Control of burner safety valves with PSS outputs according to EN 50156

PILZ
THE SPIRIT OF SAFETY

Product

Type:	PSS 4000 relay outputs (DOR)
Name:	PSSu E F 2DOR 8, PSS u2 EF 2DO R 8A
Manufacturer:	Pilz GmbH & Co. KG, Safe Automation

Document

Release Number:	01
Release Date:	07 October 2021

Application Note – 1005745_EN_01

Document Revision History

Release	Date	Changes	Chapter
01	2021-10-07	Creation	all

Validity of Application Note

This present Application Note is valid until a new version of the document is published.
This and other Application Notes can be downloaded in the latest version and for free from www.pilz.com. For a simple search, use our content document (1002400) or the direct search function in the download area.

The Pilz newsletter is free of charge and keeps you up-to-date on all the latest issues and trends in safe automation.

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 knowledge and belief.
While every effort has been made to ensure the information provided is accurate, we cannot accept liability for the accuracy and entirety of the information provided, except in the case of gross negligence. In particular, all information on applicable standards, safety-related classifications and time characteristics should be viewed as provisional. 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.

October 2021

Industrial Security

To secure plants, systems, machines and networks against cyberthreats it is necessary to implement (and continuously maintain) an overall Industrial Security concept that is state of the art.
Perform a risk assessment in accordance with VDI/VDE 2182 or IEC 62443-3-2 and plan the security measures with care. If necessary, seek advice from Pilz Customer Support.

Abbreviations

Abbreviation / term	Description	Source
AN	**A**pplication **N**ote	www.pilz.com > AN content (1002400)
PNOZ	Pilz E-STOP positive-guided (DE: **P**ilz **NO**T-AUS-**Z**wangsgeführt)	www.pilz.com > PNOZ
PSS	Programmable control system (DE: **P**rogrammierbares **S**teuerungs**s**ystem)	www.pilz.com > PSS
PSS u2	**PSSu**niversal, **2**nd generation	www.pilz.com > PSS u2
POU	**P**rogram **O**rganisation **U**nit	
NC	**N**ormally **C**losed	
NO	**N**ormally **O**pen	

Definition of Symbols

Information that is particularly important is identified as follows:

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 could be damaged and also provides information on preventive measures that can be taken.
It also highlights areas within the text that are of particular importance.

INFORMATION

This gives advice on applications and provides information on special features.

Contents

1 Useful documentation

Reading the documentation listed below is necessary for understanding this Application Note. The availability of the software used and its safe handling are also presupposed for the user.

1.1 Documentation from Pilz GmbH & Co. KG

No.	Description	Item No. /Download
1	Pilz international homepage, download section	www.pilz.com
2	Operating manual PSSu E F 2DOR 8(-T)(-R)	21334-EN-xx
3	Operating manual PSS u2 EF 2DO R 8A	1003625-EN-xx
4	PAS4000 Online Help for Library Element FS_FBL_Monitoring(_PLC)	PAS4000
5	PNOZ s4.1	21890-EN-xx

1.2 Documentation from other sources of information

No.	Description	Item No. / Download
1		
2		
3		
4		

2 Used hardware and software

2.1 Pilz products

No.	Descriptions	Order number	Version	Number
1	PSSu E F 2DOR 8	312 225	07 / 15 (HW / SW)	1
2	PSS u2 EF 2DO R 8A	328 150	01 / 1.0.x (HW / SW)	1
3	PAS4000	-	v1.22.0	1
4	Library Element FS_FBL_Monitoring(_PLC)	-	V1.0.x	1
5	PNOZ s4.1 (C) 24VDC	750 124 (751 124)	1.0	2

2.2 Structure of the application (schematic)

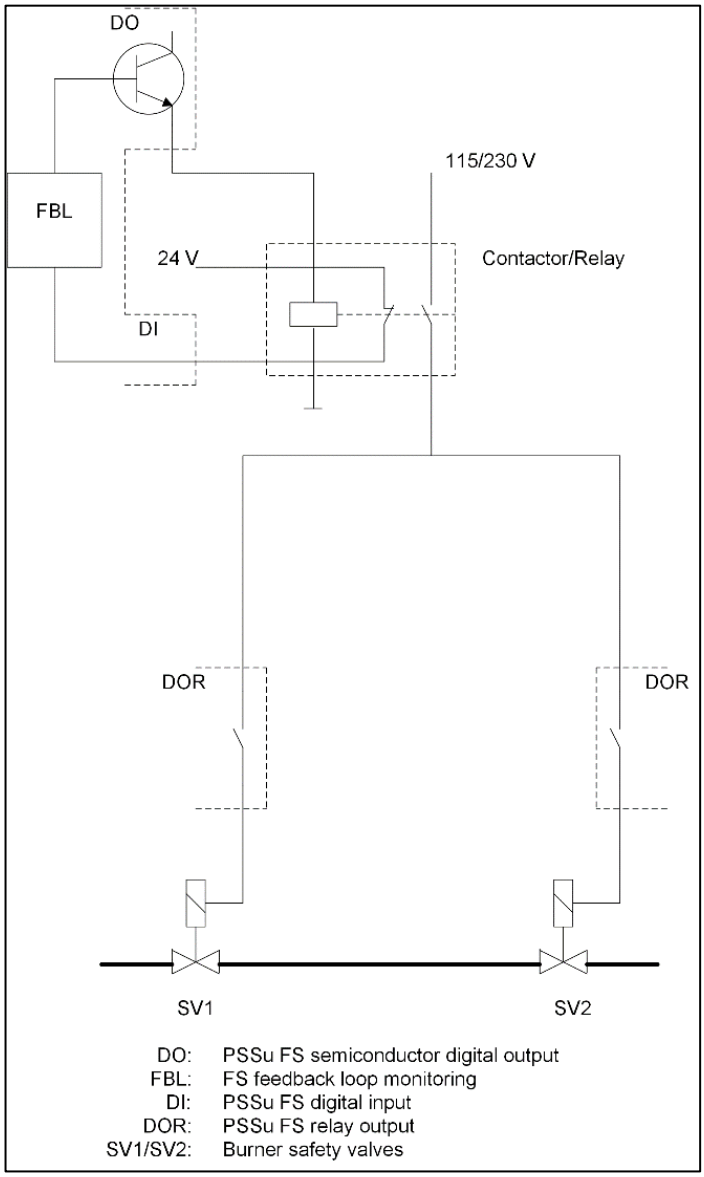


Figure 1: Application – Structure of the hardware (schematic)

3 Preface

The safety valves of a furnace are provided to obtain a safety shutdown of the entire fuel supply to the furnace. According to the standards for furnaces, two safety valves in series must be provided.

The standard EN 50156-1, “Electrical equipment for furnaces and ancillary equipment” prescribes analogously, that when the safety valves of a furnace are controlled by relay outputs and the furnace is in continuous operation (the relay outputs can not be tested regularly), these relay outputs have to be diverse in function or hardware.

This document describes an example, how to realize this diversity in hardware, when using PSSuniversal (2) to control and monitor the furnace.

This document is not applicable for the situation, where both safety valves are controlled by semiconductor outputs.

NOTICE

- A detailed explanation of safety functions used in the failsafe application and its evaluation regarding functional safety are not a part of this document.
- This document describes an example of how to comply with just a single requirement of the EN 50156-1 only (diverse relay outputs). Other requirements of the EN 50156-1 still must be considered by the user of this document and are not part of this document. These other requirements apply to Pilz products as well as to third party products.
- Other standards, like the EN ISO 13849-1 or the EN/IEC 62061, may also require redundancy and diversity for the relay outputs, for instance as a result of calculations of Performance Level (PL) or Safety Integrity Level (SIL), however, these considerations and calculations based on these standards are not part of this document. Only considerations based on EN 50156-1 are.
- Other standards, like for instance EN ISO 13849-1 or EN/IEC 62061 may also apply to furnaces. The consideration of these standards, like the calculation of a Performance Level (PL) or a Safety Integrity Level (SIL), is not part of this document. For these considerations and calculations we refer to other Application Notes.
- This document is only to be used by persons who are qualified and have the required knowledge regarding the safe operation of furnaces and regarding the applicable laws, directives and standards for furnaces.

4 Application description

4.1 Assumed starting situation

The valves for obtaining a safety shutdown of the entire fuel supply to a furnace (safety valves) have to be controlled by relay outputs, as the available semiconductor outputs are not suitable, due to insufficient power or a too low voltage of the semiconductor outputs, to drive the safety valves.

The furnace is in continuous operation, so the relay outputs cannot be tested regularly.

According to the EN 50156-1, in this situation the relay outputs must be diverse.

4.2 Solution with external contactor/relay

4.2.1 Solution

The available relay outputs are the outputs of the PSSuniversal (2) I/O modules

- PSSu E F 2DOR 8
- PSS u2 EF 2DO R 8A

Each safety valve is driven by a single output of these modules, so that each safety valve can be controlled separately (as is required to perform tightness control).

Both safety valves of one burner must be connected to one and the same relay output module.

To realize the required diversity, an external contactor/relay must be provided, which switches the common power supply to the safety valves. This external contactor/relay must be controlled by a failsafe semiconductor output of the PSSuniversal (2). This semiconductor output must be connected to the inputs A1/A2 of the contactor/relay. The common power supply to the safety valves must be switched with the contacts 1L1/2T1, 3L2/4T2 or 5L3/6T3 (contactor) respectively ..3/..4 (relay). The semiconductor output of the PSSuniversal (2) must be energized, when at least one of the safety valves is energized by the burner control and monitoring logic.

The auxiliary contact ..1/..2 of the contactor/relay must be connected to a failsafe input of the PSSuniversal (2) to realize a feedback loop monitoring. The auxiliary contact must be closed, when the contactor/relay is not actuated (NC). The feedback loop monitoring must be implemented as follows:

```
my_FS_FBL_Monitoring(
            Input := SafetyValve1 OR SafetyValve2,
            FeedbackLoop1 := ContactorFeedbackLoop,
            FeedbackLoop2 := ContactorFeedbackLoop,
            Output1 => Contactor
```

Where

- `my_FS_FBL_Monitoring` is an instance of the library element FS_FBL_Monitoring(_PLC) for feedback loop monitoring,
- `SafetyValve1` and `SafetyValve2` are the output signals to the relay outputs from the burner control and monitoring logic for the safety valves,
- `ContactorFeedbackLoop` is the feedback loop signal from the contactor/relay and
- `Contactor` is the output signal to the external contactor/relay.

The instance of the library element FS_FBL_Monitoring(_PLC) can be operated with its default settings. Possibly only the monitoring times for switching on and of (I-Variables *FBL_TimeSwitchOn* and *FBL_TimeSwitchOff*) must be adapted to the actual switching times of the contactor/relay.

The output signals to the relay outputs for the safety valves (`SafetyValve1` and `SafetyValve2`) are the output signals from a failsafe burner control and monitoring logic to control the safety valves, like for instance O-PI-Variables connected to the O-Variables *SafetyValve1* and *SafetyValve2* from the library element FS_BurnerManagementSystem(_PLC).

The enable signal from the feedback loop monitoring (`my_FS_FBL_Monitoring.Enable`) must be integrated in the safety chain of the burner control and monitoring logic, for instance connected to the I-Variable *SafetyChain1* from the library element FS_BurnerManagementSystem(_PLC) and must, when reset, evoke a fault lockout of the burner control.

To ensure, that in case of an error of the relay output module, all involved outputs are switched off, both safety valves of one burner must be connected to one and the same relay output module. Further on, relay outputs and semiconductor output must be on one and the same PSSuniversal system or (PSSuniversal 2 only) the VALID bit of the relay output module must be integrated in the safety chain of the burner control and monitoring logic.

4.2.2 Safety analysis

4.2.2.1 Relay output failure

A stuck-at-1 failure of a relay output is recognized by the PSSuniversal (2) system, when this relay output is given a command to switch off, for instance when a safety shutdown of the furnace is performed.

When the solution is implemented as described above, the PSSuniversal (2) system reacts on this failure by switching off all outputs of the PSSuniversal system or by switching off all outputs of the relay module (PSSuniversal 2 only). By this way, the other relay output is switched off, thereby switching off the other safety valve. Also, the contactor/relay is switched off, thereby cutting of the power supply to both safety valves.

The switching-off of both safety valves is by itself not recognized by the burner control and monitoring logic, however, the switching-off of all outputs of the PSSuniversal system results in a shutdown of the furnace, which again causes at least a flame error or an air pressure error causing the burner control and monitoring logic to perform at least a safety shutdown.

4.2.2.2 Contactor/relay failure

According to the logic as described in section 4.2.1, the contactor/relay is given a command to switch off, as soon as the burner control and monitoring logic switches off both relay outputs / safety valves.

A stuck-at-1 failure of the contactor/relay is recognized by the feedback loop monitoring of the contactor/relay, when the relay outputs / safety valves are switched off, for instance when a regular stop of the furnace is performed. The feedback loop monitoring will then reset its enable output, thereby interrupting the safety chain of the burner control and monitoring logic, which results in a safety shutdown of the furnace.

4.2.2.3 Resulting safe application conditions

As a result of this analysis, following safe application conditions must be fulfilled:

Both safety valves of one burner must be connected to one and the same relay output module. Further on, relay outputs and semiconductor output must be on one and the same PSSuniversal system or (PSSuniversal 2 only) the VALID bit of the relay output module must be integrated in the safety chain of the burner control and monitoring logic.

4.3 Solution with PNOZ s4.1 (C) 24VDC

4.3.1 Instead of contactor/relay

Instead of a contactor/relay, as described in section 4.2, also a PNOZ s4.1 can be used. The PNOZ s4.1 is certified according to EN 50156-1.

Alternative to the contactor/relay the wiring must be as follows: The failsafe semiconductor output must be connected to the inputs S12 and S22 of the PNOZ s4.1. The common power supply to the safety valves must be switched with the contacts 13/14, 23/24 or 33/34.

Inputs S12 and S34 have to be connected, to enable an automatic start.
For the feedback loop monitoring the feedback loop signal is provided by the auxiliary contact 41/42. The feedback loop monitoring must be implemented as described in section 4.2, where `Contactor` is the output signal to PNOZ s4.1 and `ContactorFeedbackLoop` is the feedback loop signal from the PNOZ s4.1.

The feedback loop monitoring is actually not required to meet the requirements of the EN 50156-1 regarding the self-monitoring capabilities of the used contactor/relay, as the PNOZ s4.1 is already self-monitoring. However, the feedback loop monitoring, when it is integrated in the safety chain of the burner control and monitoring logic, for instance connected to the I-Variable *SafetyChain1* from the library element FS_BurnerManagementSystem(_PLC), enables a faster reaction time and better diagnosis in case of a failure.

The PNOZ s4.1 must be setup as follows:

- In2+ : Single-channel operation
- A : Automatic start

The same safe application conditions as in section 4.2 also apply here.

Since the power supply to the safety valves is controlled by the PNOZ s4.1, the switch-on delays of the PNOZ s4.1 have to be considered, which are described in the operating manual. These delays will result in a delayed opening of the safety valves. This has to be considered when the safety time for the ignition is determined and also when the times for venting and filling for the tightness control are determined.

The switch-on delay also must be considered at the monitoring time of the feedback loop monitoring of the PNOZ s4.1.

4.3.2 No relay outputs available

A PNOZ s4.1 can also be used to drive the safety valves directly if no relay outputs at all are available and the available semiconductor outputs have insufficient power or a too low voltage to drive the safety valves.

The PNOZ s4.1 is controlled by a semiconductor output. If the safety valves must be controlled separately (as is required to perform tightness control), two semiconductor output/PNOZ s4.1 combinations must be used, one for each safety valve, as shown below:

PSS universal (2) semiconductor output *x* |––––– PNOZ s4.1 ––––– Burner safety valve 1
PSS universal (2) semiconductor output *x+1* |––––– PNOZ s4.1 ––––– Burner safety valve 2

The wiring of the PNOZ s4.1 and is the same as described in section 4.3.1, whereby the safety valve is now directly switched by the PNOZ s4.1.

The setup of the PNOZ s4.1 is the same as described in section 4.3.1.

The feedback loop monitoring must be implemented for each semiconductor output/PNOZ s4.1 combination as follows:

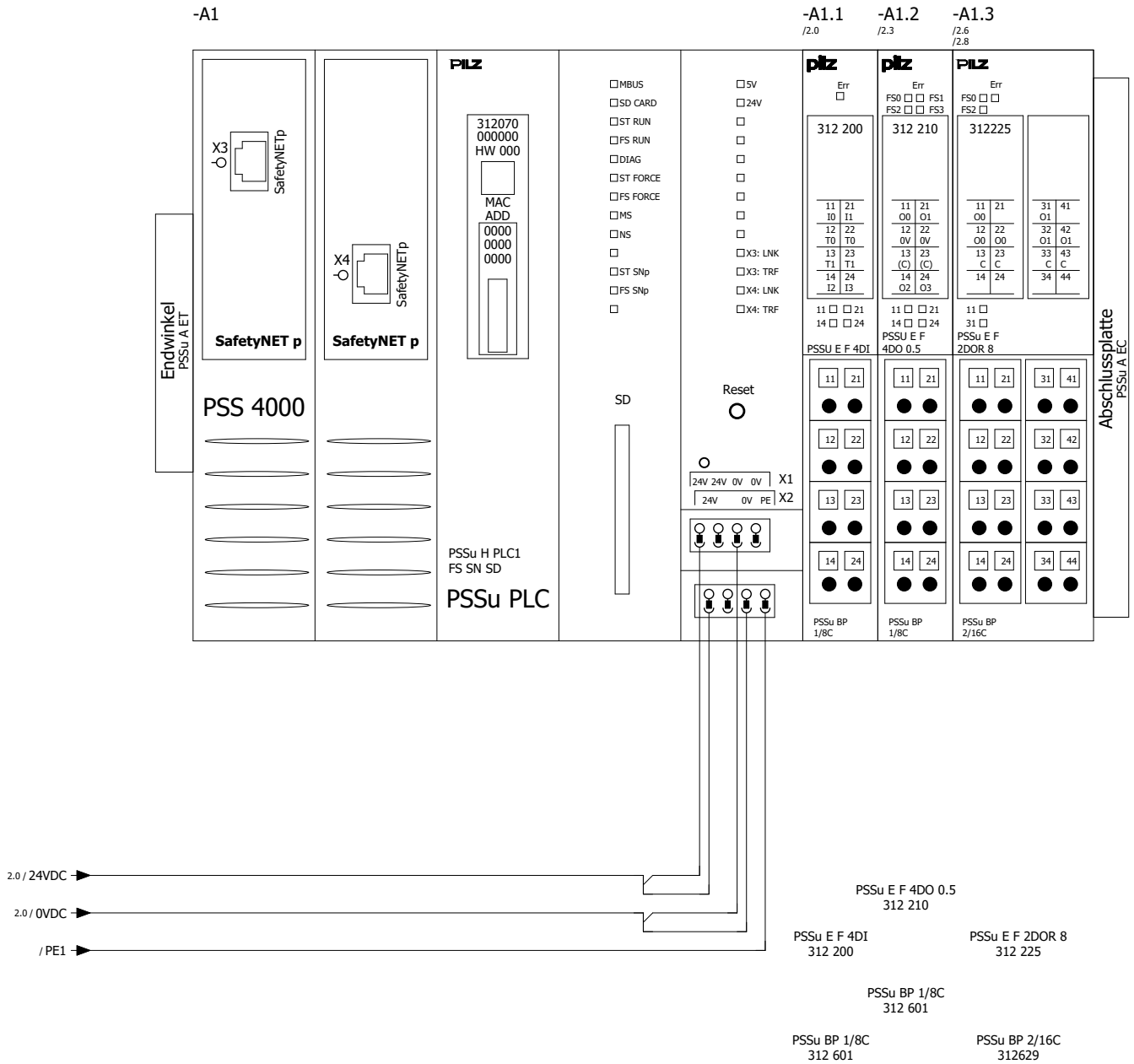
```
my_FS_FBL_Monitoring(
            Input := SafetyValve,
            FeedbackLoop1 := ContactorFeedbackLoop,
            FeedbackLoop2 := ContactorFeedbackLoop,
            Output1 => Contactor
```

Where

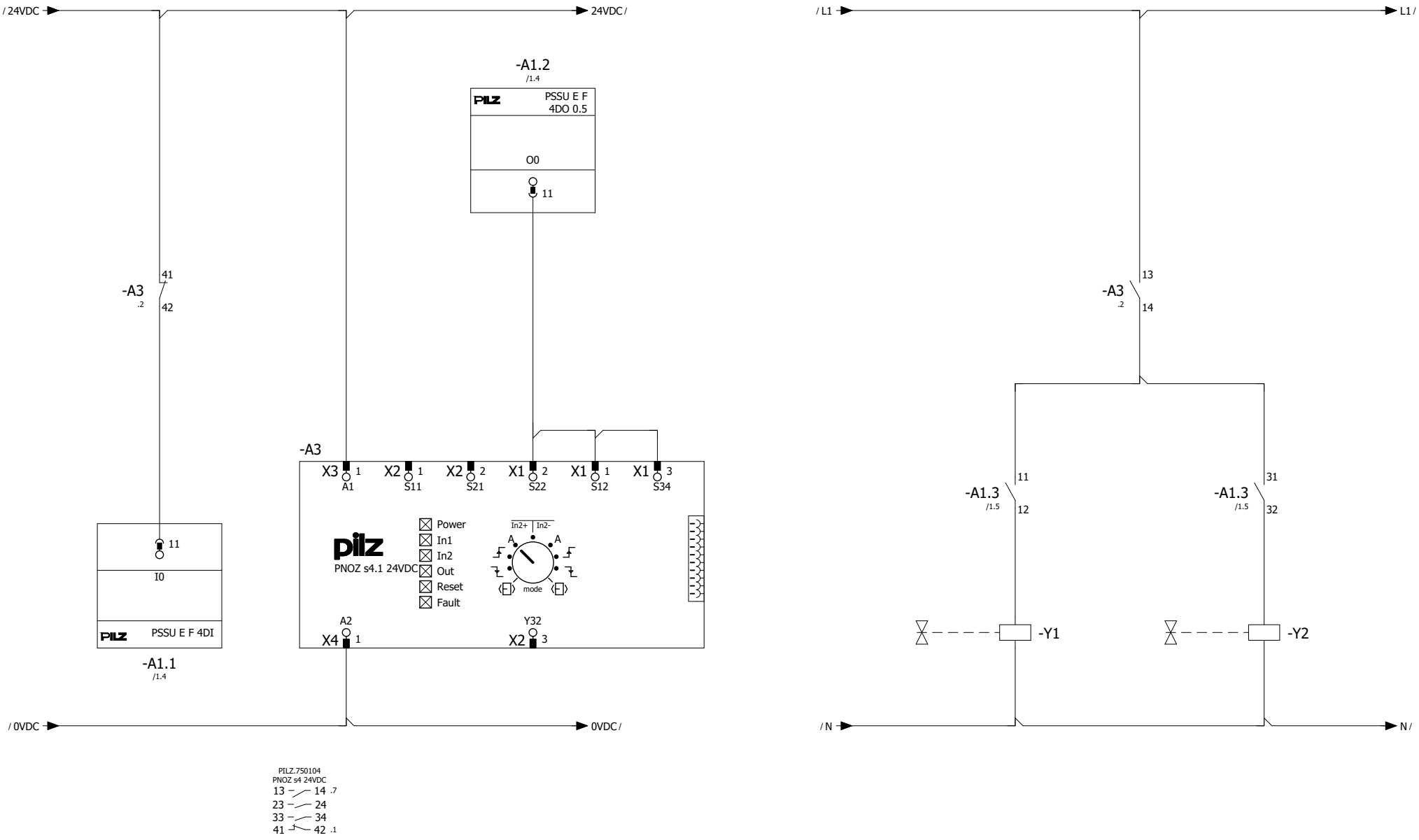
- `my_FS_FBL_Monitoring` is an instance of the library element FS_FBL_Monitoring(_PLC) for feedback loop monitoring,
- `SafetyValve` is the output signal from the burner control and monitoring logic for the safety valve,
- `ContactorFeedbackLoop` is the feedback loop signal from the the PNOZ s4.1 and
- `Contactor` is the output signal to the PNOZ s4.1.

As the safety valves are directly controlled by the PNOZ s4.1 the switch-on delays of the PNOZ s4.1 must be considered, which are described in the operating manual. These delays will result in a delayed opening of the safety valves. This must be considered when the safety time for the ignition is determined and also when the times for venting and filling for the tightness control are determined.

The switch-on delay also must be considered at the monitoring time of the feedback loop monitoring of the PNOZ s4.1.



Revision	24.08.2021	Date	24.08.2021	EN 50156-1	PILZ Pilz GmbH & Co.KG Felix-Wankel-Str.2 73760 Ostfildern	PSSu - Control Of Burner Safety Valves with PNOZ s4.1	Mounting place + AN_1005745_01
Name	Pilz	Name	Pilz				Page: 1 / 2
		Dep.	CSI				



PILZ.750104
PNOZ s4 24VDC
13 — 14 .7
23 — 24
33 — 34
41 — 42 .1

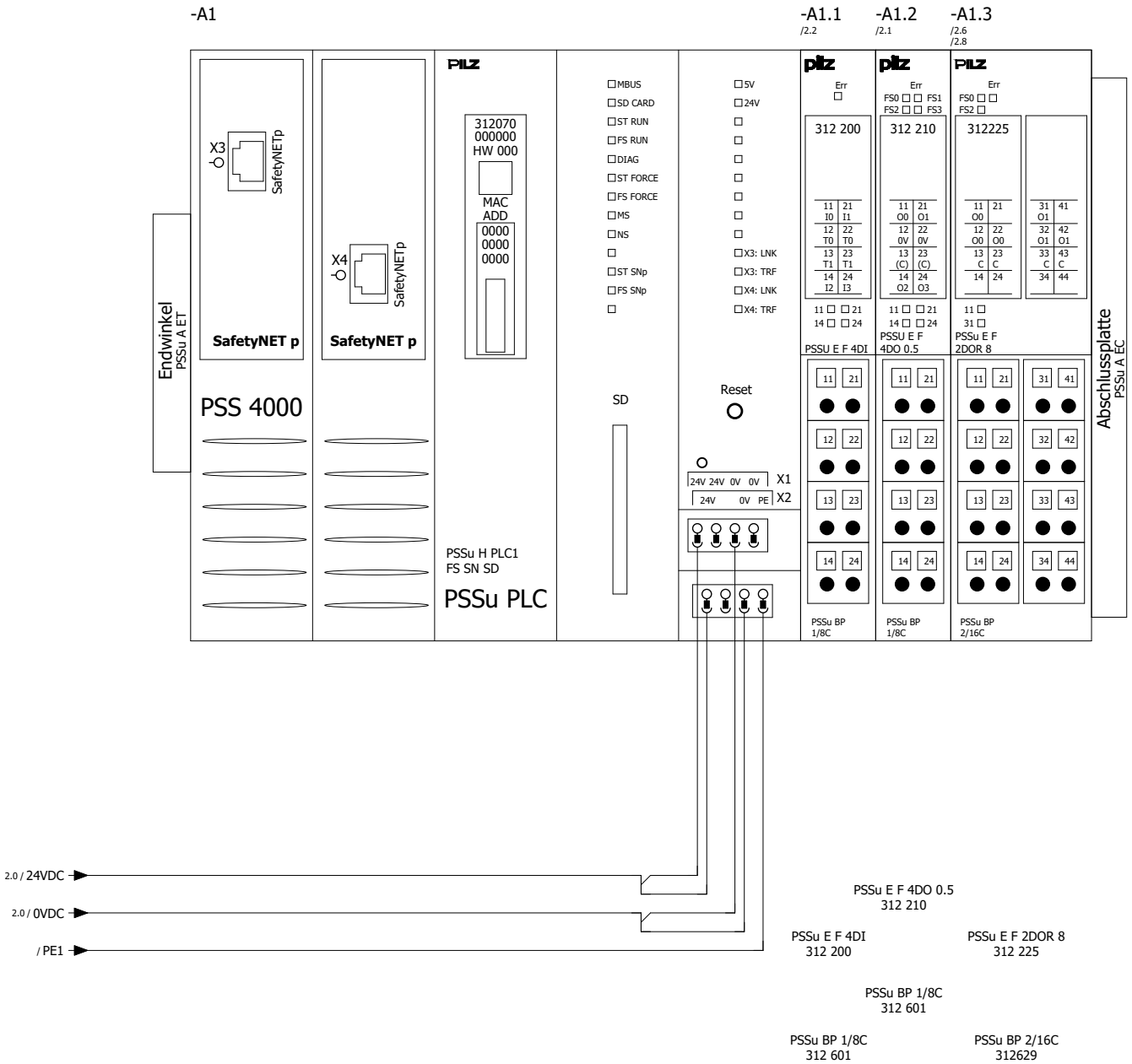
FBL

Control
Safety Valve

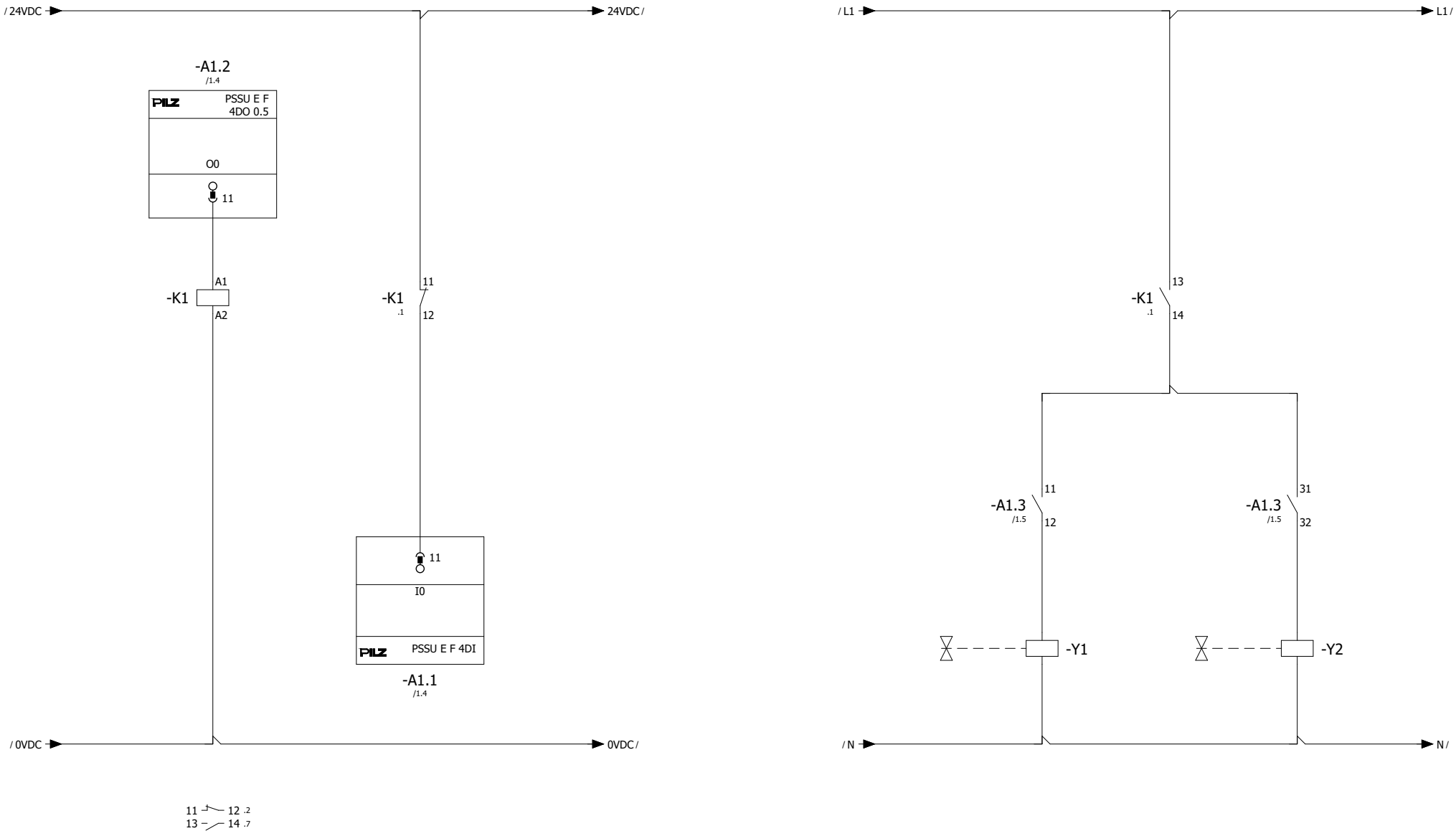
Safety Valve 1

Safety Valve 2

Revision	24.08.2021	Date	24.08.2021	EN 50156-1	PILZ Pilz GmbH & Co.KG Felix-Wankel-Str.2 73760 Ostfildern	PSSu - Control Of Burner Safety Valves with PNOZ s4.1	Mounting place + AN_1005745_01
Name	Pilz	Name	Pilz				Page: 2 / 2
		Dep.	CSI				



Revision	24.08.2021	Date	24.08.2021	EN 50156-1	PILZ Pilz GmbH & Co.KG Felix-Wankel-Str.2 73760 Ostfildern	PSSu - Control Of Burner Safety Valves With External Relay	Mounting place + AN_1005745_02
Name	Pilz	Name	Pilz				Page: 1 / 2
		Dep.	CSI				



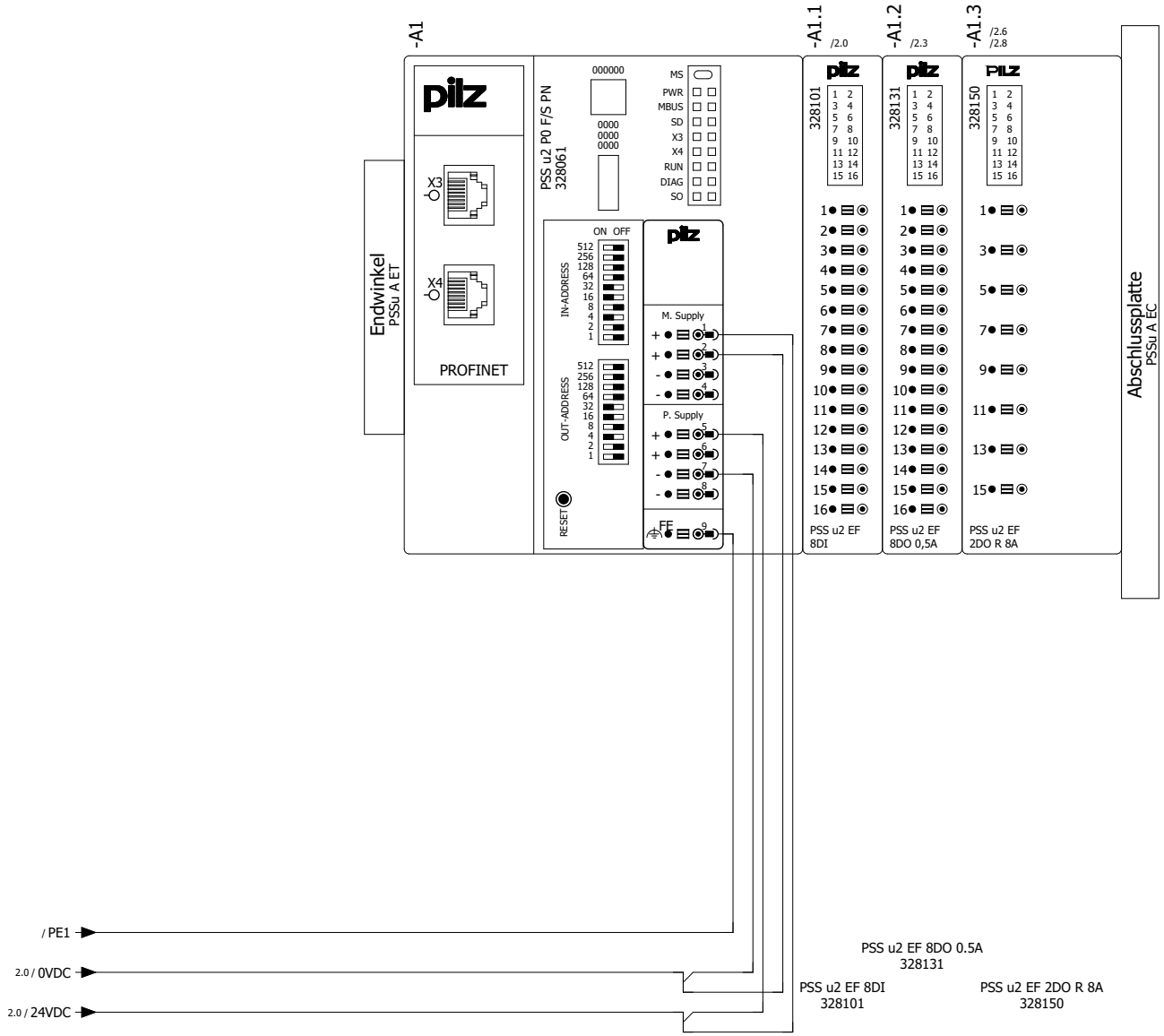
Control Safety Valve

FBL

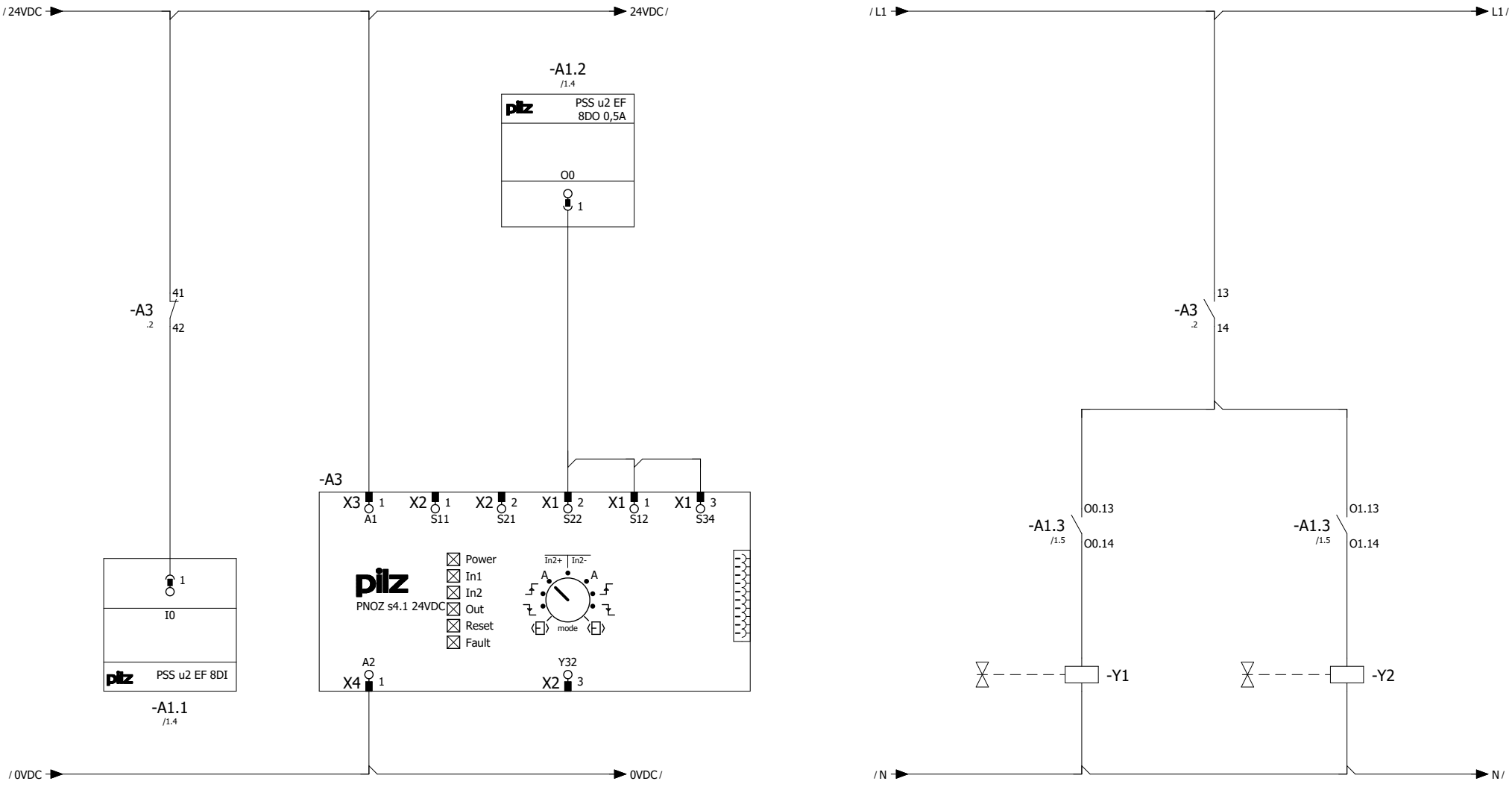
Safety Valve 1

Safety Valve 2

Revision	24.08.2021	Date	24.08.2021	EN 50156-1	PILZ Pilz GmbH & Co.KG Felix-Wankel-Str.2 73760 Ostfildern	PSSu - Control Of Burner Safety Valves With External Relay	Mounting place + AN_1005745_02
Name	Pilz	Name	Pilz				Page: 2 / 2
		Dep.	CSI				



Revision	24.08.2021	Date	24.08.2021	EN 50156-1	PILZ Pilz GmbH & Co.KG Felix-Wankel-Str.2 73760 Ostfildern	PSSu2 - Control Of Burner Safety Valves with PNOZ s4.1	Mounting place + AN_1005745_03
Name	Pilz	Name	Pilz				Page: 1 / 2
		Dep.	CSI				



PILZ.750104
PNOZ s4 24VDC
13 — 14 .7
23 — 24
33 — 34
41 — 42 .1

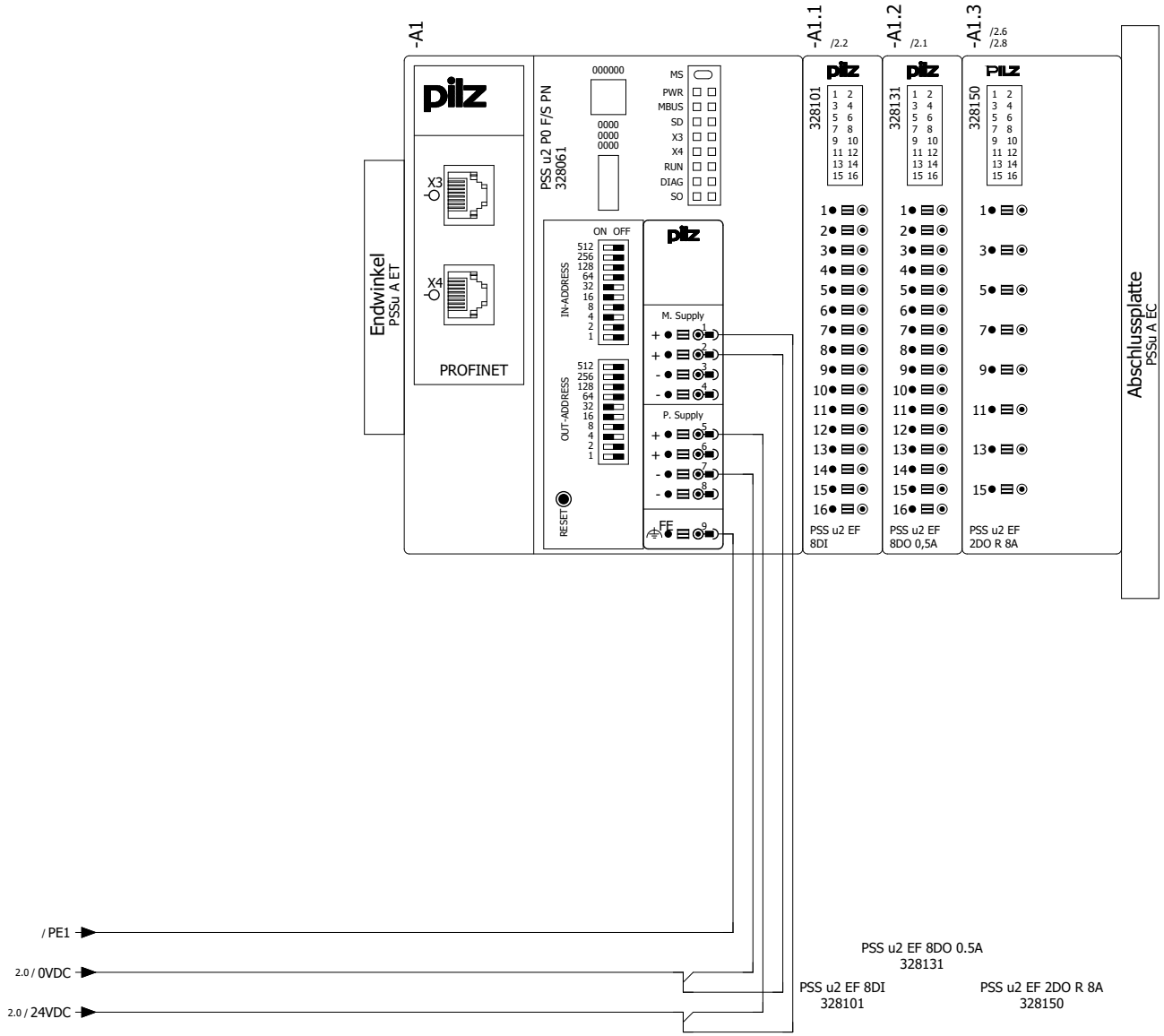
FBL

Control
Safety Valve

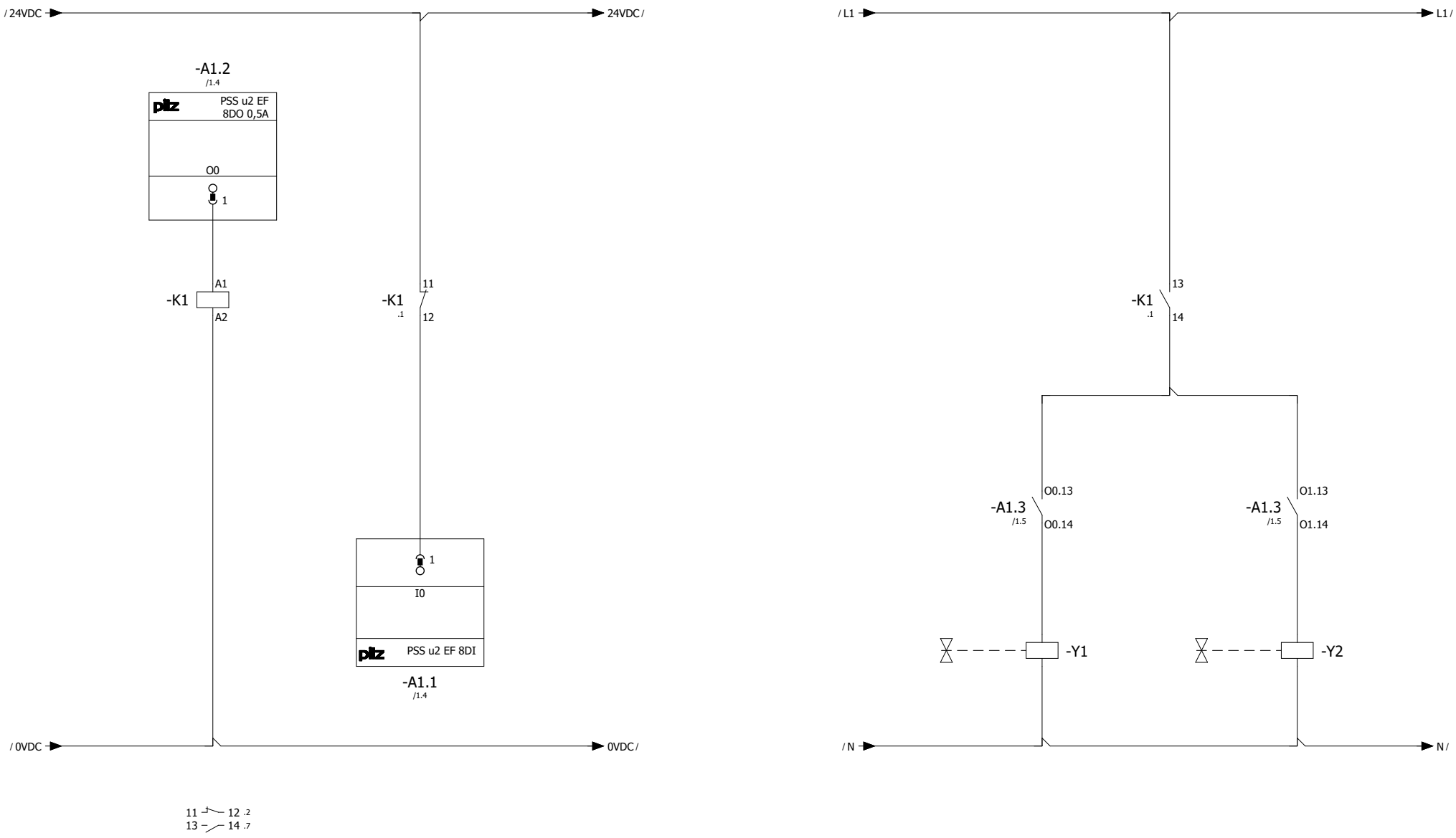
Safety Valve 1

Safety Valve 2

Revision	24.08.2021	Date	24.08.2021	EN 50156-1	Pilz GmbH & Co.KG Felix-Wankel-Str.2 73760 Ostfildern	PSSu2 - Control Of Burner Safety Valves with PNOZ s4.1	Mounting place + AN_1005745_03
Name	Pilz	Name	Pilz				Page: 2 / 2
		Dep.	CSI				



Revision	24.08.2021	Date	24.08.2021	EN 50156-1	PILZ Pilz GmbH & Co.KG Felix-Wankel-Str.2 73760 Ostfildern	PSSu2 - Control Of Burner Safety Valves With External Relay	Mounting place + AN_1005745_04
Name	Pilz	Name	Pilz				Page: 1 / 2
		Dep.	CSI				



Revision	24.08.2021	Date	24.08.2021	EN 50156-1	Pilz GmbH & Co.KG Felix-Wankel-Str.2 73760 Ostfildern	PSSu2 - Control Of Burner Safety Valves With External Relay
Name	Pilz	Name	Pilz			
		Dep.	CSI			

Mounting place
+ AN_1005745_04

Page: 2 / 2

6 Table of figures

Support

Technical support is available from Pilz round the clock.

Americas
Brazil
+55 11 97569-2804
Canada
+1 888 315 7459
Mexico
+52 55 5572 1300
USA (toll-free)
+1 877-PILZUSA (745-9872)

Asia
China
+86 21 60880878-216
Japan
+81 45 471-2281
South Korea
+82 31 778 3300

Australia
+61 3 95600621

Europe
Austria
+43 1 7986263-0
Belgium, Luxembourg
+32 9 3217570
France
+33 3 88104003
Germany
+49 711 3409-444
Ireland
+353 21 4804983
Italy, Malta
+39 0362 1826711
Scandinavia
+45 74436332
Spain
+34 938497433
Switzerland
+41 62 88979-32
The Netherlands
+31 347 320477
Turkey
+90 216 5775552
United Kingdom
+44 1536 462203

You can reach our international hotline on:
support@pilz.com

Pilz develops environmentally-friendly products using ecological materials and energy-saving technologies. Offices and production facilities are ecologically designed, environmentally-aware and energy-saving. So Pilz offers sustainability, plus the security of using energy-efficient products and environmentally-friendly solutions.

Energy saving by Pilz

BLUECOMPETENCE Alliance Member
Partner of the Engineering Industry Sustainability Initiative

pilz
Partner of:
The Best of German Engineering

1005173-EN-01 Draft 01, 2019-06 Printed in Germany

We are represented internationally. Please refer to our homepage www.pilz.com for further details or contact our headquarters.

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

PILZ
THE SPIRIT OF SAFETY