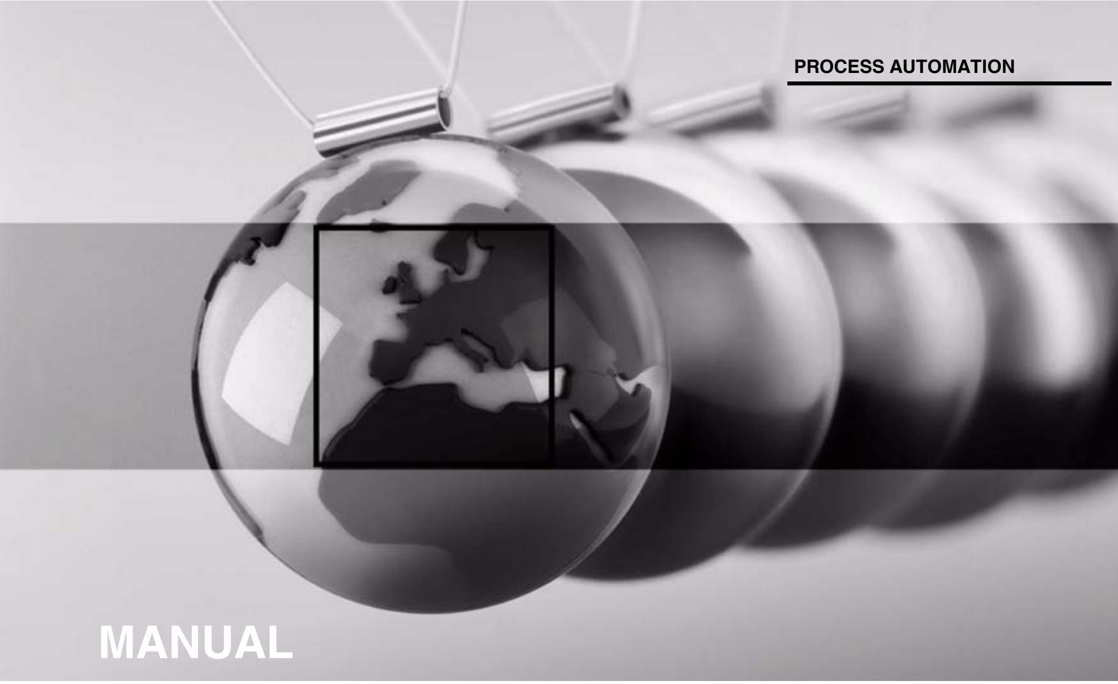
PROCESS AUTOMATION



MANUAL

Functional Safety

SMART Transmitter Power Supply/Current Driver HiD2024

SIL

IEC 61508/61511

ISO9001

SIL 2

PEPPERL+FUCHS

PROTECTING YOUR PROCESS

1 Introduction

1.1 Contents

This document contains information for usage of the device in functional safety-related applications. You need this information to use your product throughout the applicable stages of the product life cycle. These can include the following:

- Product identification
- Delivery, transport, and storage
- Mounting and installation
- Commissioning and operation
- Maintenance and repair
- Troubleshooting
- Dismounting
- Disposal

Note!

This document does not substitute the instruction manual.

Note!

For full information on the product, refer to the instruction manual and further documentation on the Internet at www.pepperl-fuchs.com.

The documentation consists of the following parts:

- Present document
- Instruction manual
- Manual
- Datasheet

Additionally, the following parts may belong to the documentation, if applicable:

- EC-type of examination
- EU declaration of conformity
- Attestation of conformity
- Certificates
- Control drawings
- FMEDA report
- Assessment report
- Additional documents

For more information about functional safety products from Pepperl+Fuchs see www.pepperl-fuchs.com/sil.

1.2 Safety Information

Target Group, Personnel

Responsibility for planning, assembly, commissioning, operation, maintenance, and dismounting lies with the plant operator.

Only appropriately trained and qualified personnel may carry out mounting, installation, commissioning, operation, maintenance, and dismounting of the product. The personnel must have read and understood the instruction manual and the further documentation.

Intended Use

The device is only approved for appropriate and intended use. Ignoring these instructions will void any warranty and absolve the manufacturer from any liability.

The device is developed, manufactured and tested according to the relevant safety standards.

Use the device only

- for the application described
- with specified environmental conditions
- with devices that are suitable for this safety application

Improper Use

Protection of the personnel and the plant is not ensured if the device is not used according to its intended use.

1.3 Symbols Used

This document contains symbols for the identification of warning messages and of informative messages.

Warning Messages

You will find warning messages, whenever dangers may arise from your actions. It is mandatory that you observe these warning messages for your personal safety and in order to avoid property damage.

Depending on the risk level, the warning messages are displayed in descending order as follows:

Danger!
This symbol indicates an imminent danger.

Non-observance will result in personal injury or death.

Warning!
This symbol indicates a possible fault or danger.

Non-observance may cause personal injury or serious property damage.

Caution!
This symbol indicates a possible fault.

Non-observance could interrupt the device and any connected systems and plants, or result in their complete failure.

Informative Symbols

Note!
This symbol brings important information to your attention.

Action

This symbol indicates a paragraph with instructions. You are prompted to perform an action or a sequence of actions.

2016-06

PEPPERL+FUCHS

2 Product Description

2.1 Function

This isolated barrier is used for intrinsic safety applications.

Bi-directional communication is supported for SMART transmitters that use current modulation to transmit data and voltage modulation to receive data.

The outputs are fully isolated from the inputs, the power supply, and each other.

An open field circuit presents a high impedance to the control side to allow alarm conditions to be monitored by control systems.

This device mounts on a HiD Termination Board.

2.2 Interfaces

The device has the following interfaces.

- Safety relevant interfaces:input I to input IV and output I to output IV
- Non-safety relevant interfaces: power supply, collective error message output

Note!

For corresponding connections see datasheet.

2.3 Marking

Pepperl+Fuchs GmbH Lilienthalstraße 200, 68307 Mannheim, Germany

HiD2024	Up to SIL 2

2.4 Standards and Directives for Functional Safety

Device-specific standards and directives

Functional safety	IEC/EN 61508, part 2, edition 2010: Functional safety of electrical/electronic/programmable electronic safety-related systems (manufacturer)

System-specific standards and directives

Functional safety	IEC/EN 61511, part 1 – 3, edition 2003: Functional safety – Safety instrumented systems for the process industry sector (user)

3 Planning

3.1 System Structure

3.1.1 Low Demand Mode of Operation

If there are two control loops, one for the standard operation and another one for the functional safety, then usually the demand rate for the safety loop is assumed to be less than once per year.

The relevant safety parameters to be verified are:

- the PFD_{avg} value (average **P**robability of dangerous **F**ailure on **D**emand) and the T_1 value (proof test interval that has a direct impact on the PFD_{avg} value)
- the SFF value (**S**afe **F**ailure **F**raction)
- the HFT architecture (**H**ardware **F**ault **T**olerance)

3.1.2 High Demand or Continuous Mode of Operation

If there is only one safety loop, which combines the standard operation and safety-related operation, then usually the demand rate for this safety loop is assumed to be higher than once per year.

The relevant safety parameters to be verified are:

- the PFH value (**P**robability of dangerous **F**ailure per **H**our)
- Fault reaction time of the safety system
- the SFF value (**S**afe **F**ailure **F**raction)
- the HFT architecture (**H**ardware **F**ault **T**olerance)

3.1.3 Safe Failure Fraction

The safe failure fraction describes the ratio of all safe failures and dangerous detected failures to the total failure rate.

$SFF = (\lambda_s + \lambda_{dd}) / (\lambda_s + \lambda_{dd} + \lambda_{du})$

A safe failure fraction as defined in IEC/EN 61508 is only relevant for elements or (sub)systems in a complete safety loop. The device under consideration is always part of a safety loop but is not regarded as a complete element or subsystem.

For calculating the SIL of a safety loop it is necessary to evaluate the safe failure fraction of elements, subsystems and the complete system, but not of a single device.

Nevertheless the SFF of the device is given in this document for reference.

3.2 Assumptions

The following assumptions have been made during the FMEDA:

- The device shall claim less than 10 % of the total failure budget for a SIL 2 safety loop.
- For a SIL 2 application operating in low demand mode the total PFD_{avg} value of the SIF (**S**afety **I**nstrumented **F**unction) should be smaller than 10^{-2}, hence the maximum allowable PFD_{avg} value would then be 10^{-3}.
- For a SIL 2 application operating in high demand mode the total PFH value of the SIF should be smaller than 10^{-6} per hour, hence the maximum allowable PFH value would then be 10^{-7} per hour.
- Failure rate based on the Siemens standard SN29500.
- Failure rates are constant, wear is not considered.
- The safety-related device is considered to be of type **A** device with a hardware fault tolerance of **0**.
- Since the safety loop has a hardware fault tolerance of **0** and it is a type **A** device, the SFF must be > 60 % according to table 2 of IEC/EN 61508-2 for a SIL 2 (sub) system.
- The device will be used under average industrial ambient conditions, which are comparable with the classification "stationary mounted" in MIL-HDBK-217F. Alternatively, the following ambient conditions are assumed:
  - IEC/EN 60654-1 Class C (sheltered location) with temperature limits in the range of the manufacturer's specifications and an average temperature of 40 ºC over a long period. The humidity level is within manufacturer's rating. For a higher average temperature of 60 ºC, the failure rates must be multiplied by a factor of 2.5 based on experience. A similar factor must be used if frequent temperature fluctuations are expected.
- The application program in the programmable logic controller (PLC) is configured to detect underrange and overrange failures.
- The devices are not protected against power supply failures. It is within the responsibility of the user to ensure that low supply voltages are detected and adequate reaction on this fault is implemented.

3.3 Safety Function and Safe State

Safe State

The safe state depends on the respective application.

Mostly a value within the signal range is defined, below which (low limit value) or above which (high limit value) the safe state is initiated.

As this individual limit value and this direction are not known to Pepperl+Fuchs, a discrepancy of more than 2 % in the signal path is as worst case rated dangerous undetected. Furthermore, the output values below 3.6 mA or above 21.5 mA indicate failures that are considered as dangerous detected.

Ensure that the programmable controller is programmed to react to these values suitably.

Safety Function

The device transfers an analog signal from the input to the output with a tolerance of 2 % of the measured range.

You have the possibility for each channel to define different functions to fit your safety application.

DIP Switch Settings

Function	Switch settings			
	S1	S2	S3	S4
Analog input with source output 4 mA ... 20 mA	OFF	OFF	OFF	ON
Analog input with source output 1 V ... 5 V	OFF	ON	OFF	ON
Analog input with sink output 4 mA ... 20 mA	OFF	OFF	ON	OFF
Analog output	ON	OFF	ON	OFF

Table 3.1

Potentiometer Settings

You can adjust the signal transfer accuracy via the potentiometers.

Reaction Time

The reaction time for all safety functions is < 100 ms.

Note!

For more information see the corresponding datasheets.

2016-06

PEPPERL+FUCHS

3.4 Characteristic Safety Values

Configure the device for the required function via the DIP switches, see chapter 3.3.

Analog Input Function

Parameters acc. to IEC 61508	Characteristic values
Assessment type and documentation	FMEDA report
Device type	A
Mode of operation	Low Demand Mode or High Demand Mode
HFT	0
SIL (SC)	2
Safety function	Signal transfer to programmable logic controller (PLC)
λ_s	0 FIT
λ_{dd}	121 FIT
λ_{du}	49.9 FIT
$\lambda_{total\ (safety\ function)}$	171 FIT
$\lambda_{not\ part}$	59 FIT
SFF [1]	70 %
PTC	100 %
MTBF [2]	314 years
PFH	4.99×10^{-8} 1/h
PFD_{avg} for T_1 = 1 year	2.18×10^{-4}
PFD_{avg} for T_1 = 2 years	4.37×10^{-4}
PFD_{avg} for T_1 = 5 years	1.03×10^{-3}
Reaction time	< 100 ms

Table 3.2

1 "Not considered" failures are considered 50 % as dangerous undetected and 50 % as "No effect". "No effect" failures are not influencing the safety functions and are therefore not included in the calculation of the SFF.

2 acc. to SN29500. This value includes failures which are not part of the safety function/MTTR = 8 h. This value is calculated for one safety function of a device.

Analog Output Function

Parameters acc. to IEC 61508	Characteristic values
Assessment type and documentation	FMEDA report
Device type	A
Mode of operation	Low Demand Mode or High Demand Mode
HFT	0
SIL (SC)	2
Safety function	Signal transfer to field device
λ_s	0 FIT
λ_{dd}	108 FIT
λ_{du}	70 FIT
$\lambda_{total\ (safety\ function)}$	178 FIT
$\lambda_{not\ part}$	43 FIT
SFF [1]	60.7 %
PTC	100 %
MTBF [2]	314 years
PFH	6.98×10^{-8} 1/h
PFD_{avg} for T_1 = 1 year	3.06×10^{-4}
PFD_{avg} for T_1 = 2 years	6.12×10^{-4}
PFD_{avg} for T_1 = 5 years	1.53×10^{-3}
Reaction time	< 100 ms

Table 3.3

1 "Not considered" failures are considered 50 % as dangerous undetected and 50 % as "No effect". "No effect" failures are not influencing the safety functions and are therefore not included in the calculation of the SFF.

2 acc. to SN29500. This value includes failures which are not part of the safety function/MTTR = 8 h. This value is calculated for one safety function of a device.

The characteristic safety values like PFD, SFF, HFT and T_1 are taken from the SIL report/FMEDA report. Observe that PFD and T_1 are related to each other.

The function of the devices has to be checked within the proof test interval (T_1).

3.5 Useful Life Time

Although a constant failure rate is assumed by the probabilistic estimation this only applies provided that the useful lifetime of components is not exceeded. Beyond this useful lifetime, the result of the probabilistic estimation is meaningless as the probability of failure significantly increases with time. The useful lifetime is highly dependent on the component itself and its operating conditions – temperature in particular. For example, the electrolytic capacitors can be very sensitive to the operating temperature.

This assumption of a constant failure rate is based on the bathtub curve, which shows the typical behavior for electronic components.

Therefore it is obvious that failure calculation is only valid for components that have this constant domain and that the validity of the calculation is limited to the useful lifetime of each component.

It is assumed that early failures are detected to a huge percentage during the installation and therefore the assumption of a constant failure rate during the useful lifetime is valid.

However, according to IEC/EN 61508-2, a useful lifetime, based on general experience, should be assumed. Experience has shown that the useful lifetime often lies within a range period of about 8 ... 12 years.

As noted in DIN EN 61508-2:2011 note N3, appropriate measures taken by the manufacturer and plant operator can extend the useful lifetime.

Our experience has shown that the useful lifetime of a Pepperl+Fuchs product can be higher

- if there are no components with reduced life time in the safety loop (for example electrolytic capacitors, relays, flash memories, optocoupler) which can produce dangerous undetected failures and
- if the ambient temperature is significantly below 60 °C.

Please note that the useful lifetime refers to the (constant) failure rate of the device. The effective life time can be higher.

4 Mounting and Installation

Installing the device

1. Observe the safety instructions in the instruction manual.
2. Observe the information in the manual.
3. Observe the requirements for the safety loop.
4. Connect the device only to devices that are suitable for this safety application.
5. Check the safety function to ensure the expected output behavior.

4.1 Configuration

Configuring the Device Function

The function of the device is configured via DIP switches. The DIP switches are on the side of the device.

1. De-energize the device before configuring the device.
2. Remove the device.
3. Configure the device for the required function via the DIP switches, see chapter 3.3.
4. Secure the DIP switches to prevent unintentional adjustments.
5. Mount the device.
6. Connect the device again.

Adjusting the Signal Transfer of the Device

You can adjust the signal transfer accuracy via the potentiometers. The potentiometers are on the front of the device.

1. Configure the device for the required function via the DIP switches, see above and chapter 3.3.
2. Open the cover.
3. Calibrate the current transfer via the potentiometer.
4. Secure the potentiometers to prevent unintentional adjustments.
5. Close the cover.

Note!

For more information see the corresponding datasheets.

5 Operation

Danger!

Danger to life from missing safety function

If the safety loop is put out of service, the safety function is no longer guaranteed.

- Do not deactivate the device.
- Do not bypass the safety function.
- Do not repair, modify, or manipulate the device.

Operating the device

1. Observe the safety instructions in the instruction manual.
2. Observe the information in the manual.
3. Use the device only with devices that are suitable for this safety application.
4. Correct any occurring safe failures within 8 hours. Take measures to maintain the safety function while the device is being repaired.

5.1 Proof Test Procedure

According to IEC/EN 61508-2 a recurring proof test shall be undertaken to reveal potential dangerous failures that are not detected otherwise.

Check the function of the subsystem at periodic intervals depending on the applied PFD_{avg} in accordance with the characteristic safety values.
See chapter 3.4.

It is under the responsibility of the plant operator to define the type of proof test and the interval time period.

Equipment required:

- Digital multimeter with an accuracy better than 0.1 %

  Use for the proof test of the intrinsic safety side of the device a special digital multimeter for intrinsically safe circuits.

  If intrinsically safe circuits are operated with non-intrinsically safe circuits, they must no longer be used as intrinsically safe circuits.
- Variable power supply 0 V DC ... 24 V DC
- Load with
  - max. 300 Ω for analog input function with current output
  - min. 1 MΩ for analog input function with voltage output
  - max. 650 Ω for analog output function
- Process calibrator with current source and current sink function with an accuracy better than 20 µA

Proof Test Procedure

1. Put out of service the entire safety loop. Protect the safety application by means of other measures.
2. Prepare a test set-up, see figures below.
3. Test the devices in the mode of operation they are used in. If necessary, change the configuration of the device. Verify the input and output values as given in table below.
4. Set back the device to the original settings for the application after the test.

Step No.	Input value (mA)	Measurement point	
		Output value (mA)	Output value (V)
1	20.00	20.00 ± 0.4	5.00 ± 0.1
2	12.00	12.00 ± 0.4	3.00 ± 0.1
3	4.00	4.00 ± 0.4	1.00 ± 0.1
4	23.00	23.00 ± 0.4	5.75 ± 0.1
5	0	< 0.3	< 0.1

Table 5.1 Steps to be performed for the proof test

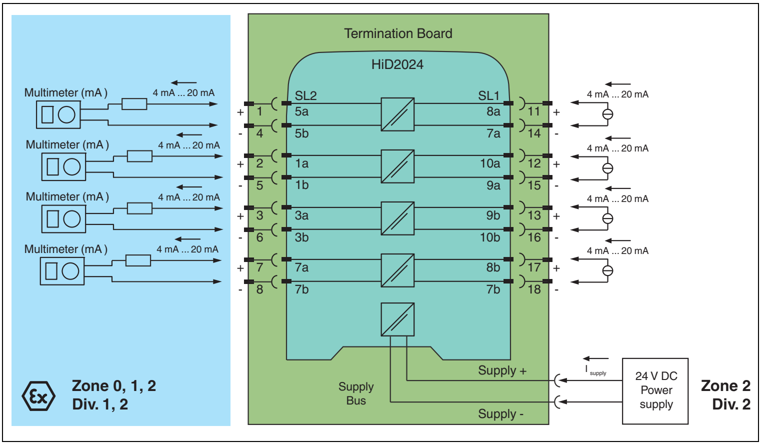


Figure 5.1 Proof test set-up for HiD2024 with analog output function

2016-06

PEPPERL+FUCHS

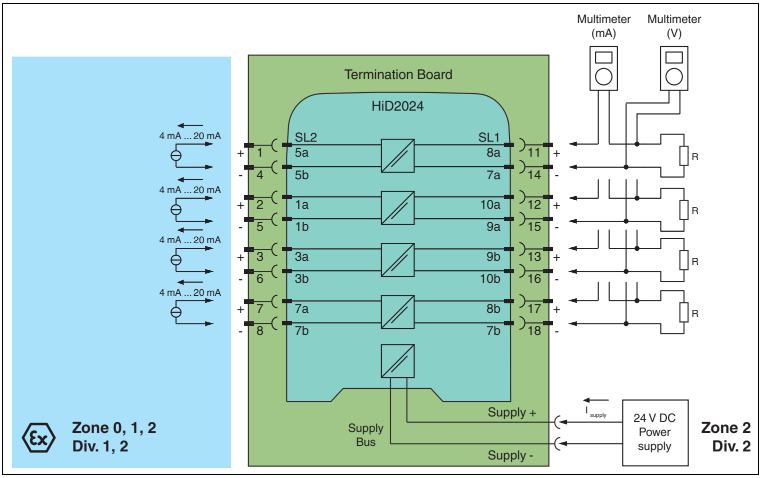


Figure 5.2 Proof test set-up for HiD2024 with analog input function with current source or voltage source output

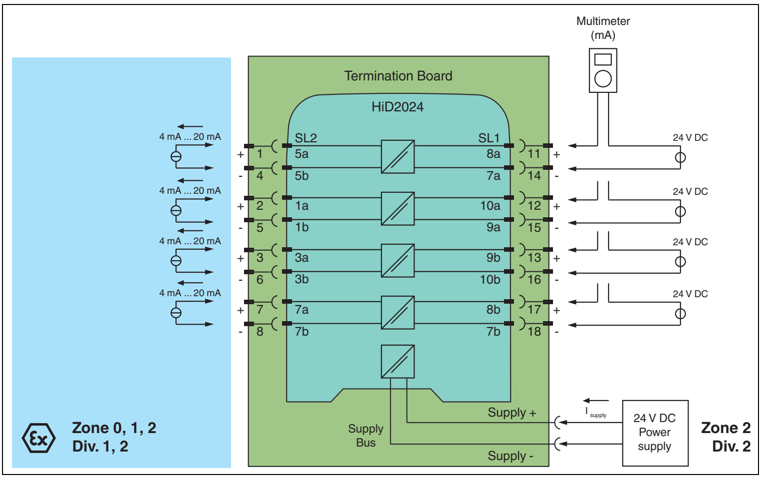


Figure 5.3 Proof test set-up for HiD2024 with analog input function with current sink

Tip

The easiest way to test HiD devices by using a stand-alone HiDTB**-SCT-***-**-** termination board. In this test, it is not necessary to disconnect the wiring of the existing application. Faults in a subsequent wiring can be avoided.

6 Maintenance and Repair

Danger!

Danger to life from missing safety function

If the safety loop is put out of service, the safety function is no longer guaranteed.

- Do not deactivate the device.
- Do not bypass the safety function.
- Do not repair, modify, or manipulate the device.

Maintaining, Repairing or Replacing the Device

In case of maintenance, repair or replacement of the device, proceed as follows:

1. Implement appropriate maintenance procedures for regular maintenance of the safety loop.
2. Ensure the proper function of the safety loop, while the device is maintained, repaired or replaced.
   If the safety loop does not work without the device, shut down the application.
   Do not restart the application without taking proper precautions.
   Secure the application against accidental restart.
3. Do not repair a defective device. A defective device must only be repaired by the manufacturer.
4. Replace a defective device only by a device of the same type.

7 Abbreviations

ESD	**E**mergency **S**hut**d**own
FIT	**F**ailure **I**n **T**ime in 10^{-9} 1/h
FMEDA	**F**ailure **M**ode, **E**ffects, and **D**iagnostics **A**nalysis
λ_s	Probability of safe failure
λ_{dd}	Probability of dangerous detected failure
λ_{du}	Probability of dangerous undetected failure
$\lambda_{no\ effect}$	Probability of failures of components in the safety loop that have no effect on the safety function. The no effect failure is not used for calculation of SFF.
$\lambda_{not\ part}$	Probability of failure of components that are not in the safety loop
$\lambda_{total\ (safety\ function)}$	Safety function
HFT	**H**ardware **F**ault **T**olerance
MTBF	**M**ean **T**ime **B**etween **F**ailures
MTTR	**M**ean **T**ime **T**o **R**estoration
PCS	**P**rocess **C**ontrol **S**ystem
PFD$_{avg}$	Average **P**robability of dangerous **F**ailure on **D**emand
PFH	Average frequency of dangerous failure
PTC	**P**roof **T**est **C**overage
SFF	**S**afe **F**ailure **F**raction
SIF	**S**afety **I**nstrumented **F**unction
SIL	**S**afety **I**ntegrity **L**evel
SIL (SC)	**S**afety **I**ntegrity **L**evel (**S**ystematic **C**apability)
SIS	**S**afety **I**nstrumented **S**ystem
T$_1$	Proof Test Interval
PLC	**P**rogrammable **L**ogic **C**ontroller

PROCESS AUTOMATION – PROTECTING YOUR PROCESS

Worldwide Headquarters
Pepperl+Fuchs GmbH
68307 Mannheim · Germany
Tel. +49 621 776-0
E-mail: info@de.pepperl-fuchs.com

For the Pepperl+Fuchs representative
closest to you check www.pepperl-fuchs.com/contact

www.pepperl-fuchs.com

PEPPERL+FUCHS
PROTECTING YOUR PROCESS

DOCT-4821A
06/2016