptance tests (in accordance with acceptance test specifications)
- Expected reactions (Documentation for test protocols pertaining to acceptance test specifications)

From these points, generate a checklist for the commissioning procedure. By means of the checklist the party responsible for the commissioning checks whether all requirements have been met to ensure safe commissioning, and carries out the commissioning procedure.
The higher the safety requirement class, the higher the qualification of the commissioning personnel. The commissioner must have the following know-how:

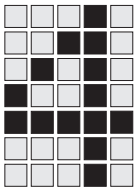
- A good understanding of the safety system system behaviour
- Thorough knowledge about the entire process (whole installation)
- Knowledge about the safety functions and the dangers associated with the process / installation.

All devices which are necessary for the commissioning (e.g. measuring instruments) must be calibrated.

A report should be written, describing the commissioning procedure in which all activities, reactions, problems and solutions as well as the test results of the test specifications should be included.

The system provides some important means which could help to solve any problems arising during the commissioning process:

- Display of variables
  Displays the status of inputs and outputs, flags, times, counts and datawords for a certain point in time.
- Dynamic program display
  Displays the current content of indirect addresses, word operands, battery and auxiliary battery status, status of the contacts and logic results in a selected section of program.



- Error display
  Displays a message about the current error
- Error stack
  Saves all error messages
- Date and CRC checksum of the program in on-line mode.
  The function "Display contents directory of the SPS" displays a status line which contains the date and the CRC checksum saved in the system. If the loaded program is not identical to the stored program, carry out the following procedure:

- Load source program into programming device
- Start program comparison; The linked program of the system is compared with the source program in the programming device. Differences in the CRC checksum and dates are displayed.
- Load the linked program back into the programming device (in the project menu) and compare the linked program with the source program. The differences in the modules are displayed.

Modifications, maintenance, decommissioning

Modifications

A change in the process / installation can become necessary due to:

- Changes in the safety requirements
- Occurrence of systematic errors
- New operation or production requirements
- Modification of the process flow, modification of the installation

Before modifying a safe process (installation), a preparatory analysis must first be carried out in which the following conditions should be determined:

- Effects on the process / installation safety
- Effect on the system safety functions
- Effects on the safety integrity of the system

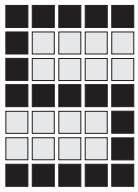
The modification requirements can be summarised in a requirements list. This should contain:

- Known dangers
- Required changes
- Reason for the modifications

The modification should only be made by personnel with the necessary expertise and experience. The same rule also applies here: The higher the safety requirements, the more competent the personnel should be (approval/verification, four-eye principle/documentation of the modifications made).

After making a modification, it must be checked. The entire process flow must also be checked. It must also be ensured that only the required changes can be found at the controller input. The "program comparison" function can be used for this purpose. Special system functions simplify the checking procedure and the error search in on-line operation:

- Program comparison
  Enables the comparison of the program in the system and the current program residing in the programming device



- All commissioning aids (see page 4-5)

INFORMATION
The system must be in a STOP condition before transferring a program. Safety relevant programs can only be transferred in linked form.

Maintenance

No maintenance work is necessary on the system. Please send back any faulty modules to the company Pilz.

Decommissioning

When decommissioning please observe the regulations concerning electronic scrap.

Dealing with errors

The safety system regularly checks the safety relevant parts of the hardware and software. It recognises the following:

- System errors
  e.g. error on self test, power supply failure; after a system error, the controller immediately switches itself into one of the conditions STOP, No FS, Fatal error, depending on the type of error.
- Some important (but not all) program errors in the application program
  e.g. feasibility errors, wrong address range; for certain program errors, the reaction can be programmed in an error organisation module.
- Wiring errors
  e.g. short-circuits and cross connection of 2-pole outputs; for clocked inputs: Short circuits and cross connection of the inputs; for a wiring error, the system reverts immediately to the STOP condition.

If an error occurs, an error message appears on the display and the error is entered into the error stack. The error stack contains the errors from the fail-safe section and from the standard section.

The error stack can hold up to 16 entries. It occupies the datawords DW85 ... DW148 in the system data module DB0. Every error occupies 4 words:

DW	Assignment
84	Pointer to the current error
85	Error class of the first error entered
86	Error number of the first error entered
87	Location of the first error entered
88	Error parameter of the first error entered
89 ... 92	Description of the 2nd error entered
93 ... 96	Description of the 3rd error entered
97 ... 100	Description of the 4th error entered
101 ... 104	Description of the 5th error entered
105 ... 108	Description of the 6th error entered
109 ... 112	Description of the 7th error entered
113 ... 116	Description of the 8th error entered
117 ... 120	Description of the 9th error entered
121 ... 124	Description of the 10th error entered
125 ... 128	Description of the 11th error entered
129 ... 132	Description of the 12th error entered

DW	Assignment
133 ... 136	Description of the 13th error entered
137 ... 140	Description of the 12th error entered
141 ... 144	Description of the 15th error entered
145 ... 148	Description of the 16th error entered

NOTICE
DB0 can only be read in the standard section. No access to the error stack is allowed from the fail-safe part.

As the error stack is organised as a ring buffer, access to the datawords is achieved via the pointer in DW84. The pointer always points to the dataword with the error class of the current error entry.

Meaning of the entries:

- Error class describes the error in coded form. The code corresponds to the displayed message.
- Error location provides information about the point where the error occurred.
- Error number and error parameter contain additional information concerning the error.

If more than 16 errors should occur, the first entry is overwritten.
The error stack contains errors occurring in both fail-safe and standard parts. Errors in the fail-safe part start with the letter "F" Errors in the standard part start with the letter "S". The fail-safe errors have an error class >100H and the standard errors have an error class <100H.

Displaying the errors as clear text messages:

- With the programming device
  Connect the programming device and activate the function "Read error stack". The current error is displayed as text, along with the error parameter and location.
- With the text display
  Connect the text display, e.g. a PX device. If the error has forced the fail-safe part into a STOP condition, the standard part can start a function module, which reads out the error stack and the contents of DB0, DW85 ... DW148, and sends it to the text display.

The relationship between error and operating condition of the system is presented in fig. 1

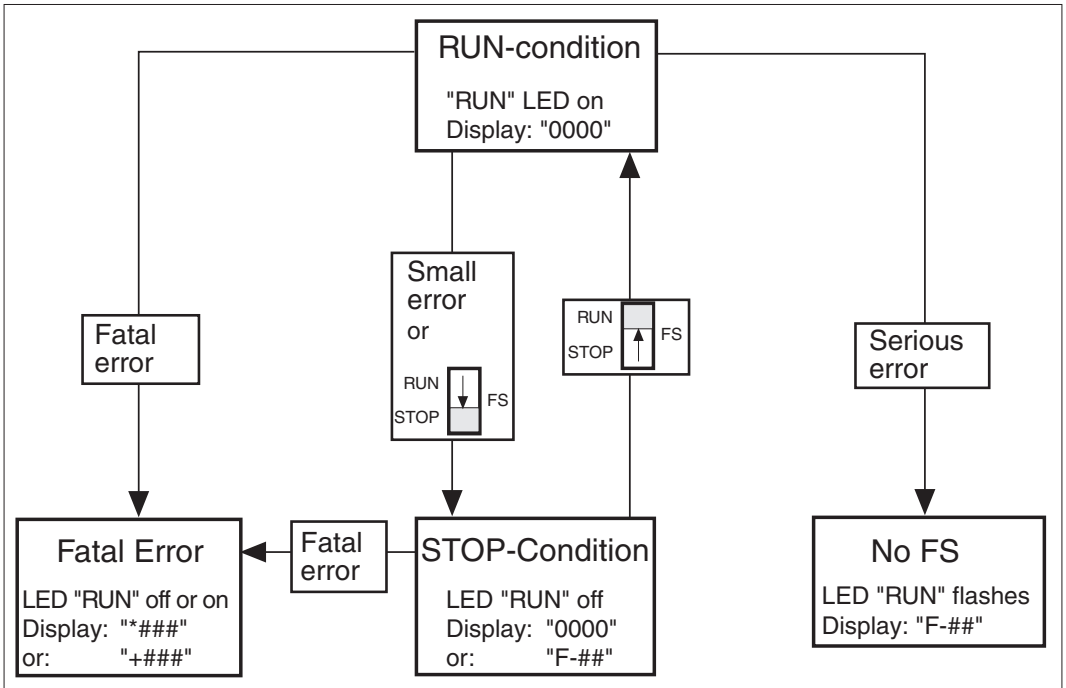
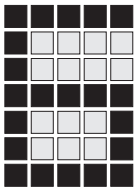


Fig. 1: Change in operating conditions due to error or change of selector switch FS

Error types and error handling:

- Small errors
  The system is forced to a stop condition, the "RUN" LED goes out and the display displays the error message "F-##". The standard application program continues running and all functions of the programming device are available.
  - Possible causes:
    Error in application program or wiring error in power supply (short circuit or crossed connection, also interruptions for DIOZ)
  - Treatment
    - Read out the error stack with the programming device
    - With errors in the application program, the error search can be carried out with the dynamic program display (Restart fail-safe application program!)
    - Rectify error



· Restart the fail-safe application program by activating the FS switch: Set to the "STOP" position and then switch back to "RUN".

- Serious errors
  The system is forced into the "No FS" condition, the "RUN" LED flashes and the display shows the message "F.##". The standard user program continues to run and the functions of the programming device are limited to read access.
  - Possible causes:
    Module failure in digital section or conflicts between the 3 channels e.g. non-identical process images.
  - Treatment:
    · Read out the error stack with the programming device
    · Switch off the system
    · Rectify the fault
    · Switch on the system

- Fatal errors (unexpected system errors which force the controller to turn off).
  The system is forced into the "Fatal Error" condition. The "RUN" LED does not signify anything under this condition and could be either off or on. The error condition is displayed clearly on the display with the message "*###" or "+###". The fail-safe and standard parts are both inoperable, the outputs are switched off. No communication with the programming device is possible.
  - Possible causes:
    System errors, which cannot normally be rectified by the user
  - Treatment
    · Establish conditions under which the error occurs
    · Write down the error indicated on the display
    · Contact the company Pilz

Remote diagnostics, remote maintenance

Remote diagnostics and remote maintenance

A qualified person can identify the reason for malfunctions of a system controlled through PSS (program error, hardware error), even though he is not on-site.
Two persons are involved in remote maintenance: on person performing a remote identification of the reasons for a system's malfunction or modifying the PSS program, and one person operating the system on-site or commissioning it after program changes have been performed.

To perform a remote diagnostics/remote maintenance, connect the programmable safety system that may be on-site with the customer, and the programming device (computer with PSS SW PG system software installed) with the manufacturer of the system.
This connection is via the telephone network. You can use e.g. special modems or "PC-Anywhere".

Remote diagnostics

The remote diagnostics must only be carried out by qualified personnel. This personnel should

- be familiar with the operation of the programming device
- know about programming of programmable safety systems
- have very good knowledge of
  - the system affected
  - the functions of all parts of the system
  - any standards and regulations relevant to this system
  - have the application program on their programmable safety device.

When performing remote diagnostics, the programming device has read-only access to the remote programmable safety system.

Remote diagnostics, remote maintenance

The permitted online functions of the programmable safety device are documented in table 7-1.

Remote diagnostics	
permitted online functions	**not permitted online functions**
• Display PSS error stack • Display variables • Dynamic program display • Display PSS configuration • Display PSS directory • Display PSS hardware • Display error stack of SafetyBUS p subscribers • Display bus diagnostics of SafetyBUS p • Display device ID of SafetyBUS p subscribers • Program comparison	• Transfer program to PSS • Delete program on PSS • Upload program from PSS • Allocating a device address to a SafetyBUS p subscriber • Start PSS • Stop PSS • SafetyBUS p: Start I/O-Group • SafetyBUS p: Stop I/O-Group • Force variables

Tab. 7-1: Online functions in remote diagnostics

CAUTION!
The programming device does not include a special mode for remote diagnostics.The person performing remote diagnostics is responsible for using only the online functions of the programming device that are permitted for remote diagnostics.
We recommend you do not use the system software PSS SW PG for remote diagnostics, but you use the PSS SW QLD service tool. The service tool includes any functions of the system software PSS SW PG with the exception of program generation and program change. The functional range may be restricted, so that only the functions permitted in remote diagnostics may be used

Remote maintenance

The remote maintenance must only be carried out by qualified personnel. The person (PSS programmer) performing a remote identification of the reason for a system's malfunction or modifying the PSS program must have the qualifications mentioned in "remote diagnostics".
The person (system expert) operating the system on-site or commissioning it after program changes have been performed has to

- know well the system affected and be able to assess the functionality of all parts of the system
- know the valid standards and directives and how to apply them
- be able to assess the dangers and effects of the system's malfunctioning and be able to take preventive measures

To be able to perform remote diagnostics, PSS programmers and the system expert need to communicate, e.g. by telephone.

If you perform a remote maintenance, the programming device has read/ write access to the remote programmable safety system. The permitted online functions of the programmeable safety device in remote maintenance are documented in table 7-2.

Remote maintenance	
permitted online functions	**not permitted online functions[1)]**
• Any online functions permitted in remote diagnostics • Transfer program to PSS • Delete program on PSS • Upload program from PSS • Allocating a device address to SafetyBUS p subscribers	• Start PSS • Stop PSS • SafetyBUS p: Start I/O-Group • SafetyBUS p: Stop I/O-Group • Force variables

[1)] these online functions must be performed only by the system expert on-site

Tab. 7-2: Online functions in remote diagnostics

Remote diagnostics, remote maintenance

CAUTION!

- The programming device does not include a special mode for remote maintenance.
  The person performing remote maintanance is solely responsible for using only online functions of the programming device that are permitted for remote maintenance.
- The PSS programmer is responsible for matching the transmitted program to the system and that any functions of the system operate correctly, in particular the safety functions.
- After transferring a program the system expert needs to commission it **on-site.** The system expert must thoroughly test all the system functions and, in particular, the safety functions, and log the test. **The PSS programmer is not permitted to start up the PSS!**
  The system expert is solely responsible for commissioning.
- In remote maintenance, the machine directive must be maintained.

INFORMATION

After changing the program

- a new approval is required
- a new detailed risk analysis has to be carried out
- a new declaration of conformity is required

Sequence of a program change in remote maintenance

To change the application program in remote maintenance, perform the following steps:

- open the original program in the programming device
  The PSS programmer needs to have the original program of the system.
- compare the program in the programming device to the program in the PSS
  A change of program is only permitted when the program in the programming device and the program in the PSS are identical, i.e. the original program is available.
- search for the error by means of remote diagnostics

- rectify errors in the program, link the program again and test the program (with a log)
- compare the new program in the programming device to the program in the PSS
  Only those blocks changed during the program change may differ, otherwise a program change of PSS is not permitted because the original program of the system is not available.
- stop the PSS on-site by the system expert (by RUN-STOP-switch at the PSS)
- delete the program in the PSS
- transfer new program to the PSS
- check whether the correct program has been transferred to the PSS
  To do this, compare the program in the programming device to the program in the PSS or display the directories of both programs and check whether the name, date and CRC checksum are identical.
- commissioning the system by the system expert on-site
  If PSS can be started up without problems and the PSS programmer agrees, the system expert on-site can start the PSS via the RUN-STOP-switch and commission the system.
- test all functions of the system
  The system expert on-site must test all the system functions including those that did not change. In this process, a test log must be created.

Notes

Checklist

Area	Tasks	Att. to
Planning the installation		
	Determine process requirements, (e.g. response times, fault reactions)	
	Define safety requirements	
	Define necessary operating modes	
	Name available operating elements	
	Identify existing accessories	
	Determine regulations which are to be complied with	
	Observe conditions in the PSS certification report (chapter 6)	
	Determine test specifications for commissioning (e.g. checklist)	
	Create wiring plan	
	Insert components into controller	
	Number of inputs	
	Number of single-pole and two-pole outputs	
	Determine switching type for sensors	
	Contact type of the operating elements	
	Type of message display (LEDs, 7-segment display, clear text display, computer interface)	
	Assignment of clocks and inputs (Observe transient times of the inputs)	
	Error exclusion via suitable wiring arrangement possible ?	
	Check sensor with sensor clock	
	Observe wiring of the standard function modules	
	Observe EMC requirements (see installation guidelines)	

Date ..... Signature.....

*1 The certification report is included in the approval folder, order no. 301 230 (PSS-ZUL-DEM).

Checklist

Area	Tasks	Att. to
Programming		
	Choice of the standard functional modules	
	Are there suitable standard function modules	
	Which operating elements must be supported ?	
	Is the element layout suited to the modules ?	
	If no suitable module is available: - Program new module - If necessary remove module	
	Determine program structure	
	Observe safety requirements defined in the planning phase	
	Separation of fail-safe and standard programs	
	Define communication procedure between fail-safe and standard programs	
	Determine functionality of the modules	
	Define flag assignments, timing, counters and datawords	
	Generate fail-safe modules	
	Configure controller	
	Aid: Configurer	
	Enter nominal configuration	
	Enter clock assignment	
	Specify preliminary run times for test purposes, optimise during commissioning	
	If necessary, specify minimum cycle time	
	When clocks are connected to the 3-ms-inputs, Set the correct DI test time	
	Link project	
	Observe warning notes	
	Generate standard modules	
	Observe conditions contained in the PSS certification reports (chapter 6) s. *1, page 8-1.	

Date..... Signature.....

Area	Tasks	Att. to
Installation		
	Observe installation guidelines	
	Comply with wiring plan	
	Observe safety-at-work and accident prevention regulations, VDE and local protection measures	

Date..... Signature.....

Area	Tasks	Att. to
Commissioning		
	Carry out commissioning with the help of a test specification	
	Check all specified safety functions	
	Check all error recognition tools (e.g. redundancy sensors, various switches, simulate short-circuits and open circuits in the wiring	
	Check that all regulations are complied with	
	Document commissioning procedure	
	Observe conditions contained in the PSS certification reports (chapter 6) s. *1, page 8-1.	

Date ..... Signature.....

Area	Tasks	Att. to
Maintenance/modification		
	Before replacing modules, switch off PSS 3000	
	Comply with safety regulations	

Date ..... Signature.....

Checklist

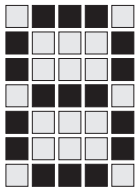
Area	Tasks	Att. to
Remote diagnostics		
	Create telephone connection between programming device and programmable safety device	
	Establish the reason for the system's malfunction with the help of online functions permitted in remote diagnostics	

Date ..... Signature.....

Area	Tasks	Att. to
Remote maintenance		
	Create telephone connection between programming device and programmable safety device	
	Create communication options between PSS programmer and system expert (e.g. telephone)	
	Open original program in the programming device	
	Compare the programs in the programming device and in the PSS device for identity. If they are not the same, remote maintenance is not permitted.	
	Establish the cause for the system's malfunction by online functions permitted in remote diagnostics	
	Deal with error	
	Link program again (note the warning of linking device)	
	Test program (with log)	
	Compare new program to program in the PSS. Programs may differ only in the blocks changed, otherwise remote maintenance is not permitted.	
	Stop PSS by system expert	
	Delete program in the PSS	
	Transfer new program to the PSS.	
	Check whether the correct program was transferred to the PSS.	

	Commissioning of the system by the system expert on-site (see also "Commissioning", page 8-3) Apply for new approval	
	Create new risk analysis	
	Make out a new declaration of conformity	

Date ..... Signature.....



Notes

Appendix

Documentation changes

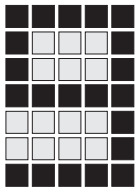
Changes in version V as compared to version IV

old page	new page	Amendment
–	7-xx	New: Chapter 7
7-4	8-4	New: Checklist Remote diagnostics and maintenance

Appendix

Notes

Notes



Notes