ENGINEERING TOMORROW

Safety Manual

PLUS+1 Controller
XL104-xxxx Functional Safety Implementation

www.danfoss.com

Revision history

Table of revisions

Date	Changed	Rev
June 2024	Corrected Design Considerations	0201
March 2022	Corrected minor issues	0102
December 2020	First edition	0101

Contents

Introduction

This safety implementation document provides information necessary to design, implement, verify and maintain a safety critical function utilizing the PLUS+1® XL104-XXXX Controller Family. This document provides necessary requirements for meeting the IEC 61508: 2010 Parts 1-7 and IEC 62061:2005+ A1:2012+ A2:2015 functional safety standards.

Abbreviations and definitions

Abbreviations

DC	Diagnostic Coverage
EUC	Equipment under control.
FMEDA	Failure modes, effects and diagnostic analysis.
HFT	Hardware fault tolerance.
PFH	Probability of failure per hour.
PFDAVG	Average probability of failure on demand.
SFF	Safe failure fraction, summarizes the fraction of failures which lead to a safe state and the fraction of failures which will be detected by diagnostic measures and lead to a defined safety action.
SIF	Safety instrumented function.
SIL	Safety integrity level.
SRS	Safety related system, implementation of one or more safety critical functions. An SRS is composed of any combination of sensor(s), control module(s), and actuator(s).
DIN	Digital input pins
DIN/AIN	Digital analog input pins
DIN/AIN/FreqIN	Digital analog and frequency input pins.
CrntIN (current)	Current input pins.
ResIN	Resistance input pins.
DOUT	Digital output pins.
CrntOUT (current)	Current output pins.
OS	Operating system.

Definitions

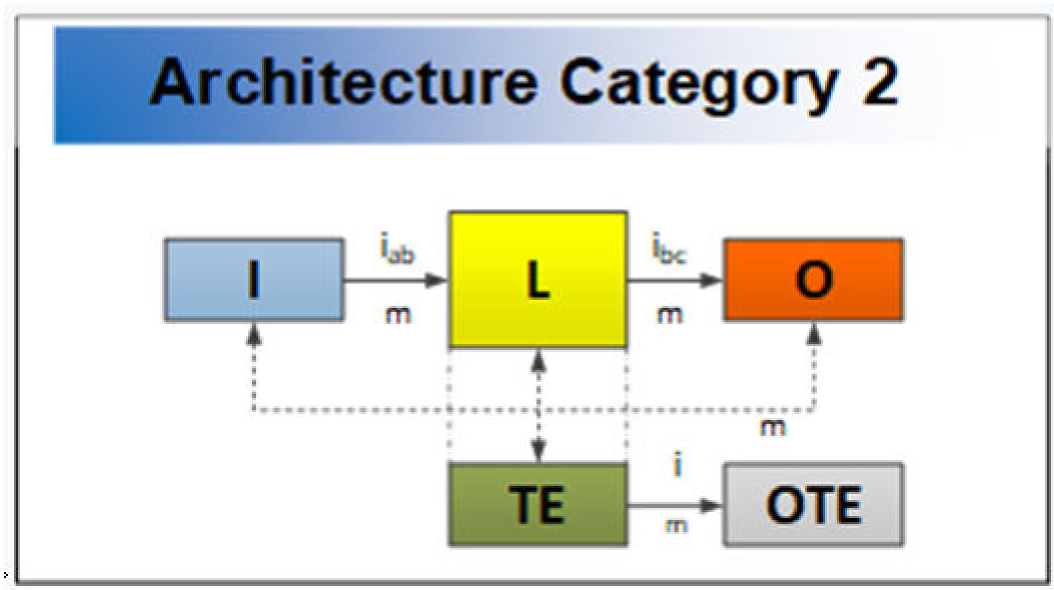
Continuous Demand Mode	Mode where the safety function retains the equipment under control in a safe state as part of its normal operation.
High Demand Mode	Mode where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year.
Low Demand Mode	Mode where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is not greater than one per year. NOTE: The E/E/PE safety-related system that performs the safety function normally has no influence on the EUC or EUC control system until a demand arises. However, if the E/E/PE safety-related system fails in such a way that it is unable to carry out the safety function, then it may cause the EUC to move to a safe state (see 7.4.6 of IEC 61508).
Safety	Freedom from unacceptable risk of harm.
Functional Safety	The ability of a system to carry out the actions necessary to achieve or to maintain a defined safe state for the equipment, machinery, plant, and apparatus under control of the system.
Basic Safety	The equipment must be designed and manufactured such that it protects against risk of damage to persons by electrical shock and other hazards and against resulting fire and explosion. The protection must be effective under all conditions of the nominal operation and under single fault conditions.

Introduction

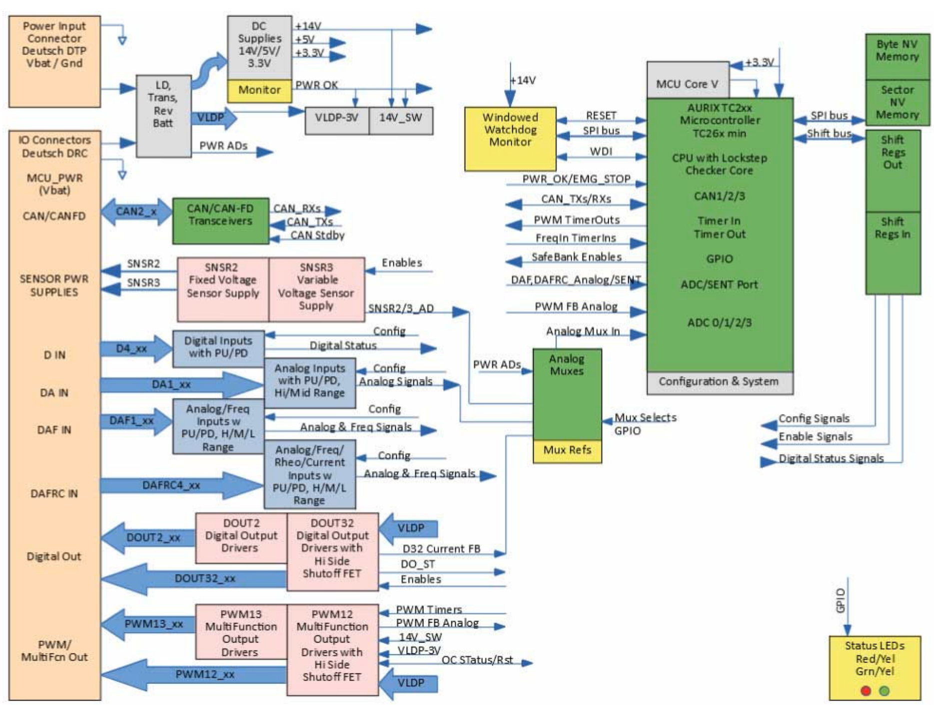
Safety Assessment	The investigation to arrive at a judgment, *based on evidence* of the safety achieved by safety-related systems.
Safety Critical Function	A set of equipment intended to reduce the risk due to a specific hazard.
Process Safety Time	The period of time between a failure occurring in the control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the safety function is not performed.
Type A Component	*Non-Complex* element (using discrete elements); for details see 7.4.4.1.2 of IEC 61508
Type B Component	Complex element (using micro controllers or programmable logic); for details see 7.4.4.1.3 of IEC 61508.
Common Logic	Electrical components and circuitry typically involved with all applications regardless of the input-output channel configuration.

Overview

The Plus+1® XL104 Controller uses a Category 2 safety architecture as defined in ISO13849:



Much of the Test Equipment function for the Category 2 safety architecture is contained within the MCU itself. The MCU Test Equipment components include memory ECC hardware, a checker core, diagnostic hardware on ADCs and GPIOs, and software independent Emergency Stop hardware. An external windowed watchdog and monitor device is used as part of the Test Equipment.



The MCU will execute the Modular Safety Kernel (MSK). The inputs will be read and provided to the application. The application processes this information and will set the outputs to the desired values. The setting of the outputs is done from the MSK.

Component description and failure rates

Detailed analysis, review and documentation for compliance to ISO 13849 or ISO 25119 must be done by the designer or integrator of the safety related system.

Failure categories description

In order to judge the failure behavior of the PLUS+1® XL104 Controller, the following definitions for the failure of the component apply.

Definitions for failure of the component

Failure category	Definition
λ_{SD}	Failure rate of all safe detected failures
λ_{SU}	Failure rate of all safe undetected failures
λ_S	Failure rate of all safe failures (detected and undetected),λ_{SD} +λ_{SU}
λ_{DD}	Failure rate of all dangerous detected failures
λ_{DU}	Failure rate of all dangerous undetected failures
λ_D	Failure rate of all dangerous failures, detected and undetected, λ_{DD} +λ_{DU}
DC	IEC 13849 Diagnostic Coverage = $\lambda_{DD}/(\lambda_{DD}+\lambda_{DU})$
SFF	IEC 61508 Safe Failure Fraction = $(\lambda_S+\lambda_{DD})/(\lambda_S+\lambda_{DD}+\lambda_{DU})$
β-factor/Beta factor	Probability of CCF between test equipment and primary subsystem
FIT	Failures In Time (failures per 10^9 hours)

Failure rates

The results of the FMEDA analysis for the PLUS+1® XL104 Controller are presented in the following table. Common Logic consists of circuits in the controller that directly affect the performance of any Safety Function. The Test Equipment Logic consists of diagnostic circuits in the controller and is not directly included in a Safety Function reliability calculation. The failure rates below assume the implementation of all Recommended Diagnostics. If no diagnostics are implemented by the application, all Dangerous Detected Failures should be assumed to become Dangerous Undetected Failures.

Refer to *Using the FMEDA results* on page 19 for an example of how to calculate the reliability of a Safety Function using these data.

Failure Rate Variation With Temperature

Hard error failure rates of electronic components will change with the average operating temperature of the controller. Soft Errors in electronic components are caused by other failure mechanisms that are not temperature dependent.

Danfoss typically provides component failure rates that are normalized to an operating temperature of 45°C. If the mission profile of the application calls for a higher or lower operating temperature, the failure rates can be scaled to that temperature. Because the failure rates of various components change at different rates with temperature, the scaling of the overall controller failure rate is complex. Contact Danfoss Power Solutions if your mission profile is different from these examples.

Subsystem failure rates at 45ºC (FIT)

Controller Subsystem	λ_S	λ_{DD}	λ_{DU}	DC
Common Logic	95.5	1400	176	89.8%
Test Equipment Logic	27.9	123	8.5	93.6%
CAN Port	0	38.9	2.9	93.1%
DIN	0	3	6.2	32.5%
DIN with key-switch	2.9	3	7.9	27.6%

Component description and failure rates

Subsystem failure rates at 45ºC (FIT) (continued)

Controller Subsystem	λ_S	λ_{DD}	λ_{DU}	DC
DIN/AIN (Digital)	0	7	7.6	48.0%
DIN/AIN (Analog)	0	11.3	3.5	76.4%
DIN/AIN/FreqIN (Digital)	0	6.9	10.5	39.6%
DIN/AIN/FreqIN (Analog)	0	13.9	4.4	75.8%
DIN/AIN/FreqIN (Frequency)	0.05	11.6	3.3	77.8%
DIN/AIN/FreqIN/CrntIN/ResIN (Digital)	0	8.7	10.8	44.5%
DIN/AIN/FreqIN/CrntIN/ResIN (Analog)	0	11.7	8.3	58.6%
DIN/AIN/FreqIN/CrntIN/ResIN (Frequency)	0.12	11.9	5.2	69.5%
DIN/AIN/FreqIN/CrntIN/ResIN (ResIN)	0	13.6	7.1	65.7%
DIN/AIN/FreqIN/CrntIN/ResIN (Current)	1.22	11.3	13.4	45.6%
DOUT	1.6	48.8	2.5	65.9%
DOUT with Safebank	30.6	7.7	1.4	84.8%
CrntOUT (Current)	19.8	48.6	9.6	83.5%
CrntOUT (Current) with Safety FET	33	57	11.6	83.1%
Fixed Sensor Supply	22.2	18.4	5.17	78%
Variable Sensor Supply	25	27.3	3.71	88%

Recommended diagnostics

The PLUS+1® XL104 Controller should be implemented with diagnostics in the application to detect many dangerous failures and other failures that would result in the controller operating in a degraded mode. The machine integrator is responsible for the function safety and compliance to relevant standards.

The following table lists recommended diagnostics. These diagnostics should be implemented in the user application software that is loaded into the PLUS+1® XL104 Controller.

Diagnostics

Function	Failure mode	Condition	Action	Continuous or Start-up
Sensor power	Short to battery	Analog reading at or near maximum	Stop reading inputs powered by sensor power.	Continuous
Sensor power	Short to ground	Analog reading at or near zero	Stop reading inputs powered by sensor power.	Continuous
Sensor power	Out of range	Analog reading different than expected	Can compensate inputs for new voltage if possible	Continuous
Analog input	At Max	Analog reading at or near max	Stop using this input	Continuous
Analog input	At zero volts	Analog reading at or near zero	Stop using this input	Continuous
Frequency input	Open	Analog reading is at or near middle voltage	Ignore frequency input	Continuous
Frequency input	No signal	Analog value doesn't change for longer than the maximum period	Ignore frequency input	Continuous
Digital output	Load shorted	Status signal indicates short circuit or open load	Application dependent	Continuous
Digital output	Open load	Status signal indicates short circuit or open load	Application dependent	Continuous

Component description and failure rates

Diagnostics (continued)

Function	Failure mode	Condition	Action	Continuous or Start-up
Current driver	Zero-state current out of range	Feedback current measurement is not within range of 14831<AnIn<19937 before sending output command	Application dependent	Continuous
Current driver	Safety FET not enabled	Status signal does not indicate that the Safety FET is enabled before sending output command	Do not use that output	Continuous
Current driver	Load shorted	Duty cycle at least 50% less than expected for known load	Information only or turn off output	Continuous
Current driver	Load shorted	Status signal indicates short circuit	Turn off output immediately	Continuous
Current driver	Open load	Duty cycle at least 50% less than expected for known load	Information only or turn off output	Start-up
Current driver	Zero-state current out of range	Feedback current measurement is not within range of 14831< .AnIn < 19937 before sending output command	Application dependent	Continuous
Current driver	Safety FET not enabled	Status signal does not indicate that the safety FET is enabled before sending output command	Do not use that output	Continuous
Current driver	Load shorted	The output current decays too slowly after the output is disabled	Turn off output immediately	Continuous
Current driver	Incorrect load	Coil resistance is greatly different than expected	Do not use that output	Continuous
Battery Power	Dangerously High	Battery voltage reading above 36V	Turn off all outputs and ignore inputs	Continuous
Battery Power	Dangerously Low	Battery voltage reading below 7V	Turn off all Current outputs	Continuous
CAN	Bus off	CAN bus status signal indicates bus off	Turn off outputs that rely on CAN information	Continuous
CAN	Time out	An expected message hasn't been received in the expected time	Turn off outputs that rely on that message	Continuous
CAN	Failed transition	Application requests message transmission while pending flag is active	Application dependent	Continuous
Configuration	Invalid configuration	Status signal indicates input or output is configured in an invalid way.	Make change to application software	Start-up

Design Considerations

Safety critical functions

The PLUS+1® XL104 Controller can perform a wide variety of control functions. If these control functions are safety critical, then additional safety reliability can be achieved by configuring the controller to monitor the sensor inputs, perform diagnostics, and act to bring the machine to a safe state if safe operating parameters are violated.

Upon detection of critical controller failures, controller outputs are de-energized to enter a safe state. The application shall ensure that de-energized outputs in the event of faults does not hamper the machine level safety functions.

The following sections describe features of the PLUS+1® XL104 Controller related to the implementation of Safety critical functions.

Functional Safety Implementation

Microcontroller

The microcontroller is the application processor containing normal application code required for machine operation machine level safety functions. The application will be developed in PLUS+1®GUIDE. The application contains modules for normal machine control and specific machine level safety functions. The processor sees all inputs and can set all outputs. The processor controls the safety functions, under kernel and application software control with a hardware-only channel from the Windowed Watchdog and Power Supply Monitor to disable the safety group functions.

Executed IN: Kernel

Application interaction: Application must have general safety handling and logical check for when it is safe to enable outputs. This may include start-up protection (FNR in neutral prior accepting driving inputs etc.)

The Application uses the API Enable signals to enable or to disable an output.

Sensor Power Outputs

The PLUS+1® XL104 Controller will generally have one or more Sensor Power Supply Outputs. The voltage level of these supplies are designed to be static. The output voltages may be constant or variable within the range of 3.0V to 12.0V, depending on the sensor supply hardware. The generated voltage level is monitored and is reported to the application. This reported value can be used by the application to use ratio metric scaling of analog inputs and to validate if the generated voltage of the sensor supply output is sufficient for connected sensors. This allows the application to bring the system into a safe state by shutting down safety relevant outputs in case the value is not in the expected state.

The sensor power outputs are current limited to prevent a high load on the supply output from affecting the internal operation of the controller. The application can use the output voltage monitor to determine if an error condition exists, and if so move the application into a safe state.

Executed IN: Kernel is providing the measurement of the sensor voltage channel and provides this to the API.

Application interaction: Application must use the Sensor Output feedback voltage (.Voltage) for ratio metric scaling and for range checking. If redundant monitoring is required, the application should use another analog input. In case of an out of range value or mismatch of reported value, the application shall bring the system into a safe state by shutting down safety relevant outputs.

Protection and Power Supplies

The elements of this circuitry protect the PLUS+1® XL104 Controller against power line transients and provide the necessary voltages for supplying the MCU, input and output circuitries, and internal control logic. The PLUS+1® XL104 Controller does not protect against nominal input voltages outside of the

Design Considerations

range from 0-36V. The internally generated 3.3V and 5V power supplies will be monitored against the 14V power supply, which has an independent internal reference. If any voltage is out of the specified tolerance, a digital indication of a power supply failure will be reported to the MCU. All outputs are then disabled by hardware without any software involvement. The power supply failure event processing is done in hardware because correct operation of the MCU cannot be assumed when a voltage rail is out of range.

Executed IN: Hardware circuitry.

Application interaction: Application must use the API signals to check whether outputs are functioning correctly.

MCU Core Voltage Supervisor

The core supply voltage for the MCU is under supervision to ensure an under voltage condition does not cause any malfunction of the MCU. This supervision uses the on chip power on reset / power down reset system. The MCU goes into or remains in reset mode when the core voltage is below its undervoltage threshold. In the reset state all the MCU outputs are disabled, and biased to an off state. All controller outputs are de-energized.

Executed IN: Hardware circuitry.

Application interaction: None. Hardware will reset the application. Hardware is designed so that a reset of the MCU brings all controller outputs to a safe or de-energized state.

ADC Checks

The MCU will generate a cyclic changing AD signal to validate the function of its AD-converter. This is used to identify a stuck-at situation.

Executed IN: Kernel creates and tests the the ADCs. The result is provided to the API.

Application interaction: Application must use this status information. In case of a problem value the application must take appropriate actions in order to ensure functional safety.

Digital Outputs

The digital output enables are set by the MCU under application and kernel control. Each Digital Output on Safebanks provides an output status signal and a current input signal. The current input signal is used to identify an overcurrent condition on the output. The Digital Outputs on Safebanks are able to be used directly in a safety function since they have multiple ways to de-energize the function by disconnecting the high side to the load.

When using a DOUT on Safebank output, the Safebank must be enabled and verified to be turned on before using the DOUT. This status is shown in the Safebank.Active bit. The application safety layer should use both the DOUT.DigFeedBack status and the Safebank.Active status when monitoring these Digital Outputs.

Each of these outputs is part of a Safe Group. The safety function application controls the enables for each Safe Group. The Safe Group Enables are turned off by the MCU Emergency Stop hardware if a power supply or watchdog event occurs.

Standard Digital Outputs are controlled by the MCU but are not part of a Safe Group. These Digital Outputs should not be used for safety critical functions.

Executed IN: The kernel controls the output, performs feedback calculations, and reads the status. The signals are provided to the API.

Application interaction: Application must use the provided feedback and status signals. In case of an identified problem, the application shall bring the system into a safe state by shutting down safety relevant outputs.

Design Considerations

Multifunctional (Current) Outputs

The Multifunctional Outputs with Safety FETs are controlled by the MCU. Each of these outputs has an individual Safe Group. Each output provides a status signal for overcurrent as well as a current input signal to be used to identify feedback of the output. The Multifunction Outputs with Safety FETs are able to be used directly in a safety function since they have multiple ways to de-energize the function by disconnecting the high side to the load.

The safety function application controls the enables for each Safe Group. The Safe Group Enables are turned off by the MCU Emergency Stop hardware if a power supply or watchdog event occurs.

Standard Multifunctional Outputs are controlled by the MCU but are not part of a Safe Group. These outputs may be used in a safety function when in an H-bridge configuration to be able to de-energize the function by disconnecting either the high side or low side of the load.

The application should check the zero-current reading of a Multifunctional Output in current mode before sending the enable command. The zero-current reading must be with the range of 14831 < .Anin < 17937 to use the output.

Executed IN: The kernel controls the output, performs feedback calculations, and reads the status. The signals are provided to the API.

Application interaction: Application must use the provided feedback and status to determine proper operation. In case of an identified problem, the application shall bring the system into a safe state by shutting down safety relevant outputs.

Inputs

All digital and analog inputs are run to the MCU. In case higher MTTFd or Diagnostic Coverage numbers are required for input devices they should be connected to the external function in a redundant manner from the controller's IO connectors. Frequency inputs will be monitored by additional checks such as counter active checks and register overflow situation when no frequency is measured to monitor possible problems with the CPU capture unit.

Executed IN: Kernel is monitoring the CPU capture unit, signals, and doing feedback calculations, etc. and is providing info to API.

Application interaction: Application must use the status information provided by the API. In case of a problem value the application shall bring the system into a safe state by shutting down safety relevant outputs.

Clocks

The MCU is supplied with a clock from an external source. The MCU runs internal diagnostic routines at startup to detect a failed clock. A failed clock situation will be reported to the MSK, and the controller application will be prevented from starting.

Executed IN: Kernel.

Application interaction: None.

SRAM checks

The MCU internal SRAMs will be checked at start-up to identify potential memory problems. In case of a SRAM failure, the system will not be started and the outputs will be kept deactivated.

The MCU uses EDC/ECC detection and correction hardware to detect runtime SRAM bit failures. MCU hardware will reset the application. Hardware is designed such that a reset of the MCU brings all controller outputs to a safe or de-energized state.

Executed IN: Kernel

Application interaction: None

Design Considerations

Runtime SRAM checks

The MCU uses ECC detection and correction hardware to detect a memory bit failure while in use.

Executed IN: Kernel uses the MCU Memory Unit.

Application interaction: None. MCU hardware will reset the application. MCU hardware circuitry is designed so that a reset of the MCU brings all controller outputs to a safe or de-energized state.

Program FLASH checks

During application download, CRC32 checksums for relevant sections are calculated and will be stored inside the MCU. The checksum of the program memory will be verified at start-up. The application will not start if a checksum failure occurs.

The MCU uses EDC/ECC protection on data reads from the Program Flash memory. If an uncorrectable memory error is detected, the Kernel will reset the application. Hardware is designed so that a reset of the MCU brings all controller outputs to a safe or de-energized state.

Executed IN: Kernel

Application interaction: None

Memory protection

The Kernel utilizes the MCU's memory protection unit to prevent memory access violations (e.g. stack overflow). When a memory access violation is detected, the system will perform a reset. Hardware is designed so that a reset of the MCU brings all controller outputs to a safe or de-energized state.

Executed IN: Kernel

Application interaction: None

Non-volatile memory (EEPROM) data

The data stored inside the Non-Volatile Memory as well as the data presented to the application (located in RAM) is protected with a checksum to make sure the data is correct.

Executed IN: Kernel is monitoring the data.

Application interaction: Application must check NVMem.Status and check the single BIT values. The application shall also take measures to ensure parameters matching the application and parameter structure. The application is responsible for not exceeding the write lifetime of the Non-Volatile Memory.

User Application Software Development Requirements

The application must monitor the system relevant IOs (examples: sensor power voltage, input voltage, memory checks, EEPROM status) and the sequences of application processing. Dependant on the system, the application must disable certain outputs to bring the system into the safe state. Applications must be developed according to the following recommendations:

- **CAN Bus**
  The lower layers of the CAN channels provided by the MSK must be treated as black channels. System-specific requirements for the reliability to the communication through the CAN / CAN-FD channels must be fulfilled by a sufficient CAN protocol, such as SAE J1939-76 or EN 50325-5 (CANopen Safety).
- **Plausibility Checks on Input Data**
  The user application software must include plausibility checks on frequency input data to detect possible failures in frequency input calculations. Moreover, the user application software must include plausibility checks on all safety relevant inputs.

Design Considerations

- **Quad Count Verification**

  The user application software must use the frequency values and the count value of the Quad encoder inputs to validate functionality.

- **Signal Comparison**

  Signal comparison must be implemented by the user application software for safety-related signals. Either inputs with redundant ADC channels should be used and/or two XL104 Controller inputs. Redundant channels must be utilized to provide reliability where there is concern about channel reliability based on PFH.

- **Input Voltage Monitoring**

  The Input Voltage to the output functions must be monitored.

- **Sensor Power Supply Monitoring**

  The sensor power supplies must be monitored and used for any ratiometric calculations for attached the analog sensor inputs.

- **Safety-Capable Digital Outputs**

  Only safety-capable digital outputs with feedback and Safe Group features should be used to control safety-related outputs.

- **Safety-capable Multifunction (PWM/DOUT/PVGOUT) Outputs**

  Only safety-capable Multifunction (PWM/DOUT/PVGOUT) outputs with feedback and a Safety-FET should be used to control safety-related outputs.

- **High-Side and Low-Side Outputs**

  A high-side and a low-side output should be used to control a safety-related load if current shall be sunk.

- **Continuous Sampling of PWM Feedback**

  PWM feedback shall continuously be sampled and compared with the setpoint.

- **Voltage Controlled Loads**

  When using a safety-related voltage controlled load, such as a PVE valve, a power control output and a PWM/Digital control output shall be used to control the load.

- **Over-Current Overload Signal**

  The application must verify that the output current overload status returns to zero after commanding a zero output current or turning off the output.

- **Shutdown of Safety-Critical Outputs**

  The user application software must implement shutdown of safety critical outputs based on user application software safety requirements.

- **Strategies to Mitigate Against Corrupted RAM**

  The user has to implement strategies to mitigiate against effects of corrupted RAM, such as checksums, CRCs, or shadow copies of safety-critical data.

- **Non-Volatile Data**

  The application is responsible to ensure that non-volatile data is consistent. This has to be ensured by the application, for example by plausibility checks, range checks, checksums or CRCs, redundant data storage etc. The application is also responsible for ensuring that the write lifetime of the NV data medium is not exceeded.

- **Software Validation**

  The application must be tested for proper function including fault insertion testing. The user application software must be tested for proper response to:

Design Considerations

- Highest frequency input conditions.
- Highest frequency output conditions.
- Highest CAN traffic load conditions on the corresponding used CAN buses.
- The user application software required OSExecTimeout has adequate safety margin

- **Applog (Application Event Logging)**

  The Applog feature (if available) shall not be used for safety-critical data.

- **Fault Manager**

  If faults must be latched, the application shall take care of this operation.

- **Handling of Safe State**

  The system must be designed in a way that it is able to handle outputs suddenly being de-energized, e.g. as a response to a safety-critical failure.

- **Output Shutdown Verification**

  The user application software must verify that the system is capable of disabling the safety related outputs.

- **Hazard Analysis/Functional Safety Assessment**

  A Hazard Analysis must be conducted for the hazards associated with any safety related system constructed using the Controller.

- **Delay Time From Failure Detection**

  The maximum delay time from the onset of a failure to the time at which the outputs reach the safe state is the diagnostic time interval plus 10 ms. The diagnostic time interval (loop time) is defined by the application.

- **Restart Interval**

  It must be ensured that the XL104 Controller is restarted at least every 12 hours.

- **Current Output Periodic Reset**

  If the user application allows it, the current output must periodically be set to zero to allow the zero offset to be recalculated. The zero current offset calculation can take up to 200 ms. For optimal performance, the output current should be set to zero after large temperature changes (>25° C [77° F]) to allow the zero offset to be re-calculated.

- **High Inductance Valves**

  When a high-inductance valve is switched off, false alarms may occur inside the safety layer because the decay of the PWM output current is too slow. This safety monitoring of PWM outputs can be disabled to improve compatibility with high-inductance valves. To do this, set DisableCurrent-DecayRateMonitoring whereby it now becomes the responsibility of the application to monitor the output current for unintended short (overcurrent) conditions. When such a condition is detected, the application must immediately disable (turn off) the output. By default, DisableCurrent-DecayRateMonitoring is not set and the monitoring is done by the kernel.

Environmental Limits

The designer or integrator of a safety critical function must verify that the PLUS+1® XL104 Controller is rated for use within the expected environmental limits of the target application. Refer to the *PLUS+1® XL104-XXXX Controller Technical Information* **BC320261740866** for controller environmental limits.

Application limits

The designer or integrator of a safety critical function must check that the PLUS+1® XL104 Controller is rated for use within the expected application limits. Refer to the *PLUS+1® XL104-XXXX Controller Technical Information* **BC320261740866** for controller limits.

Design Considerations

Design verification

Refer to **Failure rates** for a summary of failure rates for the PLUS+1® XL104 Controller.

The achieved Safety Integrity Level (SIL) of an entire Safety Critical Function design must be verified by the designer or integrator via a calculation of PFH considering the I/O required, demand mode, any implemented diagnostics, safety time, and architecture.

The failure rate data listed the FMEDA report is only valid for the useful lifetime of a PLUS+1® XL104 Controller. The failure rates will increase sometime after this useful lifetime period. Reliability calculations based on the data listed in the FMEDA report for mission times beyond the lifetime may yield results that are too optimistic; in other words, the calculated Safety Integrity Level will not be achieved.

SIL capability

Systematic capability

The systematic capability of the PLUS+1® XL104-XXXX family is SC 2 per IEC 61508 and the kernel software development is capable of achieving systematic capability of PL d per ISO 13849.

Hardware Fault Tolerance

The PLUS+1® XL104-XXXX is classified as a Type B high demand/continuous mode component with HFT = 0 per IEC 61508.

Architecture

The PLUS+1® XL104-XXXX uses a category 2 architecture in accordance with ISO 13849 and 1oo1D architecture in accordance with IEC 61508.

Random capability

Refer to *Component description and failure rates* on page 7 for a summary of circuit failure rates for the PLUS+1® XL104 Controller. For each user application, the failure rates for that particular configuration should be determined and compared to the allowable failure rate for a given SIL target.

Connection to sensors and actuators

The connection of the PLUS+1® XL104 Controller to the required sensors and actuators must be performed in accordance with the *PLUS+1® XL104-XXXX Controller Family Technical Information*, **BC320261740866**. Machine wiring should be done in a way to minimize EMI and EMC susceptibility.

Design Considerations

Safety function requirements

- The system's response time must be less than the process safety time defined by the user application.
- The worst-case response time for a change of value of an analog input or contact signal (measured at the terminals) through the complete system to the completion of change of state of the analog output or contact output (measured at the terminals) will be a maximum of two times the actual loop execution time OS.ExecTime, as measured to the standard outputs. This worst-case time must be determined for the worst-case loading of the safety controller.

Kernel Diagnostics and response times

Description	Worst case time	Additional information
Diagnostics and Response Times	100ms	To achieve 100ms,application loop time is assumed to be not greater than 20ms. With loop time greater than 20ms, worst case time of 5 * OS.ExecTime should be expected.
Flash ROM or SRAM ECC error (from detection to safe state)	10ms	
Change of input to output	2 * OS.ExecTime	

- The maximum delay time from the onset of a failure to the time at which the outputs reach the safe state is the diagnostic time interval plus 10 ms.
- Results from the functional tests and diagnostics must be recorded and reviewed periodically.
- All safety related system components, including the PLUS+1® XL104 Controller, must be operational before machine operation.
- Personnel performing testing on the PLUS+1® XL104 Controller must be competent to perform such testing. Functional Safety Training is provided by Danfoss Power Solutions, and details can be found on the Danfoss Power Solutions Learning website at: **https://www.danfoss.com/en/service-and-support/learning/**

Installation and operation considerations

Installation

The PLUS+1® XL104 Controller must be installed per standard practices outlined in the *PLUS+1® XL104-XXXX Controller Family Technical Information*, **BC320261740866**. The environmental conditions must be verified to not exceed the controller environmental ratings. Instructions on installation of latest version of the safety controller HWD file are found in *How to Install PLUS+1® GUIDE Upgrades Operation Manual*, **11078040**.

Physical location and placement

The PLUS+1® XL104 Controller must be mounted in accordance with the *PLUS+1® XL104-XXXX Controller Family Technical Information*, **BC320261740866**., in a low vibration environment. If excessive vibration is expected, special precautions must be taken to ensure the integrity of electrical connections or the vibration should be reduced using appropriate damping mounts.

Repair and placement

The PLUS+1® XL104 Controllers are not repairable and no maintenance of them is required.

Useful life

The useful life of the PLUS+1® XL104 Controller is 30 years. No proof tests are required.

Software/hardware version numbers

See the relevant PLUS+1® XL104 Controller *Data Sheet*.

Design Considerations

Security considerations

The PLUS+1® XL104 Controller does not use data that the user can configure externally, for example, by the PLUS+1® Service Tool. The user application software may contain data that is configured externally. If this is the case, then suitable security should be provided. The *PLUS+1 ® GUIDE Software User Manual*, **10100824** provides a description of how to handle parameters in a safe way.

Danfoss Power Solutions notification

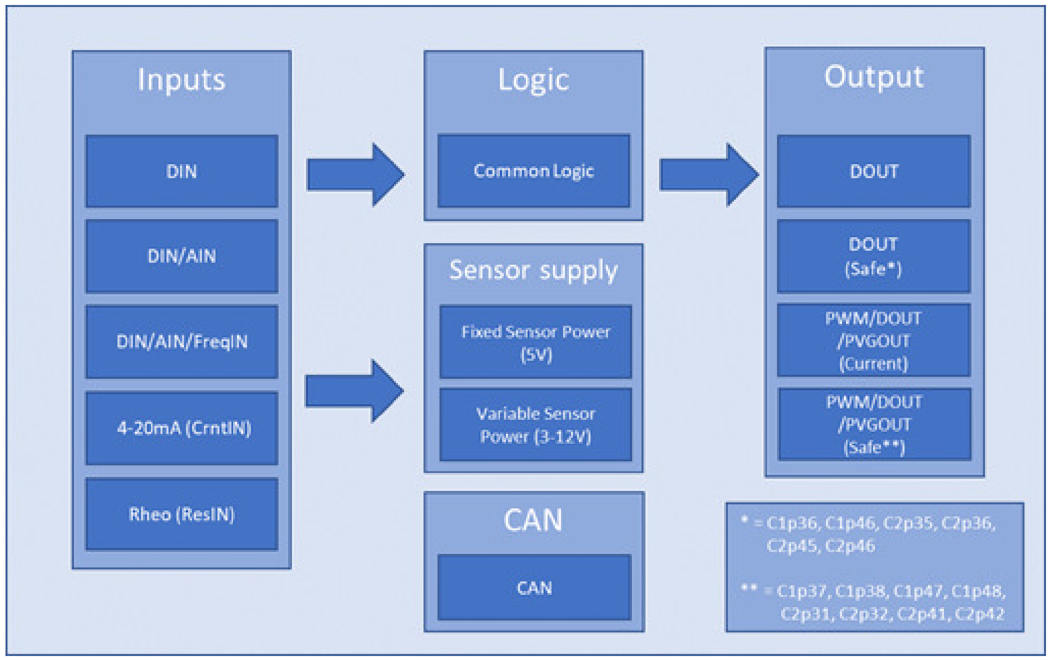
Any failures that are detected and that compromise functional safety should be immediately reported to Danfoss Power Solutions. Any change suggestions for future improvements or new features can be forwarded to Danfoss Power Solutions:

Contact information is online at: **https://www.danfoss.com/en/contact-us/**

Using the FMEDA results

This chapter explains how the results from the FMEDA analysis can be used to calculate the contribution of the XL Controller in a safety critical application.

The total will include the failure rate of all sensors and actuators that are required to perform the function as well as the elements of the PLUS+1® XL104 Controller that are utilized. The different function groups from Inputs, Logic, Power Supply and Outputs are illustrated in the safety block diagram below:

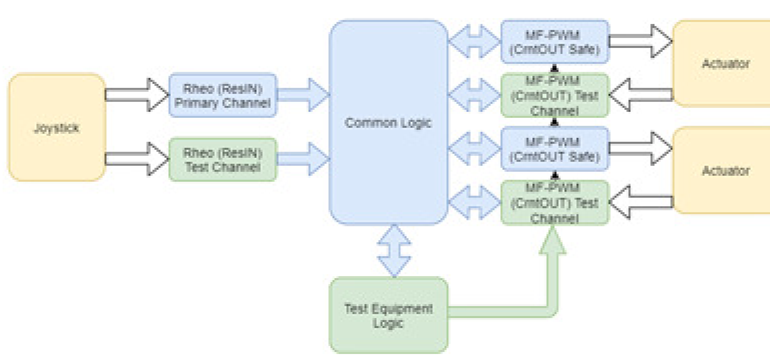


The failure rates for each subsystem are listed in the section *Component description and failure rates* on page 7.

Example application, failure rate analysis

To demonstrate how to calculate the contribution of the PLUS+1® XL104 Controller, consider the example of a propel function that is safety critical. The propel function relies on a Propel Command that is transmitted by a joystick utilizing two redundant Rheo (ResIN) – resistance inputs. The controller processes the input and controls the movement of the machine through a dual path control subsystem utilizing four PWM (current) outputs.

This Safety Function uses a 1oo1D architecture, with diagnostic/test equipment and secondary shutoff/de-energization methods.



This safety critical function uses one of the inputs as a test channel for comparison with the primary channel. The output actuators are driven in a half-H-bridge MF-PWM output configuration that uses the

Using the FMEDA results

return MF-PWM output to provide a comparison of the current measurement from the driving channel, as well as a de-energization disconnection.

The safety critical function has an overall failure rate that is the sum of controller subsystems used directly for the function. Test equipment and test channels do not directly contribute to the failure rate of the safety critical function. A Beta-factor may be used to describe the probability of a failure in the test channel at the same time as a failure in the safety function.

Please see chapter Common Cause Failure Mitigation for details on calculating a β-Factor that can be applied at the safety critical function level.

This safety critical function uses the following circuit blocks:
- (1x) Rheo (ResIN)
- (1x) Common Logic
- (2x) PWM (CrntOUT Safe)
- (1x) Rheo (ResIN) Test Channel
- (1x) Test Equipment Logic
- (2x) PWM (CrntOUT) Test Channel

In a machine application, the safety critical function could be operating in high demand. In a high demand function, only the dangerous, undetected failures are included when calculating the PFH. PFH is the probability that a system will fail dangerously, and not be able to perform its safety function when required. It is recommended that the designer or integrator review the requirements with Danfoss Power Solutions to help avoid understating PFH.

As a system metric, IEC 61508 defines SIL ratings based on the PFH of the safety function. Each SIL rating has an associated PFH which increases an order of magnitude for each increase in SIL rating. See table below.

ISO 13849 defines Performance Level ratings based on the PFH of the safety function. In addition, the Performance Level rating requires a level of Diagnostic Coverage. The following table shows the simplified relationship between Performance Level and Safety Integrity Level, and the reliability and diagnostic coverage requirements.

Performance Levels and Safety Integrity Levels for Category 2 High Demand Systems

Performance Level (PL)	Probability of dangerous failure per hour (PFH_D)	Diagnostic Coverage	Safety Integrity Level
d	>=10^{-7} to <10^{-6} ($MTTF_D$=High)	90%< DC <99% (Medium)	SIL 2
c	>= 10^{-6} to < $3x10^{-6}$ ($MTTF_D$=Medium to High)	60% < DC <90% (Low to Medium)	SIL 1
b	>= $3x10^{-6}$ to <10^{-5} ($MTTF_D$=Medium)	60% < DC <90% (Low to Medium)	SIL 1

A Probability of Failure per Hour (PFH) must be determined for each Safety Critical Function.

IEC 61508 analysis for the example function

Controller Subsystem	Qty	λ_S	λ_{DD}	λ_{DU}	Total λ_D (λ_{DD} + λ_{DU})	DC	Beta Factor
Rheo (ResIN) Primary	1	0	20.5 (.99x20.7)	0.2 (.01x20.7)	20.7 (13.6+7.1)	99%*	
Common Logic Total	1	95.5	1400	176	1576	88.8%	
MF-PWM (CrntOUT w/Safety FET)	2	33	67.9 (.99x68.6)	0.69 (.01x68.6)	68.6 (57+11.6)	99%*	
Primary Subtotal		**224**	**1556**	**177.6**	**1734**		
Rheo (ResIN) Test Channel	1	0	20.5 (.99x20.7)	0.2 (.01x20.7)	20.7 (13.6+7.1)	99%*	10%

Using the FMEDA results

IEC 61508 analysis for the example function (continued)

Controller Subsystem	Qty	λ_S	λ_{DD}	λ_{DU}	Total λ_D (λ_{DD} + λ_{DU})	DC	Beta Factor
Test Equipment Logic	1	27.9	123	8.5	131.5	93.6%	2%
PWM (CrntOUT Digital) Test Channel⊠	2	19.8	57.6 (.99x58.2)	0.58 (.01x58.2)	58.2 (48.6+9.6)	99%*	2%
TE Subtotal		**67.5**	**258.7**	**9.9**	**269.2**		
Safety Function Total (Primary + TE*Beta)		**291.5**	1556 + (.02x123+ .02x2x57.6 + .1x20.5) = **1563**	177.6 + (.02x8.5+ .02x2x.58+ .1x.2)= **177.8**	1734+ (.02x131.5+ .02x2x58.2 + .1x20.7)= **1741**	1563 / 1741 = **89.8%**	

* See note, below

NOTE: The implementation of the recommended diagnostics (see section Recommended Diagnostics) affects the system failure rate. In this example, the two input Rheo (ResIN) functions individually have a DC of 65.7%, but when used in a redundant configuration and compared against each other the diagnostic coverage is raised to 99%. Similarly, the PWM (CrntOUT) functions will have a DC of 99% when used with a low side PWM output in digital sinking mode when current measurements are compared between the high and low side drivers. A β-Factor of 10% is used for the Rheo (ResIn) inputs because they have insufficient common cause factor separation.

In this example PFH is the undetected failure rate λDU, which is 177.8 FITs (failures per 109 hours) or 17.8 x 10-7 dangerous failures per hour. The function diagnostic coverage is 89.8%.

The total contribution of the PLUS+1® XL104-XXXX to the PFH of this safety function is 177.8 FITs or 18% of the maximum allowable SIL 2 failure rate. The machine sensors and actuators can use the remaining 82% of the allowed failure rate to build the complete safety function. Note that at a higher average mission temperature profile these failure rates will increase, taking more of the allowable SIL 2 failure rate and leaving less for the machine sensors and actuators.

ISO 13849 analysis for the example function

Controller Subsystem	Qty	Total λD (λDD + λDU)	MTTFD Years	DCavg
Primary				
Rheo (ResIN) Primary	1	20.7 ⊠	5497	99%
Common Logic Total	1	1576	72.5	88.8%
MF-PWM (CrntOUT w/Safety FET)	2	68.6 x2	1666	99%
Primary Subtotal		**1734**	**65.8**	**89.8%**
Test Equipment				
Rheo (ResIN) Test Channel	1	20.7	5497	
Test Equipment Logic	1	131.5	866	
MF-PWMOUT (Digital) Test Channel⊠	2	58.2 x2	1963	
TE Subtotal		**269.2**	**424**	

Using Annex K of ISO 13849, PFH of this safety function computes to 420 FIT with the Category 2 architecture, CCF score of 65,channel $MTTF_D$ of 65.8 years and DC_{avg} of 89.8%. MTTFD of test equipment is 424 years which is greater than half of $MTTF_D$ of primary channel. The total contribution of the PLUS+1® XL104-XXXX to the PFH of this safety function is 420 FITs or 42% of the maximum allowable PL d failure rate. The machine sensors and actuators can use the remaining 58% of the allowed failure rate to build the complete safety function.

Common cause failure mitigation

ISO 13849-1 Appendix F defines an estimation of the effect of Common Cause Failures (CCF) in Table F.1 The PLUS+1® XL104 Controller scores 65 in measures against CCF in Design/Application/Experience per sections 3, 4, 5 and 6. Sections 1 and 2 are highly dependent on the machine and application implementation and are not included in the score for the PLUS+1® XL104 Controller. A score of 65 or higher is needed to meet the requirements of ISO 13849-1.

Dangerous undetected faults of primary subsystem and test equipment can be treated differently during PFH calculations for a 1oo1D architecture. The faults of test equipment are multi-point faults as they can cause a violation of a safety function only in combination with an independent fault in the primary subsystem being monitored. A β-factor, dependent on CCF evaluation, can be applied to dangerous undetected failure rates of the test equipment accounting for common cause failures between the primary subsystem and the test equipment.

IEC 62061:2021 Annex E defines an estimation of the effect of CCF that can be used to estimate the β-factor in PFH calculations. The PLUS+1® PCXXX scores 67 in measures against CCF using this method. References 1a, 1b, 2, 4 and 5 are highly dependent on the machine and application implementation and are not included in the score for the PLUS+1® PCXXX.

Table E-2 from IEC 62061:2021 shows β-factors to be used based on this scoring method:

Overall CCF Score	β-Factor
≤ 35	10%
36 to 65	5%
66 to 85	2%
86 to 100	1%

Section 1 of Table F.1 mentions various measures against CCF based on Separation and Segregation. The following discussion can be used to implement better CCF separation when using the PLUS+1® XL104 Controller's Input and Output circuits.

Digital Outputs on Safebank groups

The PLUS+1® XL104 Controller DOUT (4A) Safebank groups are implemented in pairs of outputs. The Safebank will enable or disable battery power to both Digital Outputs on that Safebank.

Safe Bank	Digital Output
1	C1p36
	C1p46
2	C2p35
	C2p45
3	C2p36
	C2p46

Common cause failure mitigation

Multifunction Current output safety function pairing recommendations

The PLUS+1® XL104 Controller Multifunction Current outputs are implemented as groups of four, sharing common amplifier and digital IC's. Their current feedback signals are grouped onto different A-D converters on the MCU for peripheral and package CCF separation. The best CCF separation for a H-bridge function uses two Current outputs from different CCF groups, different ADC groups, and different MCU Package Groups.

Source Groupings (with Safety FET)			
SFF Group 1			
ADC	**MCU**	**PWM**	**Output**
ADC G0	PKG G1	PWM G1	C1p37
			C1p38
			C1p47
			C1p48
SFF Group 2			
ADC	**MCU**	**PWM**	**Output**
ADC G3	PKG G3	PWM G2	C2p31
			C2p32
			C2p41
			C2p42

Sink Groupings			
SFF Group 3			
ADC	**MCU**	**PWM**	**Output**
ADC G3	PKG G3	PWM G5	C2p39
			C2p40
			C2p49
			C2p50
SFF Group 4			
ADC	**MCU**	**PWM**	**Output**
ADC G0	PKG G1	PWM G3	C1p31
			C1p32
			C1p41
			C1p42

The recommended combination for an half H-bridge function should use one output from SFF Group 1 and one output from SFF Group 3, or one output from SFF Group 2 and one output from SFF Group 4.

The Multifunction Current outputs in PWM Group 4 (C1p39, C1p40, C1p49, C1p50) have less MCU package separation from the other PWM groups and are thus less desirable to use for a safety function. If used in a H-bridge configuration, they should be used as a sinking output paired with a Source output from SFF Group 1 or Group 2.

Analog Input Safety Function CCF information

Analog Input signals (DIN/AIN) are implemented in groups of four, sharing common amplifier IC's and circuit pathways. The analog inputs are grouped onto different A-D converters on the MCU for peripheral and package CCF separation. Inputs for the same safety function should use as many different groups as possible. It is not recommended to use two inputs from the same DAGx group together due to poor package CCF separations. MCU package group APG2 has insufficient package separation from either APG1 or APG3 to overcome MCU package CCF considerations.

Common cause failure mitigation

Analog Input SFF Group 1			
Input	**ADC**	**MCU**	**Signal**
DA G1	ADC G0	PKG G1	C1p06
			C1p07
			C1p11
			C1p12

Analog Input SFF Group 2			
Input	**ADC**	**MCU**	**Signal**
DA G2	ADC G0	PKG G1	C1p26
			C1p27
			C1p28
			C1p29

Analog Input SFF Group 3			
Input	**ADC**	**MCU**	**Signal**
DA G3	ADC G3	PKG G3	C2p05
			C2p06
			C2p07
			C2p08

Analog Input SFF Group 4			
Input	**ADC**	**MCU**	**Signal**
DA G4	ADC G3	PKG G3	C2p01
			C2p02
			C2p03
			C2p04

Analog Input SFF Group 5			
Input	**ADC**	**MCU**	**Signal**
DA G5	ADC G0	PKG G1	C1p05
			C1p15
			C1p25
			C1p30

Analog Input SFF Group 6			
Input	**ADC**	**MCU**	**Signal**
DA G6	ADC G1	PKG G2*	C1p10
			C1p20
			C1p21
			C1p22

* MCU group PKG G2 has less package separation from either APG1 or APG3 and cannot be considered as fully independent.

Common cause failure mitigation

Analog Input SFF Group 7			
Input	**ADC**	**MCU**	**Signal**
DA G7	ADC G2	PKG G3	C1p16
			C1p17
			C1p18
			C1p19

Digital Input safety function CCF information

Digital Input signals (DIN) are implemented in groups of four to eight, sharing common receiver IC's and input registers. Package CCF for signals on one input register require using non-adjacent pins; the pin order is shown in the Reg Pin column. A good rule is to allow for a 2-pin separation, for example, pins 1 and 3. Signals with Reg Pin A can be used with any other signal in their Register Group as their pin location is further away from any of the other pins.

Input	Register	Reg Pin	Signal
G1	A	A	C2p25
	A	1	C2p23
	A	2	C2p24
	A	3	C2p15
	A	4	C2p14
	A	5	C2p21
G2	A	6	C2p22
	A	7	C2p11
	B	A	C2p12
	B	1	C2p13
	B	2	C2p19
	B	3	C2p20
G3	B	4	C2p30
	B	5	C2p17
	B	6	C2p18
	B	7	C2p27
	C	A	C2p28
	C	1	C2p29
G4	C	2	C2p26
	C	3	C2p16

ENGINEERING TOMORROW

Products we offer:

- Cartridge valves
- DCV directional control valves
- Electric converters
- Electric machines
- Electric motors
- Gear motors
- Gear pumps
- Hydraulic integrated circuits (HICs)
- Hydrostatic motors
- Hydrostatic pumps
- Orbital motors
- PLUS+1® controllers
- PLUS+1® displays
- PLUS+1® joysticks and pedals
- PLUS+1® operator interfaces
- PLUS+1® sensors
- PLUS+1® software
- PLUS+1® software services, support and training
- Position controls and sensors
- PVG proportional valves
- Steering components and systems
- Telematics

Hydro-Gear
www.hydro-gear.com

Daikin-Sauer-Danfoss
www.daikin-sauer-danfoss.com

Danfoss Power Solutions is a global manufacturer and supplier of high-quality hydraulic and electric components. We specialize in providing state-of-the-art technology and solutions that excel in the harsh operating conditions of the mobile off-highway market as well as the marine sector. Building on our extensive applications expertise, we work closely with you to ensure exceptional performance for a broad range of applications. We help you and other customers around the world speed up system development, reduce costs and bring vehicles and vessels to market faster.

Danfoss Power Solutions – your strongest partner in mobile hydraulics and mobile electrification.

Go to www.danfoss.com for further product information.

We offer you expert worldwide support for ensuring the best possible solutions for outstanding performance. And with an extensive network of Global Service Partners, we also provide you with comprehensive global service for all of our components.

Local address:

Danfoss
Power Solutions (US) Company
2800 East 13th Street
Ames, IA 50010, USA
Phone: +1 515 239 6000

Danfoss
Power Solutions GmbH & Co. OHG
Krokamp 35
D-24539 Neumünster, Germany
Phone: +49 4321 871 0

Danfoss
Power Solutions ApS
Nordborgvej 81
DK-6430 Nordborg, Denmark
Phone: +45 7488 2222

Danfoss
Power Solutions Trading (Shanghai) Co., Ltd.
Building #22, No. 1000 Jin Hai Rd
Jin Qiao, Pudong New District
Shanghai, China 201206
Phone: +86 21 2080 6201