TÜVRheinland®
Precisely Right.

Automation - Functional Safety

Report about the evaluation of the DDE-2745 relay modules

Report-No.: 968/FSP 1538.00/17
Date: 2017-12-12

Report about the evaluation of the DDE-2745 relay modules

Report-No.:	968/FSP 1538.00/17
Date:	2017-12-12
Number of pages (excl. appendices):	10
Product	DDE-2745 Relay Modules: KFD2-RSH-1.2E.L2 (ETS) KFD2-RSH-1.2D.FL2 (DTS) KFD2-RSH-1.2E.L3 (ETS) KFD2-RSH-1.2D.FL3 (DTS)
Customer/Manufacturer:	Pepperl+Fuchs GmbH Lilienthalstraße 200 68307 Mannheim Germany
Customer-Order-No. / Date:	1897706 dated 2017-06-08
Certification Body:	TÜV Rheinland Industrie Service GmbH Automation - Functional Safety (A-FS) Am Grauen Stein 51105 Köln Germany
TÜV-Quotation-No./Date:	8421765 dated 2017-05-24
TÜV-Order-No./Date:	0125182064 dated 2017-06-08
Assessor/Expert:	Dipl.-Ing. Björn Callsen
Duration:	May 2017 - November 2017

The results are exclusively related to the product/project.

Contents **Page**

1. Scope

This report summarises the results of the assessment of the DDE-2745 relay modules series.

The DDE-2745 relay modules series consists of two basic variants DTS and ETS. The DTS (de-energized to safe) module turns the output off, when the safety function needs to be executed. The ETS (energized to safe) module turns the output on, when the safety function needs to be executed.

The DTS relay modules are to be assessed for the fulfilment of the requirements of IEC 61508 (low and high demand mode of operation), IEC 62061 and ISO 13849, the ETS relay modules for IEC 61508 (low and high demand mode of operation) only.

2. Standards forming the basis for the requirements

[N1] IEC 61508 Part 1 - 7:2010
Functional safety of electrical/electronic/programmable electronic safety-related systems

[N2] IEC 62061:2015
Safety of machinery-Functional safety of safety-related electrical, electronic and programmable electronic control systems

[N3] ISO 13849-1:2015
Safety of machinery-Safety-related parts of control systems
Part 1: General principles for design

[N4] EN 61010-1:2010
Safety requirements for electrical equipment for measurement, control and laboratory use – Part1: General requirements

3. Identification of the product

3.1. Description of the device under assessment

The DTS Variants provide a galvanic isolation between field circuits and control circuits. The safe state is the de-energized state corresponding to open relay outputs.

The ETS Variants provide also a galvanic isolation between field circuits and control circuits, but the safe state is the energized state corresponding to closed relay outputs.

The relay modules are described in more detail in the PRS [U3].

Type code	Output	HW Version	SW Version
KFD2-RSH-1.2E.L2 (ETS)	24VDC	HW01.08	01.0.0
KFD2-RSH-1.2D.FL2 (DTS)	24VDC	HW29.05	01.0.0
KFD2-RSH-1.2E.L3 (ETS)	230VAC	HW01.08	01.0.0
KFD2-RSH-1.2D.FL3 (DTS)	230VAC	HW01.08	01.0.0

Table 1 :DDE-2745 variants

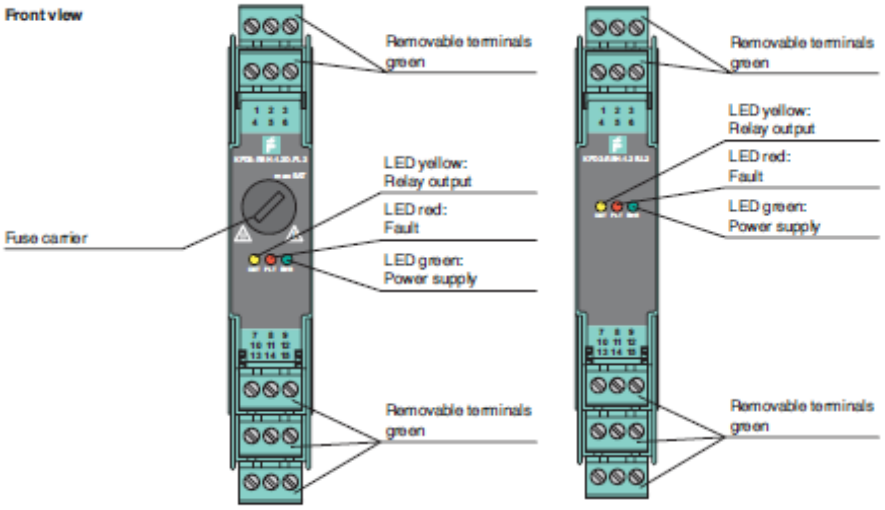

Figure 1: DTS ETS

3.2. Documents provided by the customer

[U1]	DL_P+F_DDE-2745 List of Documents	Version A3
[U2]	SC_P+F_DDE-2745 Safety Concept	Version E
[U3]	PRS_P+F_DDE-2745.docx Product Requirement Specification	Version H
[U4]	FMEDA_P+F_DDE-2745_DTS DTS FMEDA	Version D
[U5]	FMEDA_P+F_DDE-2745_ETS ETS FMEDA	Version D
[U6]	ETS and DTS schematics 019787c.pdf 019849b.pdf	 Version C Version B
[U7]	HDD_P+F_DDE-2745 Hardware Design Description	Version B
[U8]	PTS_P+F_DDE-2745 Product Test Specification	Version D
[U9]	PVP_P+F_DDE-2745 Product Verification Plan	Version C
[U10]	PTR_P+F_DDE-2745 Product Test Report inclusive Fault Insertion Test	Version B
[U11]	FSMP_P+F_DDE-2745 Functional Safety Plan	Version C
[U12]	RC_P+F_DDE-2745 Requirement Tracking Excel File	Version B
[U13]	EMC test reports Testreport_EMV_DDE2745_prdebu59.pdf	
[U14]	Environmental test report, Electrical Safety Testreport_Elmech_DDE2754_prdebu39b.pdf	

[U15] Testselection for Environmental, EMC, Electrical safety
Testselection_DDE2745_prdebcn2c.pdf

[U16] FAM_P+F_DDE-2745 Version C
Fault avoidance measures

[U17] SMHW_P+F_DDE-2745 Version C
Tables A15-17, B1-B5

[U18] Coding_Guideline_P+F_DDE-2745.docx Version C
Coding_Guideline_P+F_DDE-2745_SIGNED.pdf
Coding Guideline + Review

[U19] Requirements_Software_DDE2745 n/v
Requirement Listing Software

[U20] CCP.xlsm CCP_P+F_DDE-2745_SIGNED.pdf Version A
Code Control Plan + Freigabe

[U21] CRR_Code_Review_Report_main.xlsm n/a
Exemplary code review file

[U22] PRDE-BYC4.docx n/v
Produktfreigabe Dokument

[U23] Exemplary Datasheet, System Manual, Instruction Manual
274893_ger_KFD2-RSH-1.2D.FL2.pdf 2017.10.06
tdoct5831a_eng.pdf 2017-10
K-System.pdf 2014-10

[U24] Safety Manuals
tdoct5815__eng.pdf 2017-10
tdoct5816__eng.pdf 2017-11

A complete list of the provided documents can be found in [U1].

3.3. Documents compiled by TÜV Rheinland

[U25] LOP_DDE2745_Pepperl_Embex_Rev1.12 Version 1.12
List of open Points

[U26] FIT_Bericht_DDE2745_V1.0 Version 1.0
Functional Tests, Fault Insertion Tests

3.4. Test samples

KFD2-RSH-1.2E.L2	6784368
KFD2-RSH-1.2D.L2	4188040

Table 2: DDE-2745 test samples

The test samples from the functional test [U26] conducted on 2017-11-24 at the Test Institute with designations as in table 2 will be archived by the Test Institute.

4. Objects and results of the assessment

4.1. General

The measuring and test equipment, which has been used by the TÜV Rheinland Group in the tests described in the following, is subject to regular inspection and calibration. Only devices with valid calibration have been used. The devices used in the various tests are recorded in the inspector´s documentation.

All considerations concerning uncertainty of the measurements, so far applicable, are stated in the inspector´s documentation, too.

In cases where tests have been executed in an external test lab or in the test lab of the manufacturer and where the results of these tests have been used within the here documented approval, this has occurred after a positive assessment of the external test lab and the achieved test results in detail according to the Quality Management procedure QMA 3.310.05.

4.2. Assessment of the safety structure

4.2.1. Assessment for the variant DTS

The variant DTS is typically connected to a safety related output card (DO card) of a safety PLC. The variant DTS provides a single channel input structure. The output structure consists of three electromechanical relays, whose NO contacts are connected in series, switching a single output terminal. The output terminal typically controls connected field devices. This variant is composed of Type A components.

A FMEA has been performed by the manufacturer in order to determine the SFF for the device, see [U4]. The FMEA shows that the input structure (HFT = 0) achieves an SFF>90%. The output structure can be considered to be mainly of HFT = 2 and achieves an SFF>60%. The requirements for SIL 3 for the structure according to IEC 61508 are therefore fulfilled. The results of the FMEA are accepted by the Test Institute.

4.2.2. Assessment for the variant ETS

The variant ETS is typically connected to a safety related output card (DO card) of a safety PLC. The variant ETS provides a single channel input structure. The output structure consists of three electromechanical relays, whose NO contacts are connected in parallel, switching a single output terminal. The output terminal typically controls connected field devices. This variant is composed of Type A components.

A FMEA has been performed by the manufacturer in order to determine the SFF for the device, see [U5]. The FMEA shows that the input structure (HFT = 0) achieves an SFF>90%. The output structure can be considered to be mainly of HFT = 2 and achieves an SFF<60%. The requirements for SIL 3 for the structure according to IEC 61508 are therefore fulfilled. The results of the FMEA are accepted by the Test Institute.

4.3. Assessment of the behaviour if faults occur and determination of the safety related reliability

4.3.1. Assessment for the variant DTS

The variant DTS contains diagnostic measures such as monitoring the output for short circuits and open circuits of connected field devices (external diagnostics) and monitoring of failures of the internal relays (internal diagnostics).

For the low demand mode of operation a manual proof test can be conducted in order to detect dangerous undetected failures.

In high demand DTS applications it is recommended to switch on the internal and external diagnosis and to evaluate either the fault indication output or to monitor the test pulse from the DO card connected to the input of the relay.

The manufacturer has performed a FMEDA, see [U4]. The FMEDA shows the following results:

PFH = 8.6 E-10 1/h

PFD_{avg} = 1.12 E-5 for a Proof Test Interval of 3 years

PFD_{avg} = 7.5 E-6 for a Proof Test Interval of 2 years

PFD_{avg} = 3.8 E-6 for a Proof Test Interval of 1 years

If the required monitoring measures are implemented by the user a diagnostic coverage of 95 % can be achieved.

The results show that the requirements for the safety related reliability for SIL 3 are fulfilled. The results of the FMEDA are accepted by the Test Institute.

4.3.2. Assessment for the variant ETS

The variant ETS contains diagnostic measures such as monitoring the output for short circuits and open circuits of connected field devices (external diagnostics) and monitoring of failures of the internal relays (internal diagnostics).

For the low demand mode of operation a manual proof test can be conducted in order to detect dangerous undetected failures.

In high demand ETS applications the internal and external diagnosis shall be switched on. It is required that the fault indication output is evaluated and that the test pulse from the DO card connected to the input of the relay is monitored.

Additionally the input of the ETS shall always be monitored by the safety PLC (e.g. DO card) for open circuits as these failures are not covered by the internal diagnosis of the device.

If the diagnostics (internal and external) is not activated equivalent measures shall be implemented by the user such as monitoring the output signal for short and open circuits and/or using redundant power supplies.

The manufacturer has performed a FMEDA, see [U5]. The FMEDA shows the following results:

PFH = 3.5 E-9 1/h

PFDavg = 4.6 E-5 for a Proof Test Interval of 3 years

PFD_{avg} = 3.0 E-5 for a Proof Test Interval of 2 years

PFD_{avg} = 1.5 E-5 for a Proof Test Interval of 1 years

If the appropriated diagnostic measures (internal and external) and additionally the monitoring of the input for open circuits are implemented a diagnostic coverage of 81 % can be achieved.

The results show that the requirements for the safety related reliability for SIL 3 are fulfilled. The results of the FMEDA are accepted by the Test Institute.

4.4. Assessment of the systematic capability

4.4.1. Assessment of applied measures for fault avoidance

The assessment of the techniques to avoid systematic failures during the different phases of the lifecycle has shown that sufficient measures have been implemented in order to fulfil the requirements for SIL 3, see [U16] and [U17].

4.4.2. Assessment of the systematic safety integrity for the variant DTS

The assessment of the implemented measures for the control of systematic failures has shown that sufficient measures have been implemented in order to fulfil the requirements for SIL 3, see [U17].

4.4.3. Assessment of the systematic safety integrity for the variant ETS

The assessment of the implemented measures for the control of systematic failures has shown that sufficient measures have been implemented in order to fulfil the requirements for SIL 3, if the system is being operated in the low demand mode of operation.

If suitable additional measures are implemented by the user in order to control systematic failures such as the use of redundant power supplies and monitoring of the input for short circuits and open circuits, etc. the variant ETS can be used in SIL 3 systems in the high demand mode of operation.

4.5. Assessment according to IEC 62061 and ISO 13849-1

4.5.1. Assessment of the variant DTS

The variant DTS fulfils the requirements for SIL 3 according to IEC 61508, see chapters 4.2 to 4.4. It can therefore be concluded that the variant DTS can also be used in applications according to IEC 62061 up to SIL 3.

Due to the equivalence of IEC 62061 and ISO 13849-1 it can be concluded that the variant DTS also fulfils the requirements for PL e according to ISO 13849-1.

4.5.2. Assessment of the variant ETS

The standards IEC 62061 and ISO 13849-1 require that safety devices are implemented according to the idle current principle. As the ETS variant is implemented following the working current principle no safety classification according to IEC 62061 and ISO 13849-1 will be done for this variant within this type assessment.

In case the ETS is intended to be used in machinery safety functions, the specific application has to be assessed individually and it has to be shown that an equivalent safety level will be achieved.

4.6. Assessment of the software used for diagnostic measures

The software is used for diagnostic measures and is not part of the safety function, meaning when the software fails the safety function can still be executed.

The requirements for the software are specified in [U19]. The code was designed under the consideration of coding rules, mainly MISRA and implemented accordingly (see [U18]). Code reviews have been performed with a positive result (see [U20]).

The implemented diagnostic measures have been verified with a positive result by the manufacturer and the Test Institute (see 4.7).

4.7. Conduction of functional and fault insertion tests

The manufacturer has conducted functional tests and fault insertion tests, see [U8] and [U10]. The Test Institute has done selected functional and fault insertion tests in order to confirm the findings from the testing, see [U26]. The test results show that the required functionality and the required diagnostics have been properly implemented.

4.8. Assessment of environmental tests

The climatic and mechanical tests were performed by the manufacturer. The review of the provided test report has shown that the environmental requirements according to EN 60068-2-x (see [U14]) are fulfilled. The test results are accepted by the Test Institute.

4.9. Assessment of EMC tests

The EMC tests were performed by the manufacturer. The review of the provided test report has shown that the EMC requirements according to EN 61326-1, EN 61326-3-1 and EN 61326-3-2 (see [U13]) are fulfilled. The test results are accepted by the Test Institute.

4.10. Assessment of the electrical safety

The testing according to the requirements of [N4] was performed by the manufacturer, see [U14]. The test results show that the requirements for the electrical safety are fulfilled. The test results are accepted by the Test Institute.

4.11. Review of the user documentation

A review has been performed concerning the information for the safe installation and safe usage of the devices. It can be confirmed that the datasheet, K-system description, installation manual and safety manuals ([U24]) contain the information necessary for the safe installation and operation of the DDE-2745 relay modules.

5. Summary

The assessment of the relay modules of the DDE-2745 series came to the following conclusions. The relay modules fulfil the requirements of the above listed standards, see chapter 2. The relay modules can be classified as follows:

Variant DTS:

SIL 3 according to IEC 61508 for low and high demand mode of operation, SIL CL 3 according to IEC 62061, PL e according to ISO 13849-1.

Variant ETS:

SIL 3 according to IEC 61508 for low demand mode of operation

SIL 3 according to IEC 61508 for high demand mode of operation, if the measures described in chapter 4.3.2 and 4.4.3 are implemented by the user. The required measures are described in the associated safety manual for the variant ETS, see [U23].

The instructions of the associated safety manual, the K-system description, the instruction manual and the datasheet shall be followed.

Cologne, 2017-12-12
TIS/A-FS/Kst. 968 ca-nie

Report released after review:
Date: 2017-12-12

The assessor

Dipl. Ing. Björn Callsen

Dr. Peter Robben