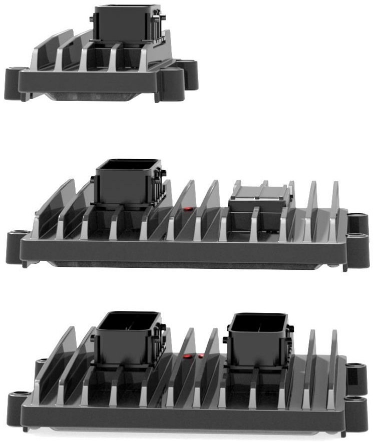
Functional Safety in Mobile Machinery

Achieving functional safety without compromising performance with IQAN controllers

ENGINEERING YOUR SUCCESS.

February 11, 2022

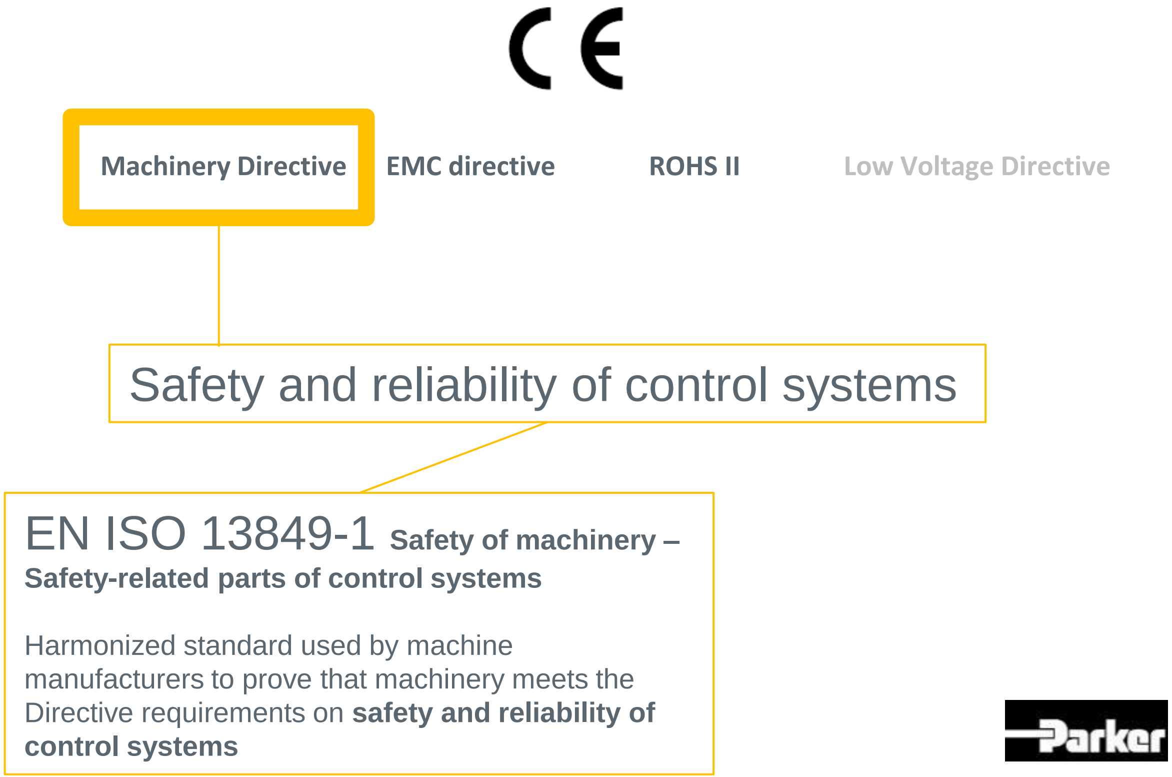
Mobile machinery – applications for IQAN-MC4xFS



Application	Application safety standard
Aerial platform	EN 280
Refuse rear loader	EN 1501-1
Refuse side loader	EN 1501-2
Refuse front loader	EN 1501-3
Refuse bin lift	EN 1501-5
Steer-by-wire	ISO 5010
Reach stacker LLMC	EN 15000
Lift truck	EN 1175
Loader crane	EN 12999
Telehandler LLMC	EN 15000
Forestry machinery	EN ISO 11850
Construction machinery	EN 474-1, ISO 19014
…	

CE marking of machinery

- control system aspects



Machinery Directive

EMC directive

ROHS II

Low Voltage Directive

Safety and reliability of control systems

EN ISO 13849-1 **Safety of machinery – Safety-related parts of control systems**

Harmonized standard used by machine manufacturers to prove that machinery meets the Directive requirements on **safety and reliability of control systems**

The Machinery directive states:

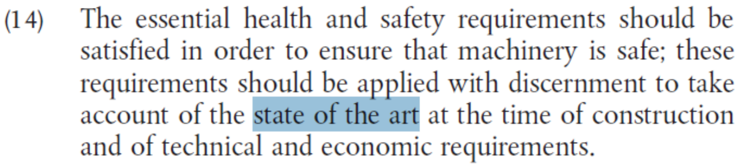
Safety and reliability of control systems

- Control systems must be designed and constructed in such a way as to prevent hazardous situations from arising. Above all, they must be designed and constructed in such a way that:
  - they can withstand the intended operating stresses and external influences,
  - **a fault in the hardware or the software of the control system does not lead to hazardous situations,**
  - **errors in the control system logic do not lead to hazardous situations,**
  - reasonably foreseeable human error during operation does not lead to hazardous situations.

Directive 2006/42/EC, Annex 1, clause 1.2.1.

State of the art is evolving

The Machinery Directive* states:

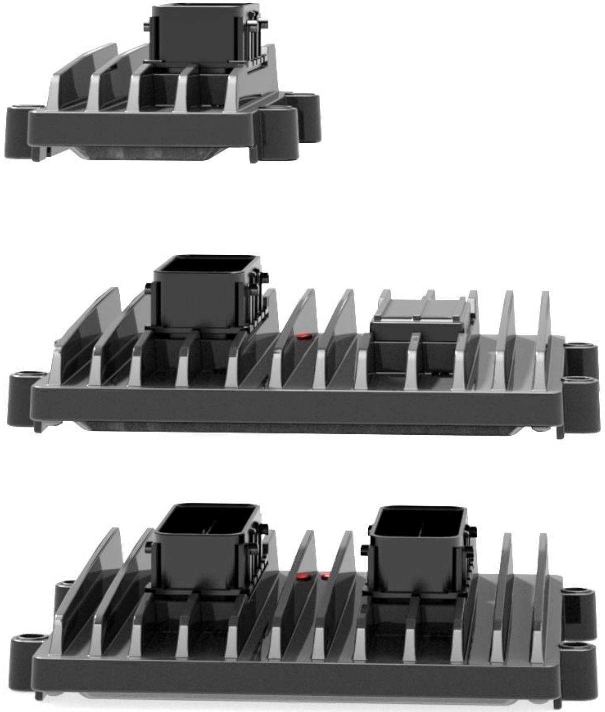


(14) The essential health and safety requirements should be satisfied in order to ensure that machinery is safe; these requirements should be applied with discernment to take account of the state of the art at the time of construction and of technical and economic requirements.

Mobile machinery application specific standards evolve; with increased level of detail on control system requirements. Most include reference to EN 13849-1 Performance Levels on specific **safety functions**.

*** Directive 2006/42/EC**

IQAN-MC4xFS



For applications requring IEC 61508 **SIL2** / EN ISO 13849-1 **PLd**

- Used where safety relies on **de-energizing** the coils on hydraulic valves
- Normal functions and **safety functions** can be implemented in the same module

Scalable design

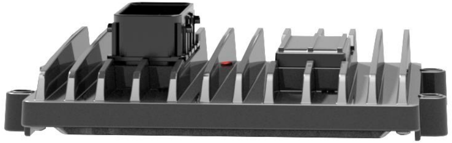
- **MC41FS** for one or two safety functions
- **MC42FS** higher number of safe outputs
- **MC43FS** large centralized controller for several safety functions

IQAN-XC4x expansions

IQAN-XC43, -XC42 and -XC41 designed for I/O expansion in safety functions
Use with IQAN master module; IQAN-MC4xFS in safety functions

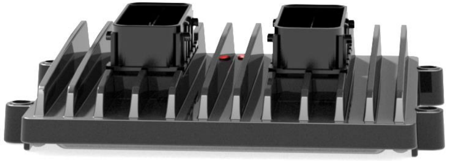
Design

- Built upon the MC4x controller hardware
- Built upon the MC4xFS controller software



Features

- Safe CAN protocol
- CAN protocol supporting classic CAN and CAN FD
- Firmware update in field
- Safety certified by RISE



Safety function

“function of the machine whose failure can result in an immediate increase of the risk(s)”

EN ISO 12100-1

Structure of a safety function

Input subsystem

Logic subsystem

IQAN-MC43

Output subsystem

Examples of safety functions

- Examples from EN ISO 13849-1
  - start/restart function
  - hold-to-run function
  - enabling device function
  - control modes and mode selection
  - Emergency stop function (complimentary protective measure).

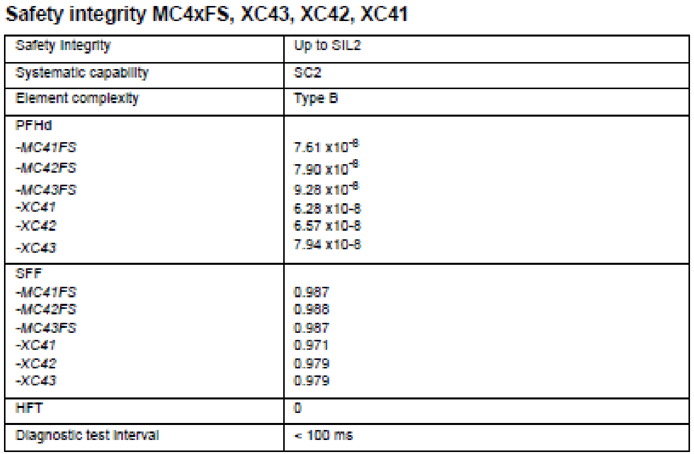
Standards used for implementing safety functions

- **IEC 61508**
  - Used in different industries, including machinery
  - High focus on development process and detailed analysis
  - Well suited for developing subsystems with complex electronics and embedded software

- **EN ISO 13849-1**
  - Specific to machinery
  - High focus on hardware architecture, allows for estimates on diagnostics, covers also hydraulics, somewhat limited in requirements on software
  - Can bring in IEC 61508 subsystems as safety related parts
  - Well suited for complete safety function

IEC 61508

- The gold standard for **functional safety** in electrical, electronic and **programmmable electronic systems**
  - Foundation for other application area international standards
- **Safety integrity levels, SIL 1 to SIL 4**
  - Hardware safety integrity, quantifying effect of random failures (PFHd)
    - Robust components, architecture, hardware diagnostics
  - Systematic capability
    - Development process, software design, EMI, ..



Safety integrity MC4xFS, XC43, XC42, XC41

Safety Integrity	Up to SIL2
Systematic capability	SC2
Element complexity	Type B
PFHd *-MC41FS* *-MC42FS* *-MC43FS* *-XC41* *-XC42* *-XC43*	 $7.61\ x10^{-8}$ $7.90\ x10^{-8}$ $9.28\ x10^{-8}$ 6.28 x10-8 6.57 x10-8 7.94 x10-8
SFF *-MC41FS* *-MC42FS* *-MC43FS* *-XC41* *-XC42* *-XC43*	 0.987 0.988 0.987 0.971 0.979 0.979
HFT	0
Diagnostic test interval	< 100 ms

EN ISO 13849-1

- For functional safety in **machinery,** applicable to electrical, programmable electronic, hydraulic, pneumatic and mechanical.
  - Referenced by mobile machinery C-standards, often specifying safety functions with PL c and PL d.
- **Performance Level (PL) Levels PL a to PL e**, evaluated based on:
  - Quantifiable aspect of PL, hardware reliability modelling based on
    - Architecture (categories B, 1, 2, 3 or 4)
    - MTTFd of components
    - Diagnostics (DC)
    - Common cause failures (CCF)
  - Non-quantifiable aspects
    - Safety related software (SRASW, SRESW)
    - Avoidance of systematic faults
    - Environmental robustness

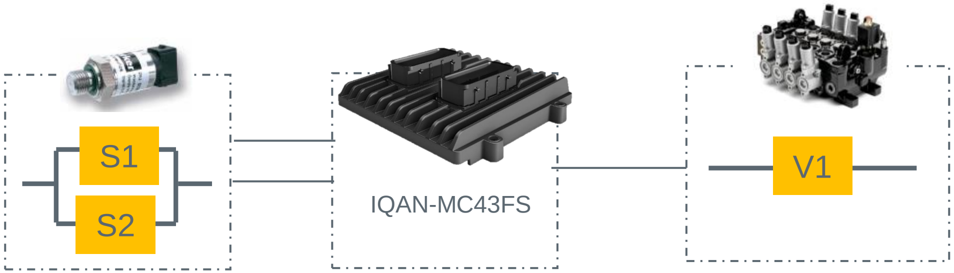
EN ISO 13849-1:2015

solutions depending on required PL

EN 13849-1 **PL**	IEC 61508 **SIL**	EN 13849-1 **hardware electronics**	EN 13849-1 **safety related embedded SW**
a	-	Basic safety principles (category B)	Basic requirements only
b	1	MTTFd on controllers and sensors	Basic requirements only
c	1	Category 2 or 3, MTTFd, DC, CCF *or* IEC 61508 SIL 1	EN 13849-1 4.6.2 *or* IEC 61508 SIL 1
d	2	Category 2 or 3, MTTFd, DC, CCF *or* **IEC 61508 SIL 2**	EN 13849-1 4.6.2 *or* **IEC 61508 SIL 2**
e	3	Category 3 or 4, MTTFd, DC, CCF *or* IEC 61508 SIL 3	IEC 61508-3 SIL 3

EN ISO 13849-1

Combining subsystems



Sensors initiating safety function

Evaluate with EN 13849-1

- Combine two redundant sensors to Category 3
- Component MTTFd from datasheet (e.g. IQAN-SP500)
- Evaluate DC and CCF
- Calculate PL =

Logic unit

Already certified to

IEC 61508 **SIL2**

PL = **PL d**

Directional valve

Evaluate with EN 13849-1

Reliable non-complex

Category 1

PL = **PL c**

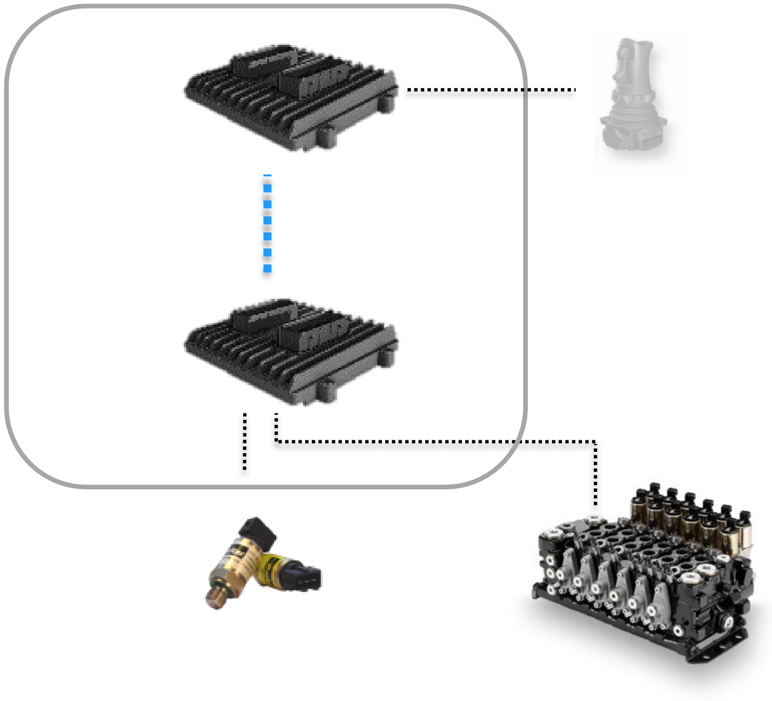
Safety function on multiple modules

CAN

I/O signals

Master, IQAN-MC43FS

Expansion, IQAN-XC43



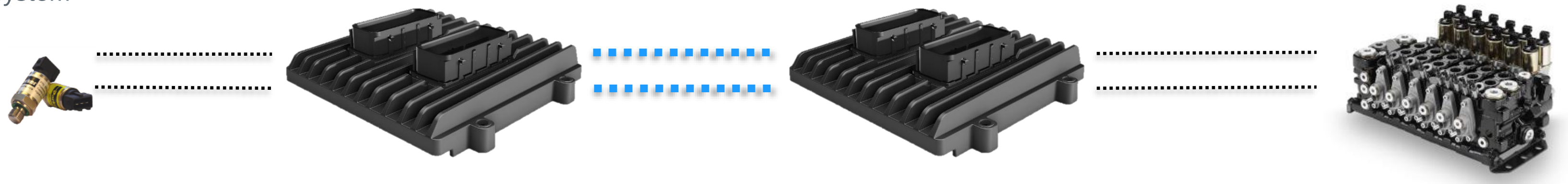
Combination of subsystems
IQAN-MC4xFS with IQAN-XC4x expansion module

Input subsystem

Logic subsystem

I/O expansion subsystem

Output subsystem



Sensors

Analog inputs

Design to EN ISO 13849-1

Evaluate PL and PFHd

IQAN-MC43FS

Logic unit

IEC 61508 SIL2 =>**PLd**

PFHd = **9.29*10^{-8}**

IQAN-XC43FS

“Logic unit” (I/O expansion)

IEC 61508 SIL2 =>**PLd**

PFHd = **7.94*10^{-8}**

From IQANdesign 6.07

Directional valve

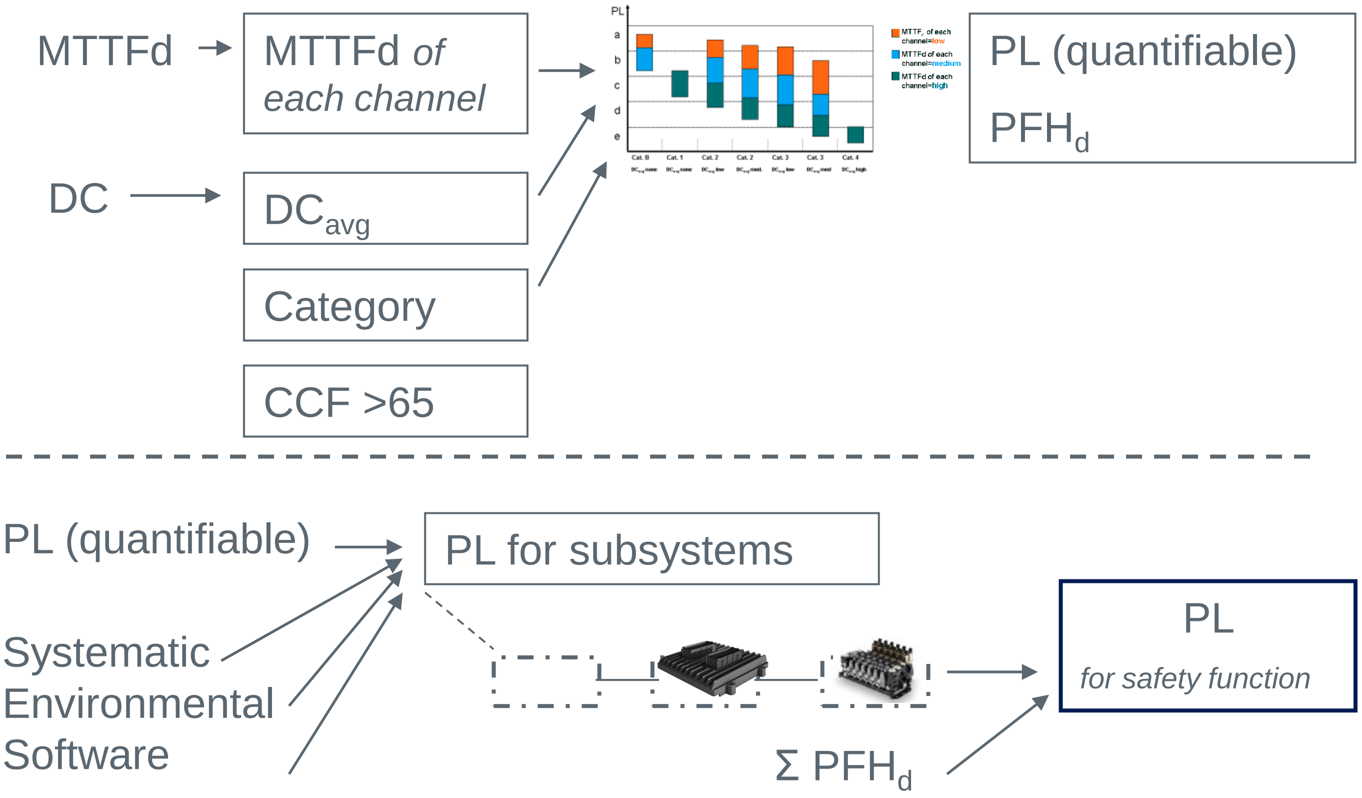
Hydraulic output

Design to EN ISO 13849-1

Evaluate PL and PFHd

EN ISO 13849-1

Overview of PL for safety function



MTTFd

MTTFd of each channel

DC

DC_{avg}

Category

CCF >65

PL (quantifiable)

PFH_d

PL (quantifiable)

Systematic

Environmental

Software

PL for subsystems

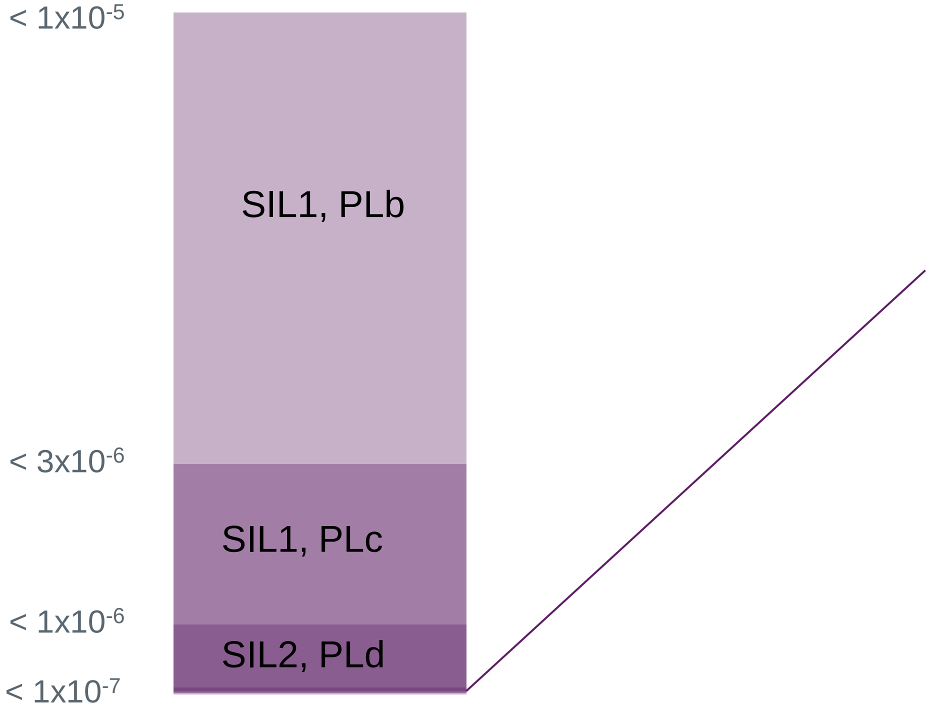
Σ PFH_d

PL

for safety function

Complete safety function, calculate combined PFHd

Probability of dangerous failure per hour



The IQAN-MC4xFS gives margins to complete safety function

IQAN-MC41FS	$7.63 x10^{-8}$
IQAN-MC42FS	$7.92 x10^{-8}$
IQAN-MC43FS	$9.29 x10^{-8}$
IQAN-XC41	$6.28 x10^{-8}$
IQAN-XC42	$6.57 x10^{-8}$
IQAN-XC43	$7.94 x10^{-8}$

IQAN-MC4xFS, hardware and embedded software

Inputs

- Monitoring of VREF
- Monitoring of ADC
- Monitoring of pulse inputs

Outputs

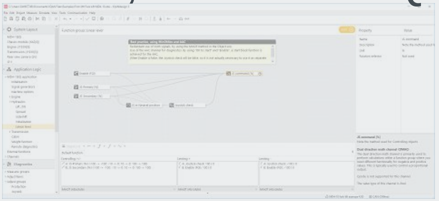
- Monitoring of power drivers
- Monitoring of wiring

Core

Hardware diagnostics

Correct execution of software

Application, created in IQANdesign



Inputs

Use inputs in pair

Cross monitor sensors

Outputs

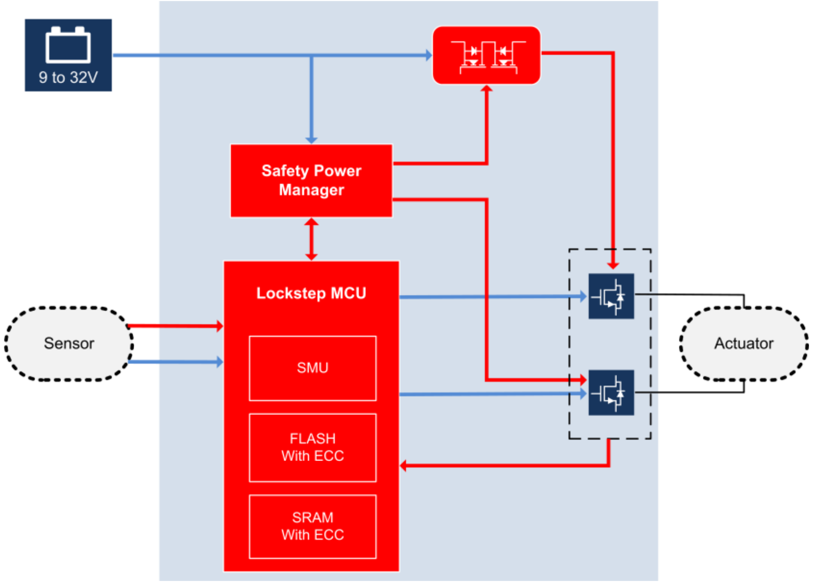
Use safe outputs

Control hydraulics

Functionality

Correct application logic

IQAN-MC4xFS

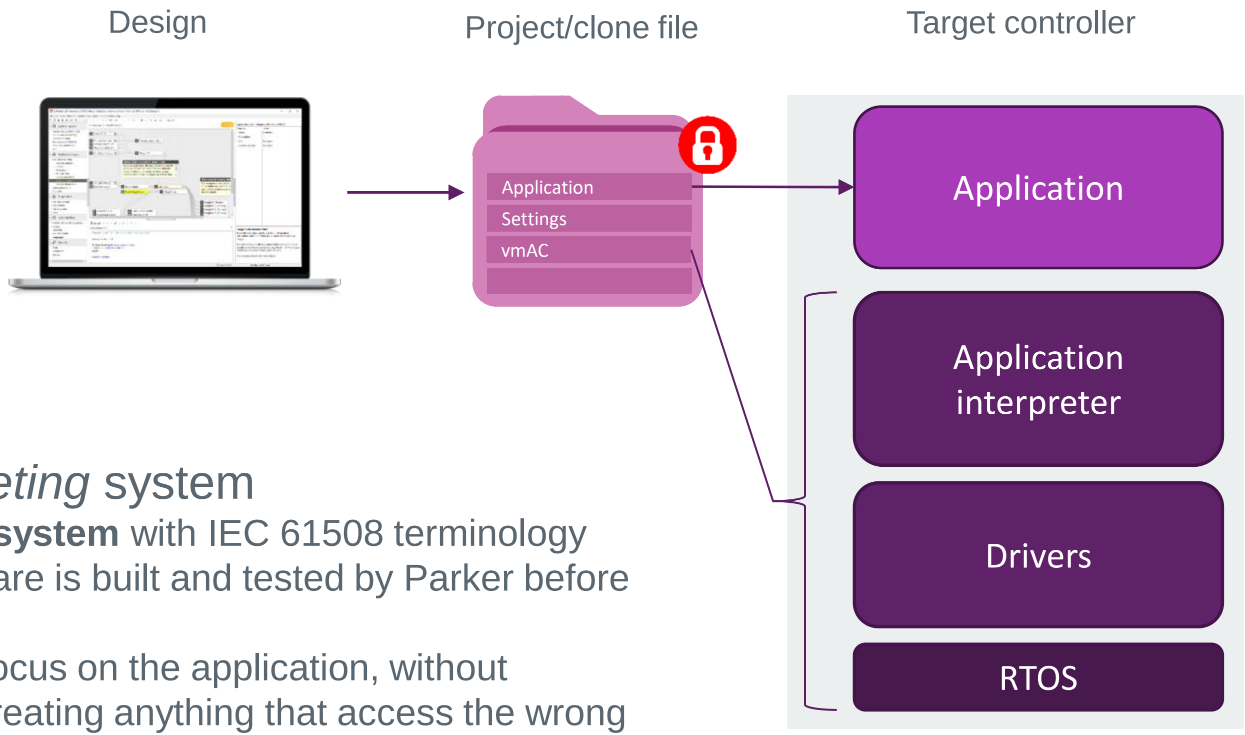


Key features for functional safety

- Lockstep MCU
- Safety related application executed in lockstep core
- ECC protected Flash and RAM
- Checksums on settings (FRAM)
- Independent safety power supply
- Monitoring of all voltages and critical temperatures
- Using IEC 61508 SIL3 safety certified real-time OS
- Isolation using MPU
- Running IQAN application interpreter (vmAC)
- Automatic error detecton and action on COUT/DOUT
- Built to withstand the harsh environment on mobile machinery
- Meets and exceeds EMI requirements for mobile machinery
- Development process in accordance with IEC 61508:2010
- IEC 61508 functional safety assessment and certification by RISE
- 2006/42 EC type examination by RISE as logic unit to ensure safety functions

IQAN

Data driven system



Design

Project/clone file

Target controller

Application

Settings

vmAC

Application

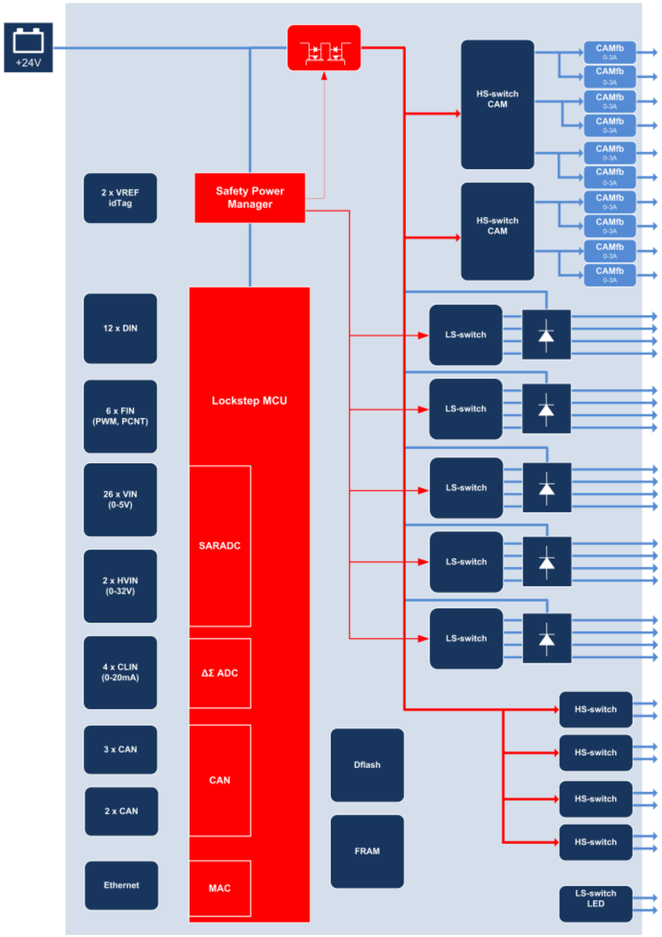
Application interpreter

Drivers

RTOS

IQAN is an *interpreting* system

- Called **data-driven system** with IEC 61508 terminology
- All embedded software is built and tested by Parker before each release.
- IQANdesign users focus on the application, without running the risk of creating anything that access the wrong parts



IQAN-MC43FS inputs

50 input pins

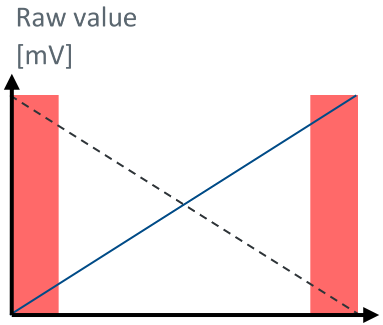
- **26 analog inputs** use for 0-5V or as digital input
- **2 analog inputs** for 0-32V
- **4 current loop inputs** for 4-20mA signals
- **6 timer inputs** frequency, pulse or digital inputs
- **12 digital inputs** dedicated

All possible to use in safety functions

- Any input pin may be used as part of a safety functions
- Normal input usage is in pairs for redundant sensors
  - IQANdesign compare channels recommended

Analog inputs on MC4xFS /-XC4x

- **VIN**, Voltage input 0.5-4.5V
  - Dual crossed signals **recommended for diagnostics on both sensor and inputs**
  - Internal monitoring of AD Converter and reference:
    - Single signal or dual identical signals possible with wider margins on safe failure 10%
  - Range limit in application required
- **CIN**, Current loop input 4-20mA
  - Dual crossed signals **recommended for diagnostics on both sensor and inputs**
  - Internal monitoring of AD Converter and reference:
    - Single signal or dual identical signals possible with wider margins on safe failure 10%
  - Range limit in application required



Frequency type inputs on MC4xFS /-XC4x

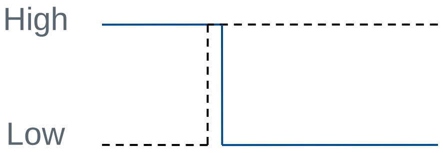
Each frequency inputs is connected to two separate processor input ports

- **PWMIN**, PWM input 5%-95% MR
  - Dual signals **recommended for diagnostics on both sensor and inputs**
  - Input monitoring of MR range and frequency
      - Single signal possible
  - Range limit in application required

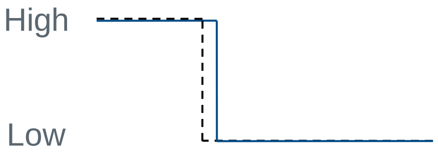
- **FIN, PCNT, DFIN, DPCNT**, Frequency/pulse inputs 0-50 kHz
  - Dual signals **required** for diagnostics on both sensor and inputs
  - Use IQANdesign compare channel

Digital inputs on MC4xFS /-XC4x

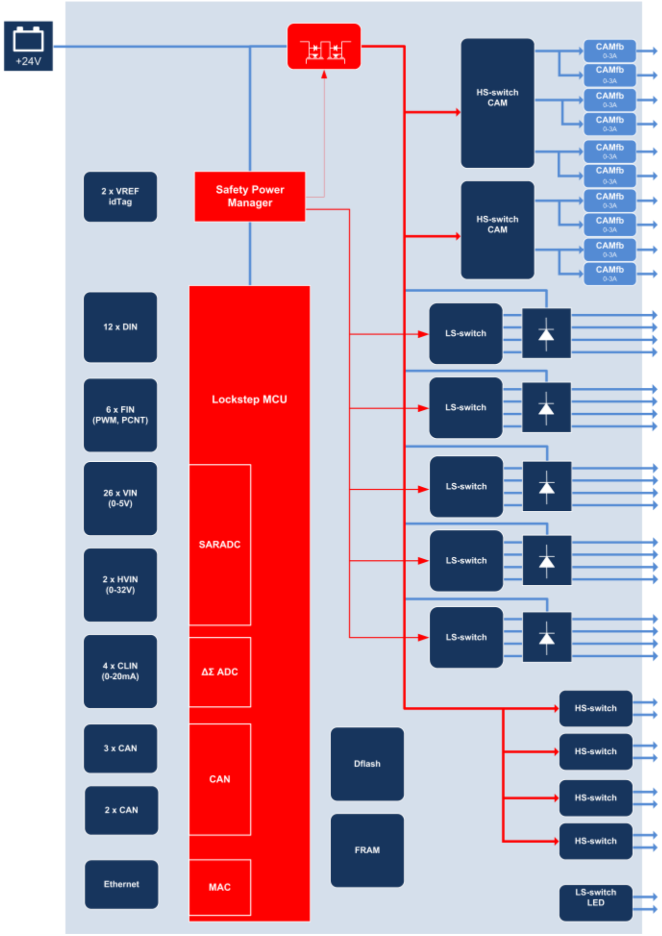
- **DIN**, on-off input with pull-up or pull-down
  - Dual signals are always **required** for DIN
  - Use IQANdesign *Digital Compare channel*
  - Dual antivalent signals **recommended for best diagnostics on both sensor and inputs**
  - Dual identical signal *possible,* application must consider if sensor diagnostics is reduced



Dual opposite signals



Dual identical signals



IQAN-MC43FS outputs

46 output pins

- **10 COUT** for CAM precision control of up to 10 directional proportional valves, pins combine with
- **20 power low side** used in COUT or Digital out HS+LS for up to 2.5A
- **8 DOUT/PWM** high side driver up to 4 A
- **8 low current low side** for LED lamp control (non safety related)

IQAN COUT

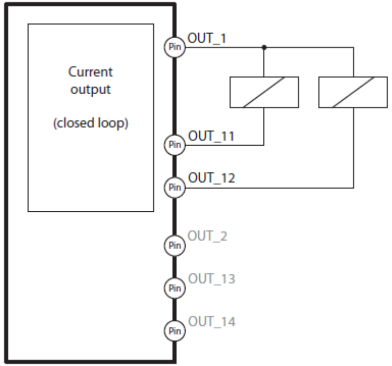
Motion control made easy with Parker Hannifin's CAM regulator for proportional control of mobile pumps and valves based on 30+ years of experience.

CAM - Parker Hannifin solution for precision control of proportional mobile pumps and valves

- **No tuning or tweaking** CAM regulator circuit guaranties consistent performance
- **Precision control** with a resolution down to 1 mA, a must when there is need for controlling hydrostatic transmissions or precise crane movements
- **Zero drift control** provide the lowest possible output offset current and drift. Parker Hannifin's zero drift CAM offer initial offset current of less than 5mA and almost immeasurable offset current drift over time, temperature and load change

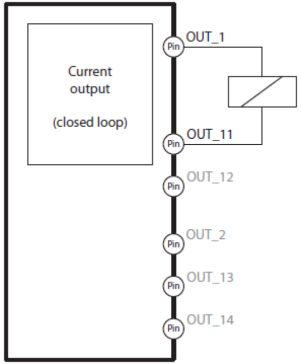
Output connections for safety functions

COUT, bidirectional



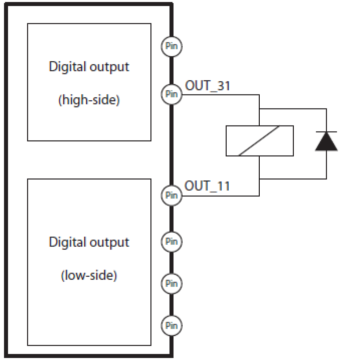
100-2500 mA

COUT, single coil



100-2500 mA

DOUT HS +LS

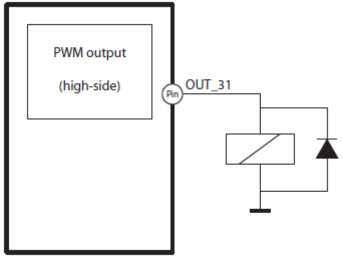


60-2500 mA

Other output connections

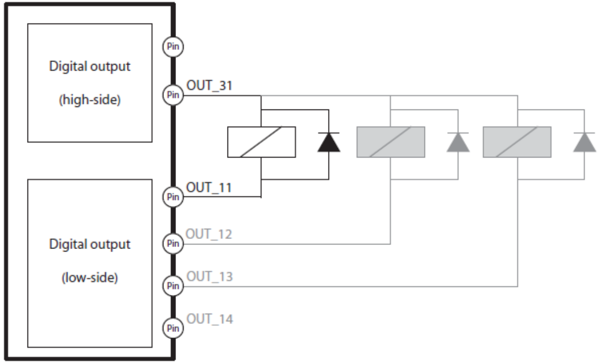
Not for safety related machine control

PWM out HS
DOUT HS



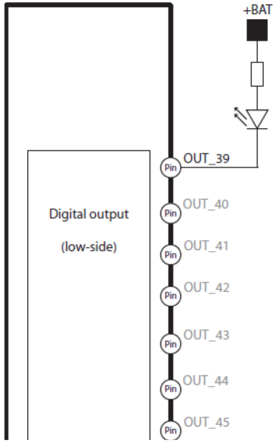
≤ 4000 mA

DOUT HS +LS,
multiple low side



60-2500 mA

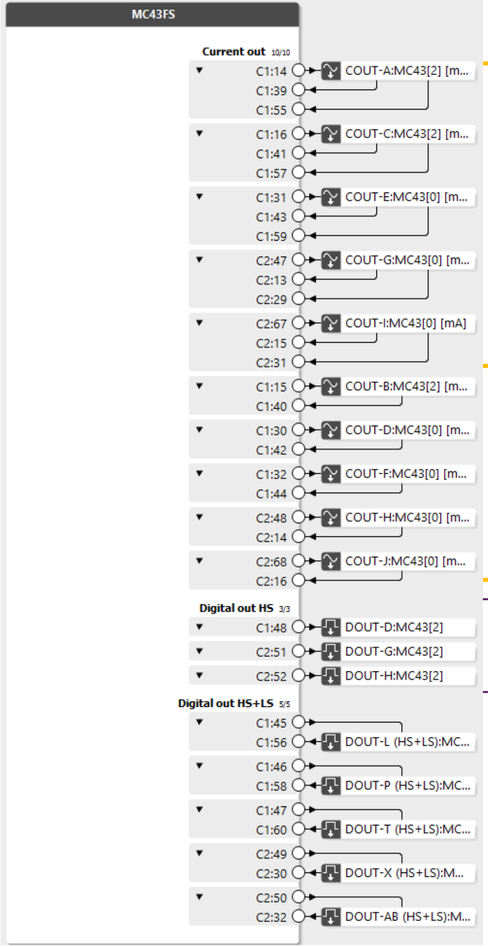
DOUT LS
low current (MC43)



≤ 300 mA

MC43FS outputs

- Combination of high-side and low side switches for handling also external wiring faults
- On FS versions, each DOUT HS+LS has exactly one highside switch per coil.
- Each unused DOUT HS+LS combination can make one more COUT bidirectional and leave one DOUT HS for non safety related functions



MC43FS

Current out 10/10

C1:14 COUT-A:MC43[2] [m...
C1:39
C1:55

C1:16 COUT-C:MC43[2] [m...
C1:41
C1:57

C1:31 COUT-E:MC43[0] [m...
C1:43
C1:59

C2:47 COUT-G:MC43[0] [m...
C2:13
C2:29

C2:67 COUT-I:MC43[0] [mA]
C2:15
C2:31

C1:15 COUT-B:MC43[2] [m...
C1:40

C1:30 COUT-D:MC43[0] [m...
C1:42

C1:32 COUT-F:MC43[0] [m...
C1:44

C2:48 COUT-H:MC43[0] [m...
C2:14

C2:68 COUT-J:MC43[0] [m...
C2:16

Digital out HS 3/3

C1:48 DOUT-D:MC43[2]

C2:51 DOUT-G:MC43[2]

C2:52 DOUT-H:MC43[2]

Digital out HS+LS 5/5

C1:45
C1:56 DOUT-L (HS+LS):MC...

C1:46
C1:58 DOUT-P (HS+LS):MC...

C1:47
C1:60 DOUT-T (HS+LS):MC...

C2:49
C2:30 DOUT-X (HS+LS):M...

C2:50
C2:32 DOUT-AB (HS+LS):M...

5 COUT bidirectional
(safe)

5 COUT single coil
(safe)

3 DOUT HS, for non safety related functions

5 DOUT HS+LS
(safe)

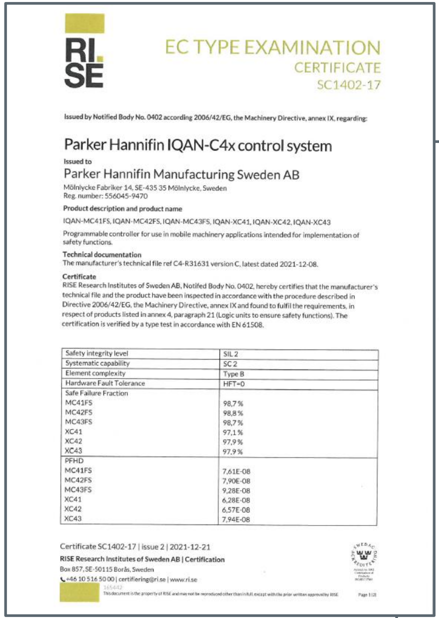
Advantages of using IQAN for functional safety

- Safety certification on IQANdesign tool for development
  - No compilation of application or embedded software, all embedded SW and the IQAN application interpreter is compiled and verified by Parker
  - Highlight and document safety functions, guided by project check
  - Built-in well defined and secure interface if IQAN master display is used for tuning of a safety related parameter, limits and security handled by safety master.
  - Design tool that is specific to the needs of mobile machinery, easy to create the intended function
  - Predictable real-time performance
- Safety certification on IQANrun for SW download and parametrization
  - Security level for tuning/calibration of any safety related parameters
- Simulation in IQANsimulate helps when checking the application software, before verification even begins.

Bottom line

- Enables the machine designer to **focus on machine functionality** and **safety**

EC type examination and IEC 61508 SIL2 certification by RISE



EC TYPE EXAMINATION CERTIFICATE SC1402-17

Issued by Notified Body No. 0402 according 2006/42/EG, the Machinery Directive, annex IX, regarding:

Parker Hannifin IQAN-C4x control system

Issued to

Parker Hannifin Manufacturing Sweden AB

Mölnlycke Fabriker 14, SE-435 35 Mölnlycke, Sweden
Reg. number: 556045-9470

Product description and product name

IQAN-MC41FS, IQAN-MC42FS, IQAN-MC43FS, IQAN-XC41, IQAN-XC42, IQAN-XC43

Programmable controller for use in mobile machinery applications intended for implementation of safety functions.

Technical documentation
The manufacturer's technical file ref C4-R31631 version C, latest dated 2021-12-08.

Certificate
RISE Research Institutes of Sweden AB, Notifed Body No. 0402, hereby certifies that the manufacturer's technical file and the product have been inspected in accordance with the procedure described in Directive 2006/42/EG, the Machinery Directive, annex IX and found to fulfil the requirements, in respect of products listed in annex 4, paragraph 21 (Logic units to ensure safety functions). The certification is verified by a type test in accordance with EN 61508.

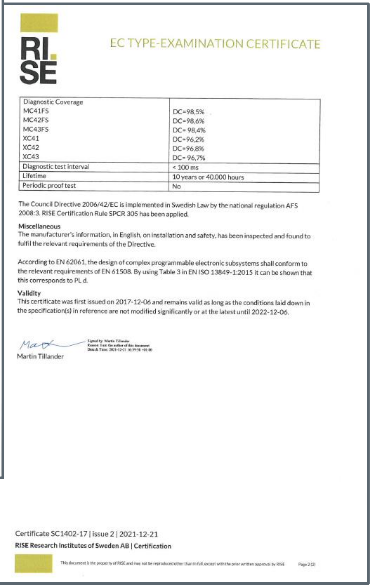
Safety integrity level	SIL 2
Systematic capability	SC 2
Element complexity	Type B
Hardware Fault Tolerance	HFT=0
Safe Failure Fraction MC41FS MC42FS MC43FS XC41 XC42 XC43	 98,7 % 98,8 % 98,7 % 97,1 % 97,9 % 97,9 %
PFHD MC41FS MC42FS MC43FS XC41 XC42 XC43	 7,61E-08 7,90E-08 9,28E-08 6,28E-08 6,57E-08 7,94E-08

Certificate SC1402-17 | issue 2 | 2021-12-21
RISE Research Institutes of Sweden AB | Certification
Box 857, SE-50115 Borås, Sweden
+46 10 516 50 00 | certifiering@ri.se | www.ri.se

SWEDAC ACKREDITERING

165442

Page 1 (2)



EC TYPE-EXAMINATION CERTIFICATE

Diagnostic Coverage
MC41FS
MC42FS
MC43FS
XC41
XC42
XC43
	
	DC=98,5%
	DC=98,6%
	DC= 98,4%
	DC=96,2%
	DC=96,8%
	DC= 96,7%

Diagnostic test interval	< 100 ms
Lifetime	10 years or 40.000 hours
Periodic proof test	No

The Council Directive 2006/42/EC is implemented in Swedish Law by the national regulation AFS 2008:3. RISE Certification Rule SPCR 305 has been applied.

Miscellaneous
The manufacturer's information, in English, on installation and safety, has been inspected and found to fulfil the relevant requirements of the Directive.

According to EN 62061, the design of complex programmable electronic subsystems shall conform to the relevant requirements of EN 61508. By using Table 3 in EN ISO 13849-1:2015 it can be shown that this corresponds to PL d.

Validity
This certificate was first issued on 2017-12-06 and remains valid as long as the conditions laid down in the specification(s) in reference are not modified significantly or at the latest until 2022-12-06.

Signed by: Martin Tillander
Reason: I am the author of this document
Date & Time: 2021-12-21 16:39:38 +01:00

Martin Tillander

Certificate SC1402-17 | issue 2 | 2021-12-21
RISE Research Institutes of Sweden AB | Certification

Page 2 (2)

WARNING — USER RESPONSIBILITY

FAILURE OR IMPROPER SELECTION OR IMPROPER USE OF THE PRODUCTS DESCRIBED HEREIN OR RELATED ITEMS CAN CAUSE DEATH, PERSONAL INJURY AND PROPERTY DAMAGE.

This document and other information from Parker-Hannifin Corporation, its subsidiaries and authorized distributors provide product or system options for further investigation by users having technical expertise.

The user, through its own analysis and testing, is solely responsible for making the final selection of the system and components and assuring that all performance, endurance, maintenance, safety and warning requirements of the application are met. The user must analyze all aspects of the application, follow applicable industry standards, and follow the information concerning the product in the current product catalog and in any other materials provided from Parker or its subsidiaries or authorized distributors.

To the extent that Parker or its subsidiaries or authorized distributors provide component or system options based upon data or specifications provided by the user, the user is responsible for determining that such data and specifications are suitable and sufficient for all applications and reasonably foreseeable uses of the components or systems.

ENGINEERING YOUR SUCCESS.