PSS 4000 Emergency Stop with PITestop Instruction List

Product
Type: FS_EmergencyStop, FS_OutputFBL
Name: PSS 4000, Blocks, PAS4000, PLC, IL
Manufacturer: Pilz GmbH & Co. KG, Safe Automation

Document
Release Number: 05
Release Date: 20 April 2012

Document Revision History

Release	Date	Changes	Chapter
01	2010-04-08	Creation	all
02	2010-09-28	Adjustments for publication on Pilz website,	only editorial,
03	2011-01-04	Adjustments for publication on Pilz website	only editorial
04	2011-07-27	Revision for Pilz Automation Suite	all
05	2012-04-20	Revision of the Application Note	all

Exclusion of liability

We have taken great care in compiling our application note. It contains information about our company and our products. All statements are made in accordance with the current status of technology and to the best of our know-ledge and belief.
However, we cannot accept liability for the accuracy and entirety of the information provided, except in the case of gross negligence. In particular it should be noted that statements do not have the legal quality of assurances or assured properties.
We are grateful for any feedback on the contents.

April 2012

Support

Technical help round the clock!
Technical support is available from Pilz round the clock.
This service is provided free of charge beyond standard business hours.

Americas
- Brazil
  +55 11 8245-8267
- Mexico
  +52 55 5572 1300
- USA (toll free)
  +1 877-PILZUSA (745-9872)

Asia
- China
  +86 21 62494658-216
- Japan
  +81 45 471-2281
- Korea
  +82 2 2263 9540

Australia
- Australia
  +61 3 95446300

Europe
- Austria
  +43 1 7986263-0
- Belgium, Luxembourg
  +32 9 3217575
- England
  +44 1536 462203
- France
  +33 3 88104000
- Germany
  +49 711 3409-444
- Ireland
  +353 21 4804983
- Italy
  +39 031 789511
- Scandinavia
  +45 74436332
- Spain
  +34 938497433
- Switzerland
  +41 62 88979-30
- The Netherlands
  +31 347 320477
- Turkey
  +90 216 5775552

You can reach our international hotline on:

+49 711 3409-444 or **mailto:support@pilz.com**

Pilz GmbH & Co. KG
Safe Automation
Felix-Wankel-Straße 2
73760 Ostfildern, Germany

Telephone: +49 711 3409-0
Telefax: +49 711 3409-133
E-Mail: pilz.gmbh@pilz.de
Internet: www.pilz.com

Contents

Abbreviations

PAS	**P**ilz **A**utomation **S**uite (software platform)
PSS	Programmable control system (DE: **P**rogrammierbares **S**teuerungs**s**ystem)
PNOZ	Pilz E-STOP Positive-guided (DE: **P**ilz **NO**T-AUS-**Z**wangsgeführt)
POU	**P**rogram **O**rganisation **U**nit
PRG	**Pro**g**r**am
FB	**F**unction **B**lock
FUN	**Fun**ction
IL	**I**nstruction **L**ist

1. Useful documentation

Reading the documentation listed below is necessary for understanding this application note. The availability of the indicated tools and safe handling are also presupposed with the user.

1.1. Documentation from Pilz GmbH & Co. KG

No.	Description	Item No.
1	Pilz international homepage, download section	www.pilz.com
2	Operating Manual PSSu H PLC1 FS SN SD	21939-EN-xx
3	Operating Manual PSSu E F 4DI	21 311-xx
4	Operating Manual PSSu E F DI OZ 2	21 329-xx
5	Operating Manual PSSu E F 4DO 0.5	21 317-xx
6	Operating Manual PSSu E S 4DI	21 340-EN-xx
7	Operating Manual PSSu E S 4DO 0.5	21 346-EN-xx
8	System Description Programmable safety and control system PSS 4000	1001 467-EN-xx
9	Safety Manual Programmable safety and control system PSS 4000	1001 468-EN-xx
10	PAS4000 online help	-
11	Operating instructions PITestop	21 136-xx

1.2. Documentation from other sources of information

No.	Description	Item No.
1		
2		

Note
The present example (PSS 4000 Emergency Stop with PITestop) is also available in the programming languages Structured text and PASmulti.

2. Hardware configuration

2.1. Pilz products

No.	Description	Order number	Version	Number
1	PSSu H PLC1 FS SN SD	312 070	001	1
2	PSSu E F 4DI	312 200	-	1
3	PSSu E F DI OZ 2	312 220	-	1
4	PSSu E F 4DO 0.5	312 210	-	2
5	PSSu E S 4DI	312 400	-	1
6	PSSu E S 4DO 0.5	312 405	-	1
7	PSSu BP 1/8 C	312 601	-	6
8	PITestop Set 1.1	400 410	-	1
9	PAS4000	-	v1.5.0	1

2.2. Hardware configuration

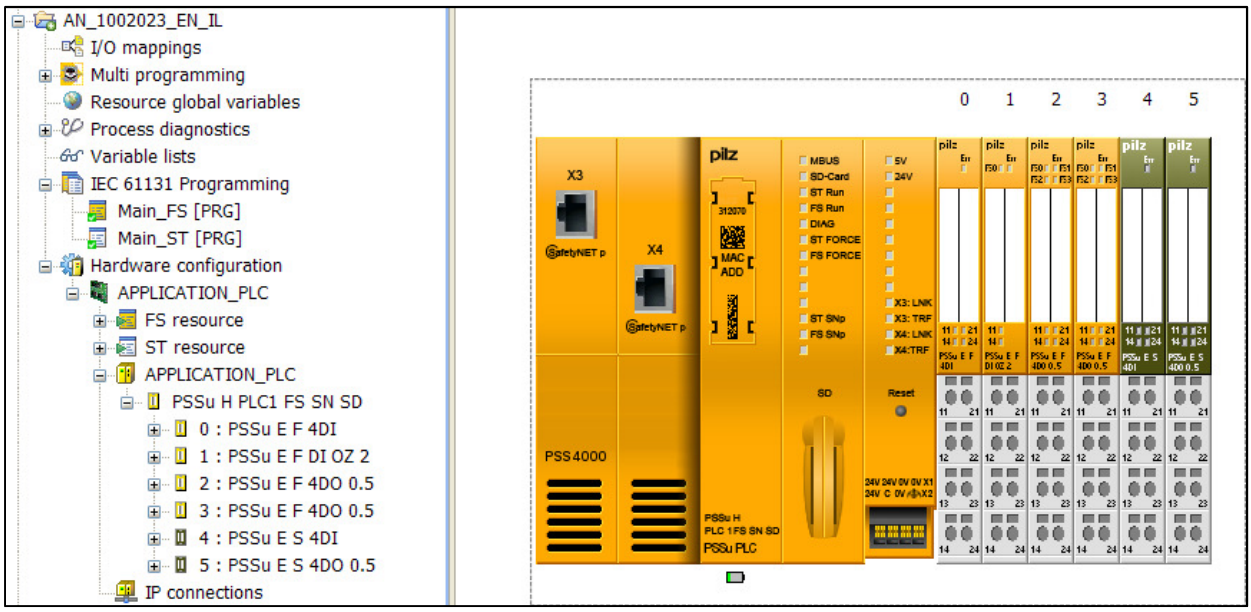


Fig. 1: Hardware configuration

3. Application Task

3.1. Description

The example shows the implementation of an emergency stop application with a PSS 4000 PLC.
The safe control and evaluation of the signals is taken over by two Pilz Function blocks (FS-FB) from the library.

- FS_EmergencyStop
  - CRC EA57

- FS_OutputFBL
  - CRC B3A7

The workflow is divided into the following two main functions:
- Emergency Stop and
- Feedback Loop Monitoring

3.1.1. Emergency stop function

The control system monitors the emergency stop button (S1) via the user program. An instance of the Pilz Function block *“FS_EmergencyStop”* is assigned to them. This FS-FB detects whether the assigned emergency stop button has been operated, as well as detecting incorrect input signals and whether the contact synchronization time has been exceeded, etc.

If the emergency stop button (S1) is operated or an error occurs, the enable output *“Enable”* on the FS-FB will immediately be reset.
The enable output *“Enable”* is also reset when the PSS is stopped and when the PSS is switched on. The signal from the enable output “*Enable*” must be evaluated by the user program and trigger an appropriate reaction.

Based on the diagnostic outputs (*“DiagSwitchError”*, *“DiagInputNotValid”*) it can be determined why “Enable” was reset.
The outputs *“DiagOperated”*, *“DiagReadyForReset”* and *“DiagReadyForTest”* are used as status messages.

A “valid bit” is formed by the system for the respective hardware input to determine whether a process value received from a sensor is valid.
The valid bit is queried in the Function block and indicates whether an error has occurred in the signal transmission between hardware input and processor (such as test clock error, module overheats, etc.).
If the valid bit is FALSE, the process value is invalid and the Pilz function block provides an appropriate diagnostic message. The error signal reset enable.
(For more information, see “Validity of process data” in PAS4000 online help)

The way in which the error is reset will depend on the operating mode set on the FS-FB.
In this application example, parameters for FS-FB have been set in such a way that *"Reset"* (S3) is required in order to reset output parameter *"Enable"* when:

- the PSS is cold started (PSS switched from off to on),
- warm started (PSS transferring from STOP to RUN) or
- when the emergency stop button (S1) is released.

Although the emergency stop functions are configured to reset themselves, a PSS cold start or the release of an emergency stop button that has been operated may not directly enable a machine to start up without further conditions being met.

Input circuit safety assessment

- If a contact on the emergency stop button is overridden, the Pilz function block will detect this as an error at the next operation.
- A short between the input circuits within a multicore cable will be detected as an error by the programmable control system.
- A short between 24 VDC and an input circuit will be detected as an error by the programmable control system.
- The highest category can only be achieved when the contacts on the E-STOP pushbutton are supplied with test pulses and the E-STOP pushbutton has dual-channel wiring.
- If an operator completely (or even maybe partly) is able to access the dangerous area, a risk analysis should clarify whether an additional, separate "manual reset function" is required.

3.1.2. Feedback loop monitoring function

The control system monitors the feedback circuits (NC contacts) of the motor contactors KM1 and KM2 via the user program.
An instance of the Pilz function block *"FS_OutputFBL"* is assigned to them.
The FS-FB drives the contactors as well as monitoring the feedback loop.
A 1-signal at input parameter *"Input"* of the FS-FB sets the outputs that drive the contactors, *"Output1"* and *"Output2"*, to "1"; a 0-signal sets it to "0".
If an error occurs, the outputs *"Output1"* and *"Output2"*, that drive the contactors on FS-FB will immediately be reset. Both outputs are also reset when the PSS is stopped and when the PSS is switched on.

Based on the diagnostic outputs (*"DiagFeedbackLoopError"*, *"DiagFeedbackLoopNotValid"*) it can be determined why the outputs were reset.

A "valid bit" is formed by the system for the respective hardware input to determine whether a process value received from a sensor is valid.
The valid bit is queried in the Function block and indicates whether an error has occurred in the signal transmission between hardware input and processor (such as test clock error, module overheats, etc.).
If the valid bit is FALSE, the process value is invalid and the Pilz function block provides an appropriate diagnostic message. The error signal reset enable.
(For more information, see "Validity of process data" in PAS4000 online help)

If an error occurs, a new activity has to take place at the input "*Input*" of the FS-FB once the error has been rectified, so that the outputs "*Output1*" and "*Output2*" will be set again.

Feedback loop monitoring safety assessment

- A short between 24 VDC and a safety output or a feedback loop input will be detected as an error by the programmable control system. The load can be switched off via the second shutdown route.
- The feedback loop contacts must be installed in a single mounting area (control cabinet).
- To achieve a higher level of safety, 2 actuators must be used.

3.2. Functional safety

3.2.1. Safety-related characteristics in accordance with EN ISO 13849-1

No.	Safety function	PL	Safety-related parts of the control system
1	Machine shut down via E-STOP	PL e	Sensor (PITestop S1) Input (PSSu E F 4DI) Logic (PSSu H PLC1 FS SN) Output (PSSu E F DI OZ 2) Actuator (contactors KM1, KM2)

Prerequisites

No.	Description		Identification
1	Common cause failure (CCF)		Requirements are considered to be met (must be tested on implementation)
2	Mission time		20 years
3	Operating interval (electromechanical components)	Sensor	one operation per week
		Actuator	one operation per week
4	Characteristic data of contactors KM1/KM2	B10d	2,000,000

Please note the further requirements of EN ISO 13849-1, e.g. requirements for avoiding systematic faults.

3.2.2. Safety-related characteristics in accordance with EN 62061

No.	Safety-related control function (SFCF)	Safety Integrity Level	Subsystems
1	Machine shut down via E-STOP	SIL 3	Sensor (PITestop S1) Input (PSSu E F 4DI) Logic (PSSu H PLC1 FS SN) Output (PSSu E F DI OZ 2) Actuator (contactors KM1, KM2)

Prerequisites

No.	Description		Identification
1	Common cause failure (CCF)		ß = 2% (must be tested on implementation)
2	Proof test interval		20 years
3	Operating interval (electromechanical components)	Sensor	one operation per week
		Actuator	one operation per week
4	Characteristic data of contactors KM1/KM2	B10d	2,000,000
		Dangerous failure rate	65%

Please note the further requirements of EN 62061, e.g. requirements for systematic safety integrity.

3.3. PAS-Project

To operate a plant with one or more programmable control systems PSS 4000, a project must be created in PAS4000.
A project consists of the hardware configuration and the user program.

3.3.1. IEC 61131 Programming

When programming in accordance with IEC 61131, the user program is structured by three types of program organisation units (POUs):

- Programs (PRG)
- Function blocks (FB)
- Functions (FUN)

The program forms the higher structural level. Functions and function blocks may be called up within a program.
Function blocks and functions undertake specific individual tasks within the program.

Each POU consists of a declaration part and an instruction part.

The variables and type declarations are made in the declaration part, which is shown in text format, irrespective of the programming language.

The instruction part contains the instructions. The instructions can be formulated in one of the IEC 61131 programming languages.

(For more information about programming with PAS4000, look at PAS4000 online help)

3.3.1.1. IL-Editor

The program for the cyclic process is created in a POU of the type “Program”.
The Pilz function blocks for emergency stop and feedback loop were added from the library.
(Right-click in the declaration part of the POU “Add Library Element”).

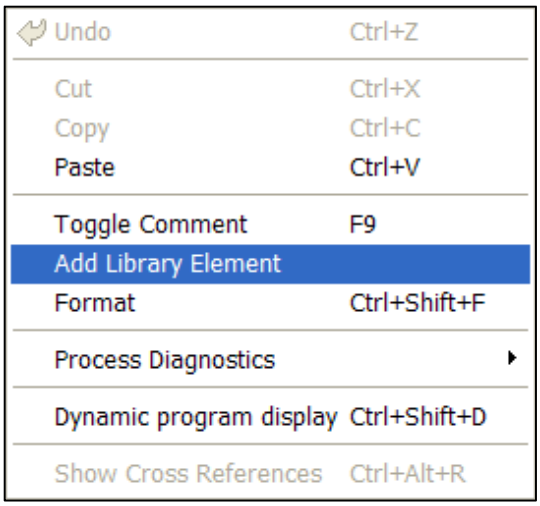


Fig. 2: Add library element

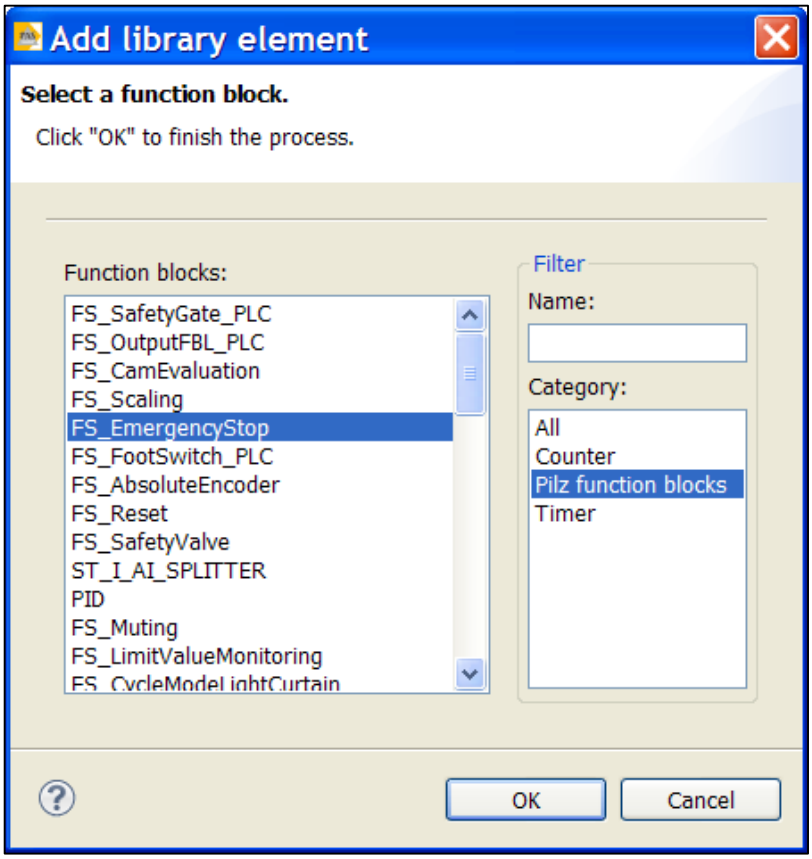


Fig. 3: Selection library element

Failsafe program

Declaration part

```
001 PROGRAM Main_FS
002 VAR
003         // EStop
004         MyEmergencyStop1                                : FS_EmergencyStop;
005         MyEStop1_DiagOperated              AT %Q* : SAFEBOOL;
006         MyEStop1_DiagReadyForReset AT %Q* : SAFEBOOL;
007         MyEStop1_DiagReadyForTest  AT %Q* : SAFEBOOL;
008         MyEStop1_DiagSwitchError   AT %Q* : SAFEBOOL;
009         MyEStop1_DiagInputNotValid AT %Q* : SAFEBOOL;
010         MyEStop1_Enable                                 : SAFEBOOL;
011
012         // FBL
013         MyFeedBackLoop1                                 : FS_OutputFBL;
014         MyFBL1_DiagFblError        AT %Q* : SAFEBOOL;
015         MyFBL1_DiagFblNotValid             AT %Q* : SAFEBOOL;
016 END_VAR
017
018 VAR CONSTANT
019         // Declaration SwitchType 3 (NCNC)
020         MyESTOP1_DOUBLE_CH                        : USINT := USINT#3;
021 END_VAR
```

Instruction part

```
022         // Safety-Block Emergency-Stop1
023         CAL    MyEmergencyStop1(
024         SwitchType := MyESTOP1_DOUBLE_CH,
025         AutoStart := FALSE,
026         AutoReset := FALSE,
027         MonitoredReset := TRUE,
028         StartupTest := FALSE,
029         SimultaneityTime := T#100ms,
030         DelayTime := T#40ms,
031         Enable => MyEStop1_Enable,
032         DiagOperated => MyEStop1_DiagOperated,
033         DiagReadyForReset => MyEStop1_DiagReadyForReset,
034         DiagReadyForTest => MyEStop1_DiagReadyForTest,
035         DiagSwitchError => MyEStop1_DiagSwitchError,
036         DiagInputNotValid => MyEStop1_DiagInputNotValid
037         )
038
039         // Safety-Block monitoring FBL1 and release motor1
040         CAL    MyFeedBackLoop1(
041         Input := MyEStop1_Enable,
042         FeedbackLoopTime := T#200ms,
043         DiagFeedbackLoopError => MyFBL1_DiagFblError,
044         DiagFeedbackLoopNotValid => MyFBL1_DiagFblNotValid
045         )
046
047         END_PROGRAM
```

Standard program

The signals from the start- and stop switch are imported from a standard module PSSu E S 4DI (1A4). These signals belong to the motor control and thus to the standard control functions of the machine.
The program code for the evaluation and processing of these signals is not processed within the FS resource (safety-related part) of the control, but in a ST resource in a separate task as independent application (additional POU of type program).

Declaration part

```
001 PROGRAM Main_ST
002 VAR
003         MyRisingEdge1                          : R_TRIG;
004         Start                          AT %I*  : BOOL;
005         Stop                           AT %I*  : BOOL;
006         Start_FLR                              : BOOL;
007         Set_Motor1                             : BOOL;
008         Reset_Motor1                           : BOOL;
009         Motor1_On                      AT %Q*  : BOOL;
010         Other_Stop_Conditions          AT %I*  : BOOL;
011         FF_Motor1On                            : RS;
012 END_VAR
```

Instruction part - I

```
013         // Rising Edge 1 - Monitoring Start
014         CAL MyRisingEdge1(
015         clk     := Start,
016         q       => Start_FLR
017         )
018
019         // Start Motor1
020         LD      Start_FLR
021 //      AND     Other_Start_Conditions //e.g. Operating Mode
022         ST      Set_Motor1
023
024         // Stop Motor1
025         LDN     Stop
026         ORN     Other_Stop_Conditions //e.g. Enable Signal EStop1
027         ST      Reset_Motor1
028
029         // Flip-Flop Motor1 On
030         CAL FF_Motor1On(
031         set       := Set_Motor1,
032         reset1    := Reset_Motor1,
033         q1        => Motor1_On
034         )
035
036         END_PROGRAM
```

3.3.2. I/O Mapping

In PAS4000, variables can be created and the user program can be programmed without the need of the mapping to the hardware being present at the beginning of the project.
After identification of the used I/O from the variable declaration, the required hardware can be determined.
The I/O mapping editor forms the connecting between the user program and the hardware and coordinates the available I/O and existing PI-variables.

3.3.2.1. I/O Mapping Editor

The PI variables declared in the user-program can be assigned in the I/O mapping editor to the hardware configuration.

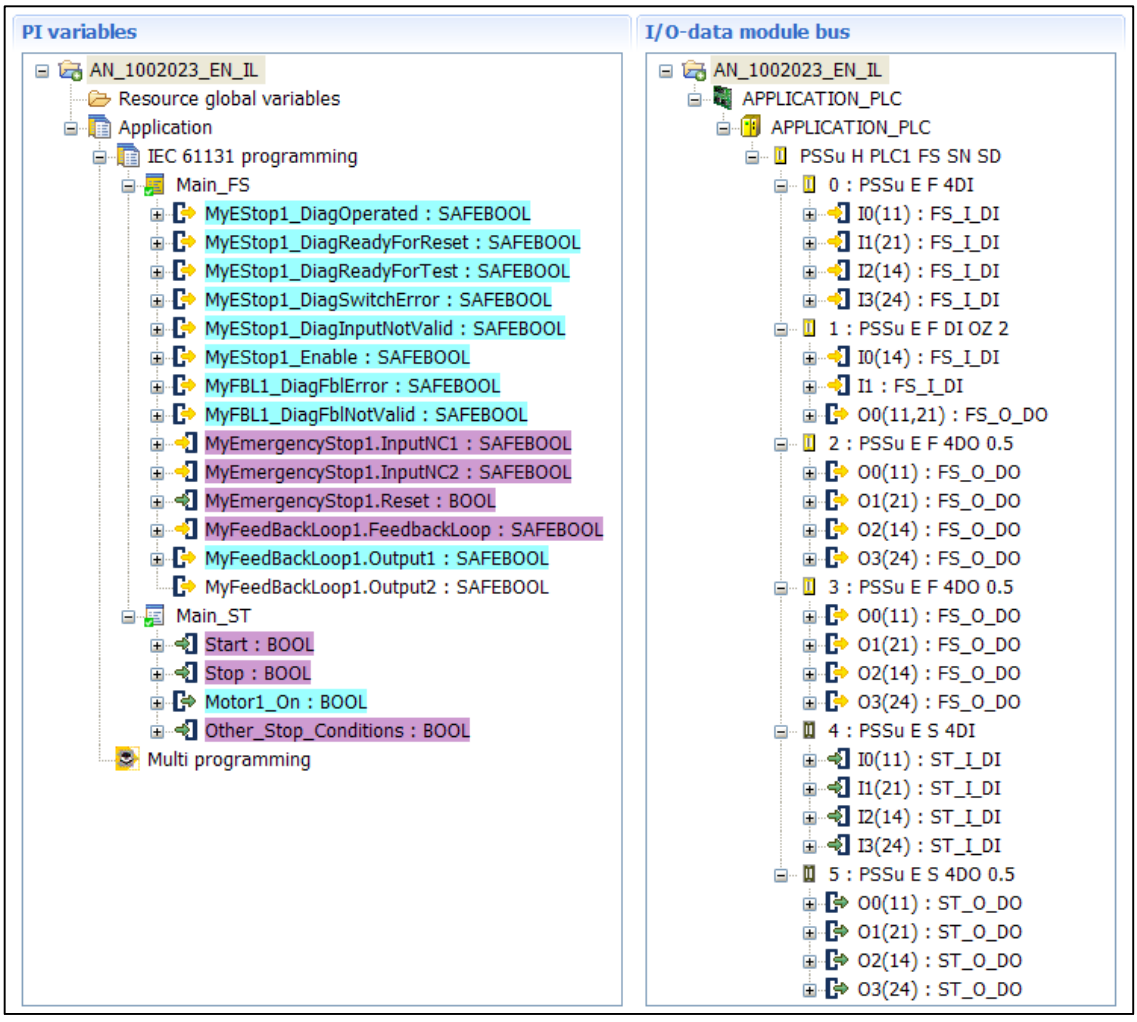


Fig. 4: Mapping Editor – IL-program

3.3.3. Process PAS Project

- Step 1: In the IL editor, PI variables and the logical sequence will be generated as a program.

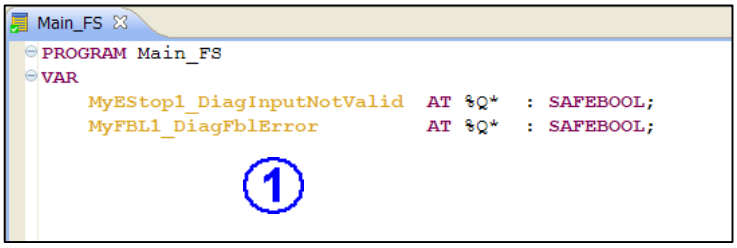


Fig. 5: PI variables

- Step 2: The design of the hardware (control, I/O, sensor, actor) will created as a circuit diagram. (parallel possible to Step 1)

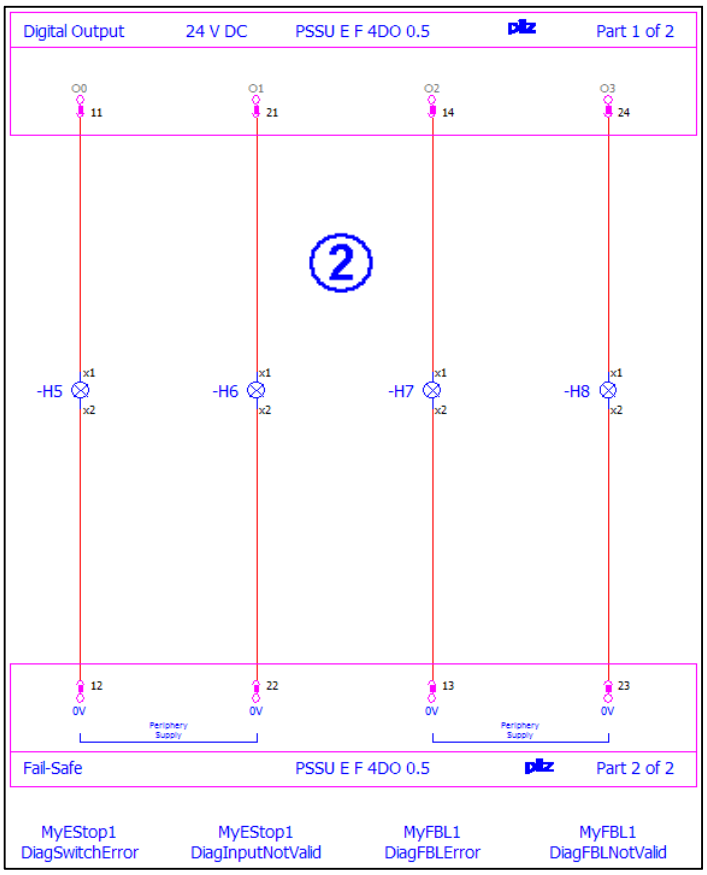


Fig. 6: Circuit diagram (extract)

- Step 3: Based on the PI variables (I/O), the required power of control (PLC, Multi) is selected. The implementation of the I/O modules in the PAS system occurs in the PSSu module editor.

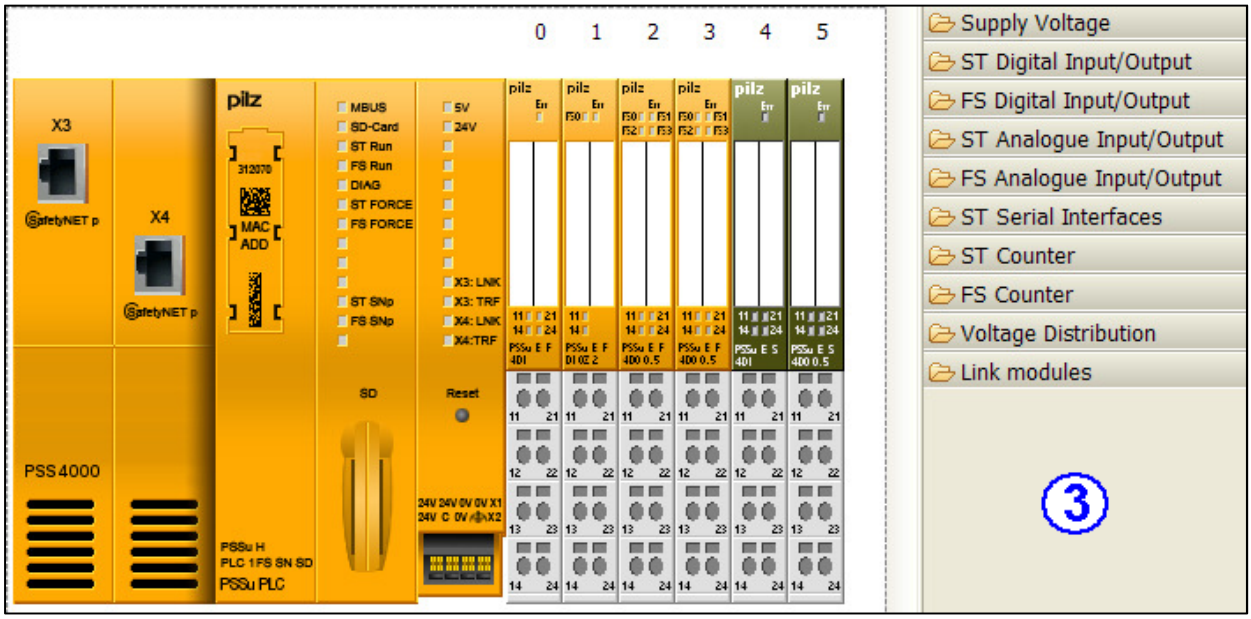


Fig. 7: PSSu Module Editor

- Step 4: Assignment of the PI variables in the I/O Mapping Editor.

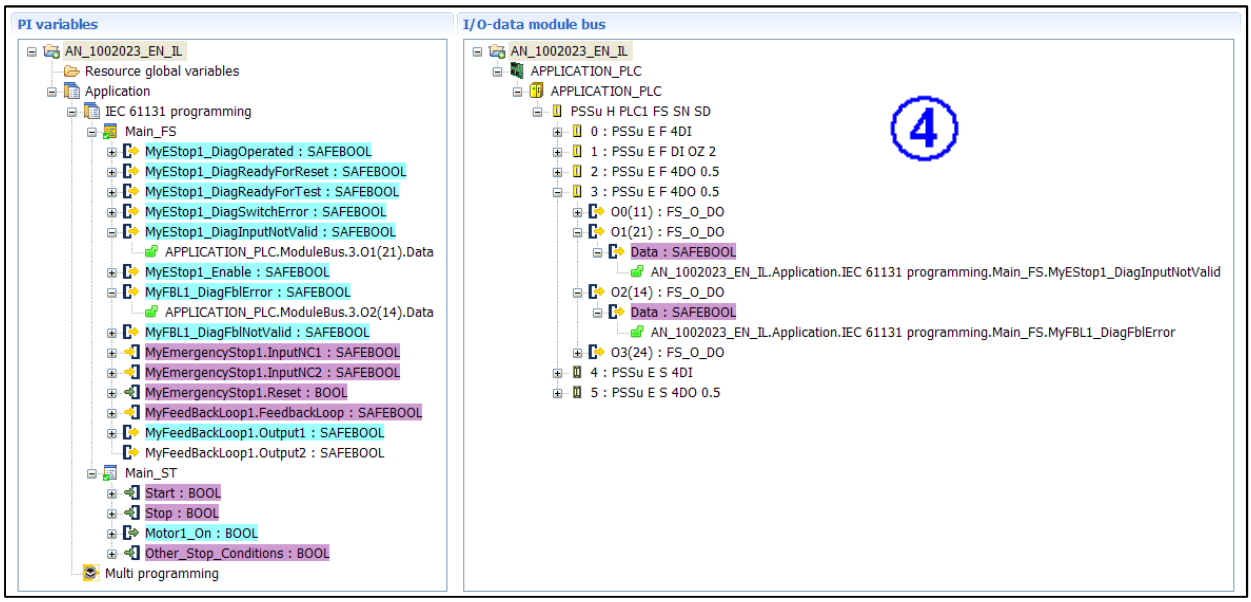


Fig. 8: I/O Mapping Editor

- Overview process PAS Project (Steps 1-4)

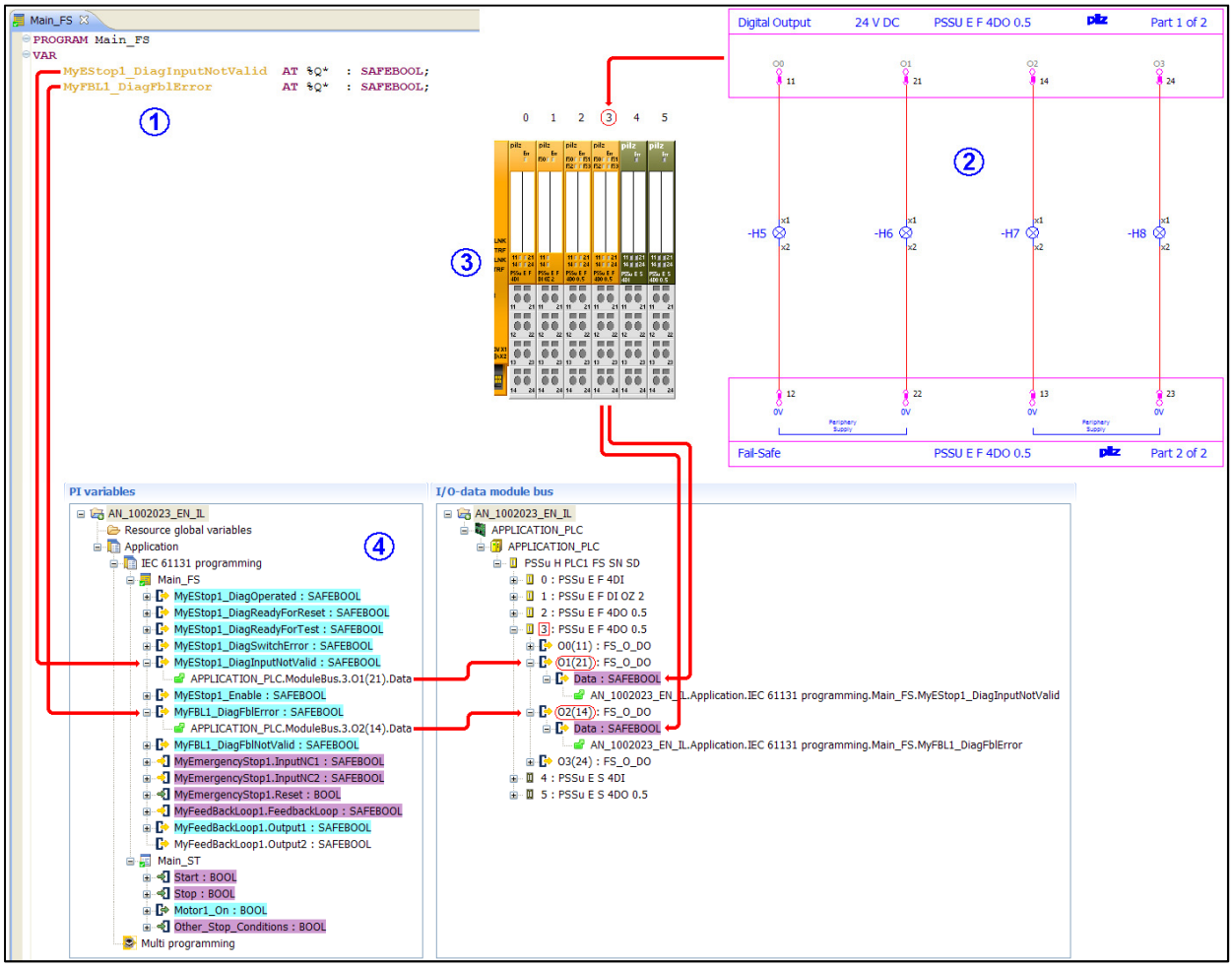
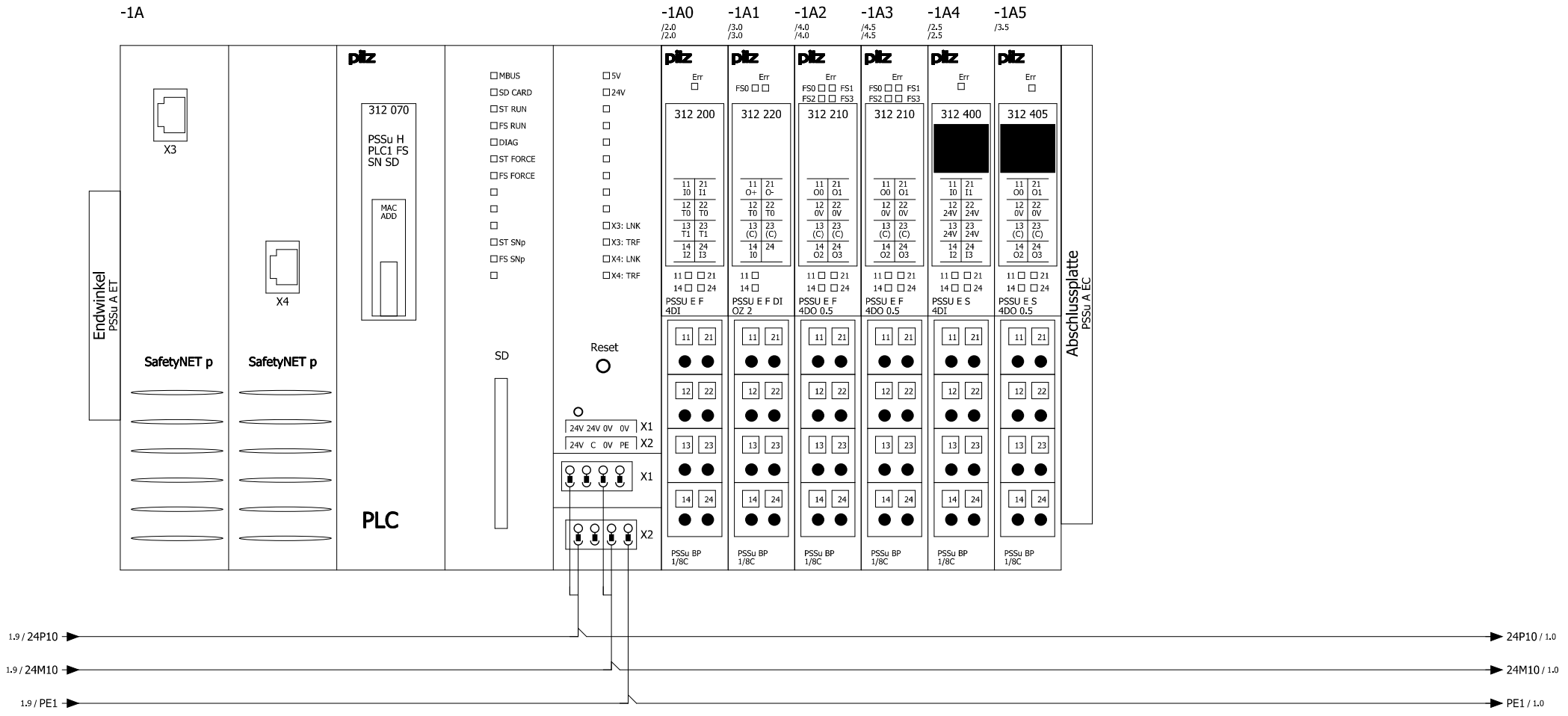


Fig. 9: Process PAS Project



PSSu E F 4DI
312 200

PSSu E S 4DI 0.5
312 400

PSSu E S 4DI 0.5
312 400

PSSu E F DI OZ 2
312 220

PSSu E S 4DO 0.5
312 405

PSSu E S 4DO 0.5
312 405

PSSu BP 1/8C
312 601

PSSu BP 1/8C
312 601

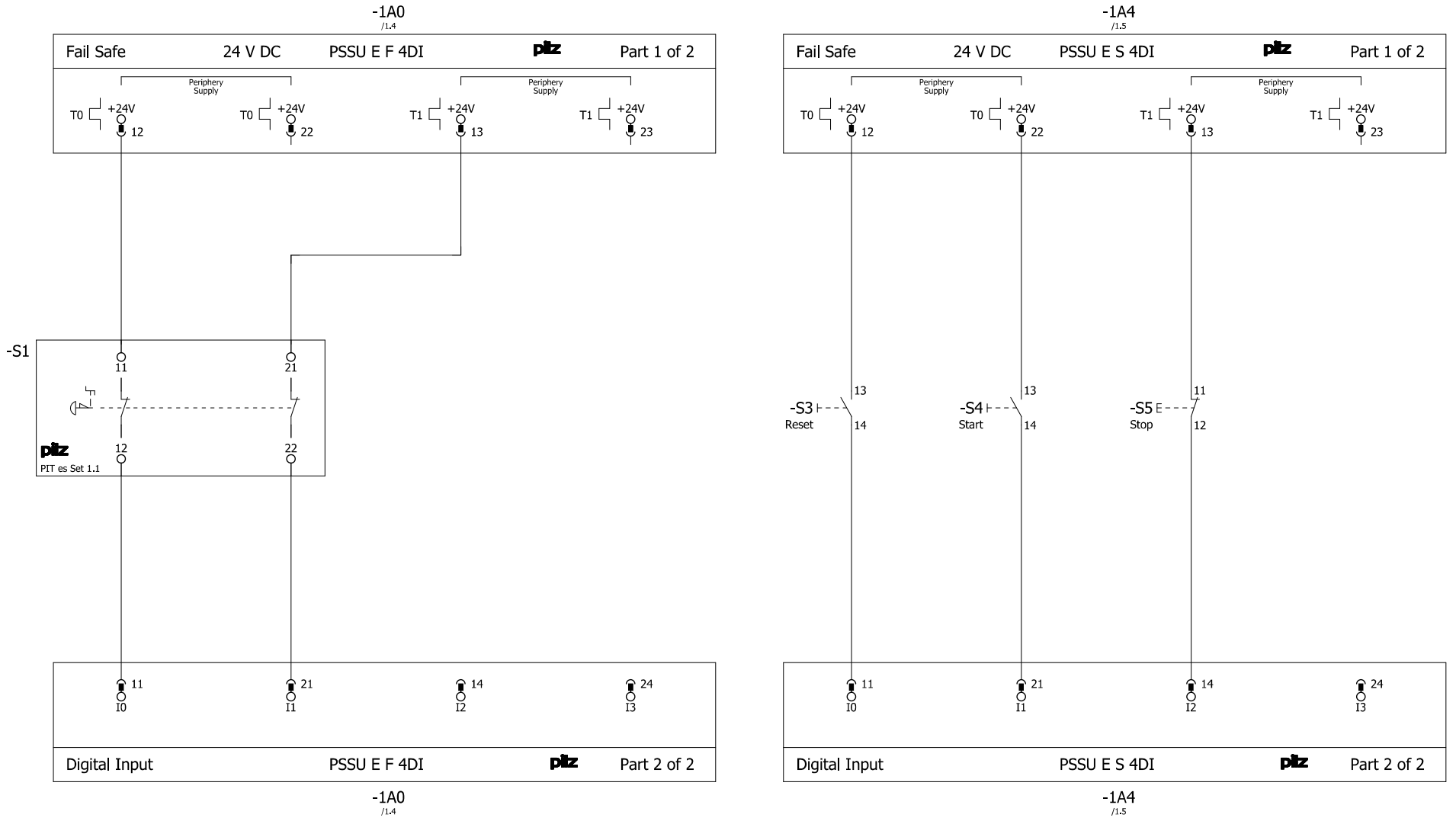
PSSu BP 1/8C
312 601

PSSu BP 1/8C
312 601

PSSu BP 1/8C
312 601

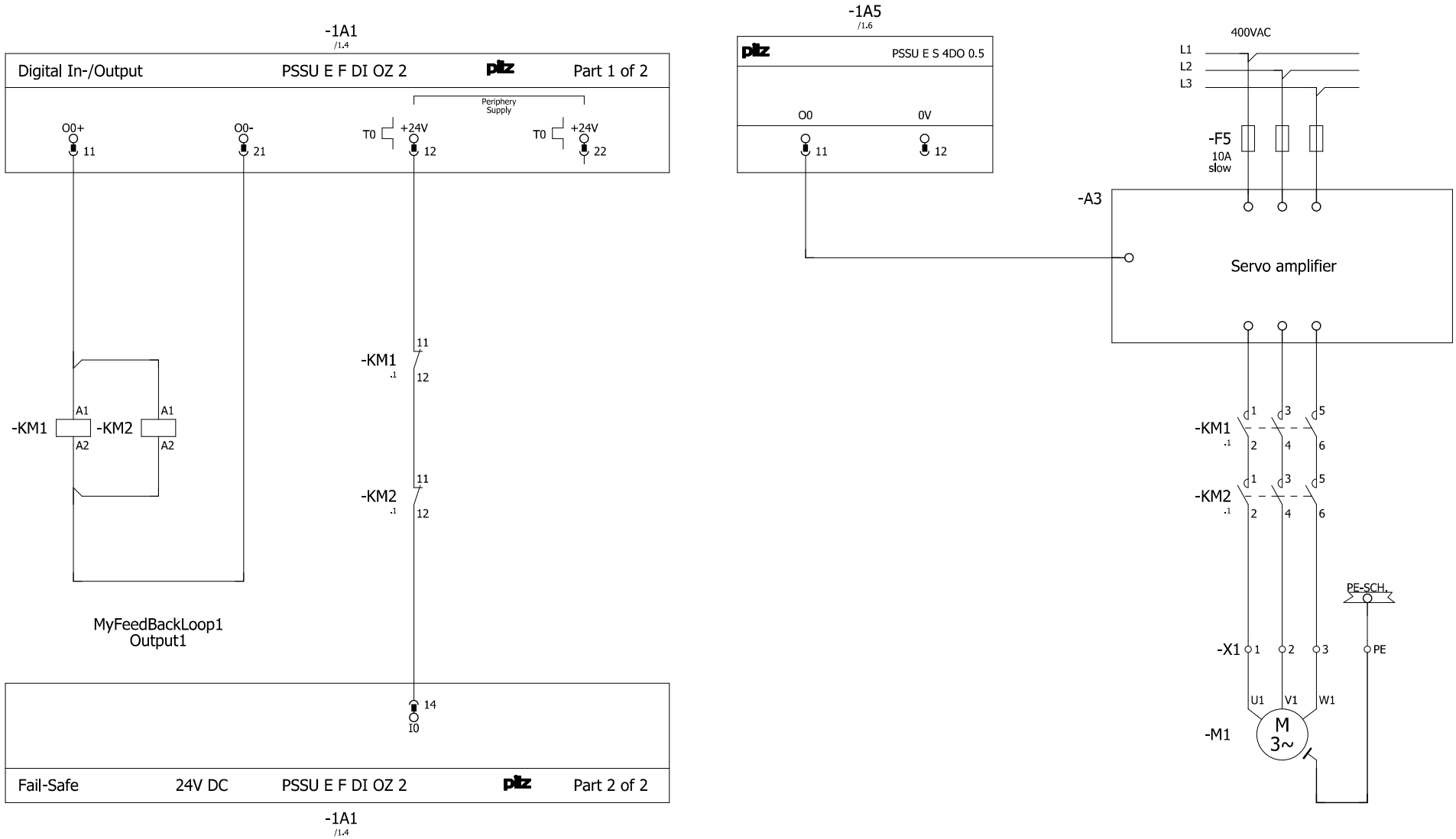
PSSu BP 1/8C
312 601

Revision	08.03.2012	Date	19.01.2005	EN ISO 13849-1:2006 PL e	Pilz GmbH & Co.KG Felix-Wankel-Str.2 73760 Ostfildern	PSS 4000 - Emergency Stop with PITestop
Name	RDS	Name	RDS			Power supply PSS 4000
				EN 62061:2005 SIL 3		Page: 1 / 4
		Dep.	CS			Mounting place + AN_1002023_02

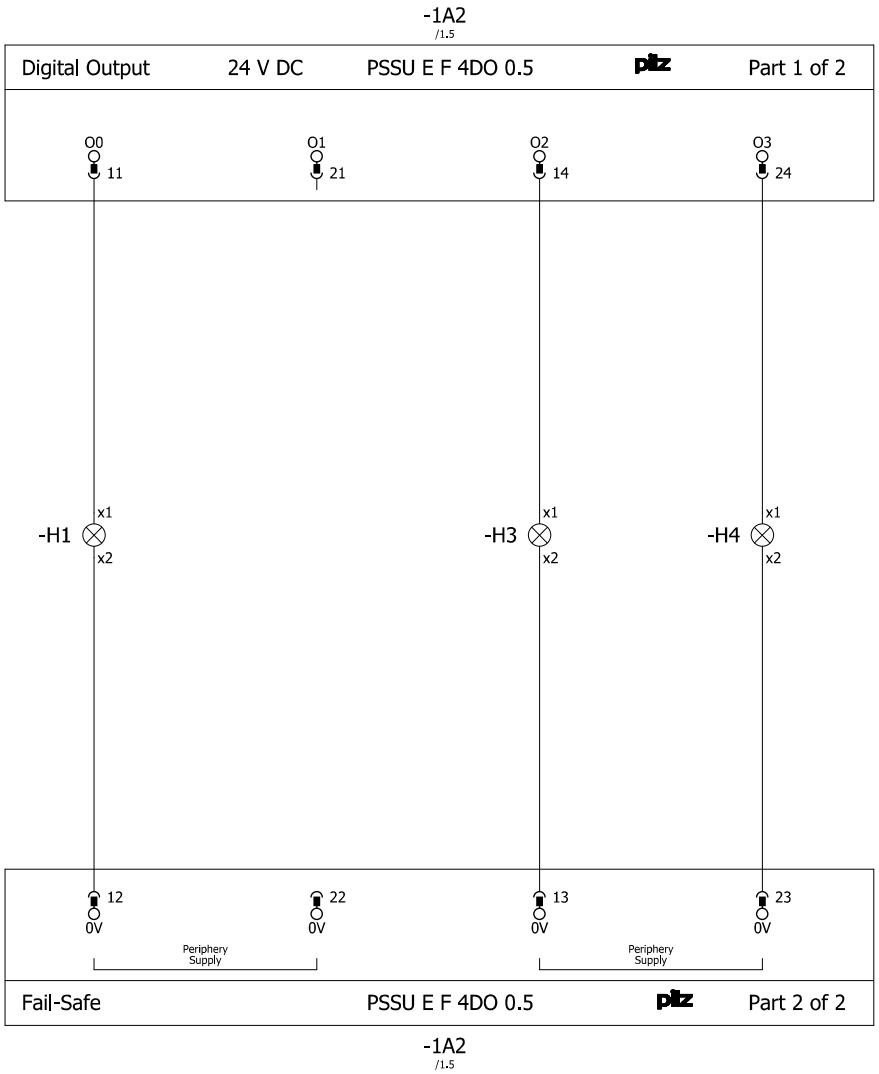


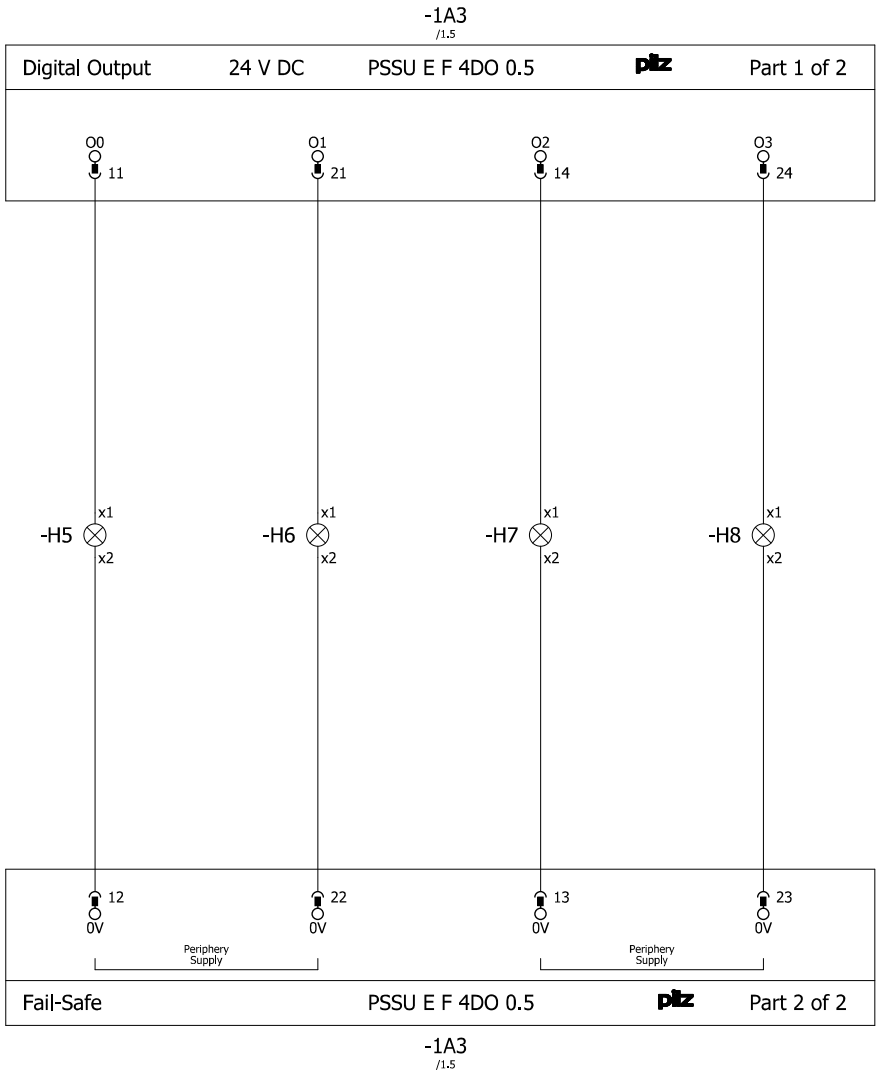
MyEmergencyStop1 InputNC1	MyEmergencyStop1 InputNC2	Spare	Spare
MyEmergencyStop1 Reset	Start	Stop	Spare

Revision	08.03.2012	Date	19.01.2005	EN ISO 13849-1:2006 PL e	Pilz GmbH & Co.KG Felix-Wankel-Str.2 73760 Ostfildern	PSS 4000 - Emergency Stop with PITestop	Mounting place + AN_1002023_02
Name	RDS	Name	RDS				
				EN 62061:2005 SIL 3		Inputs	Page: 2 / 4
		Dep.	CS				



Revision	08.03.2012	Date	19.01.2005	EN ISO 13849-1:2006 PL e	Pilz GmbH & Co.KG Felix-Wankel-Str.2 73760 Ostfildern	PSS 4000 - Emergency Stop with PITestop	Mounting place + AN_1002023_02
Name	RDS	Name	RDS			Drive	Page: 3 / 4
				EN 62061:2005 SIL 3			
		Dep.	CS				





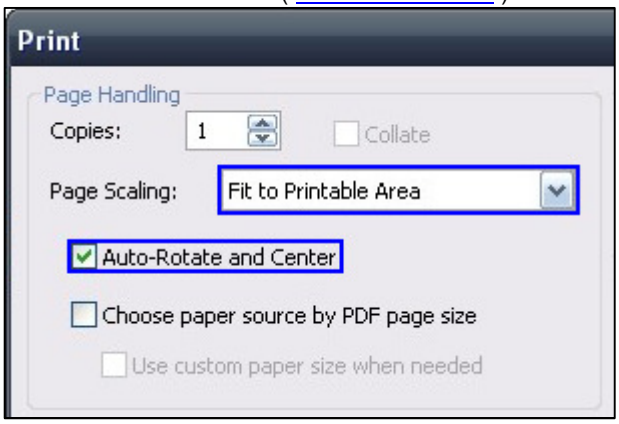
MyEStop1 DiagOperated	Spare	MyEStop1 DiagReadyForReset	MyEStop1 DiagReadyForTest	MyEStop1 DiagSwitchError	MyEStop1 DiagInputNotValid	MyFBL1 DiagFBLError	MyFBL1 DiagFBLNotValid

Revision	08.03.2012	Date	19.01.2005	EN ISO 13849-1:2006 PL e	Pilz GmbH & Co.KG Felix-Wankel-Str.2 73760 Ostfildern	PSS 4000 - Emergency Stop with PITestop	Mounting place + AN_1002023_02
Name	RDS	Name	RDS				
				EN 62061:2005 SIL 3		Status/Error message	Page: 4 / 4
		Dep.	CS				

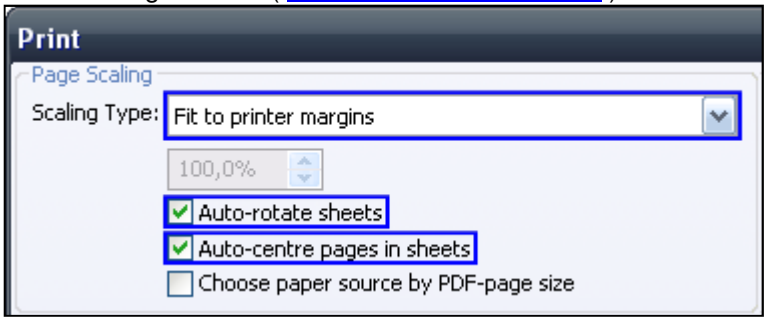
4. Table of figures

Recommended printer settings

Adobe Acrobat Reader (www.adobe.com)



PDF-XChange Viewer (www.tracker-software.com)



Technical support
+49 711 3409-444
support@pilz.com

...
In many countries we are represented by our subsidiaries and sales partners.

Please refer to our homepage for further details or contact our headquarters.

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern, Germany
Telephone: +49 711 3409-0
Telefax: +49 711 3409-133
E-Mail: pilz.gmbh@pilz.de
Internet: www.pilz.com