PVED-CLS Valve Controller For Electro-hydraulic Steering

Safety Manual

Software version 2.00

Important User Information

Danfoss is not responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included for illustration purposes. Due to the many variables and requirements associated with any particular installation, Danfoss cannot assume responsibility or liability for the actual used bases on the examples and diagrams.

Reproduction of whole or part of the contents of this safety manual is prohibited.

The following notes are used to raise awareness of safety considerations.

Warning ⚠	Identifies information about practices or circumstances that can cause a hazardous situation, which may lead to personal injury or death, damage or economic loss.
Attention ⚠	Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.
Important	Identifies information that is critical for successful application and understanding of the product.
Recommendation	Identifies a typical use of a functionality or parameter value. Use recommendations as a starting point for the final configuration process of the system.

Document references

Literature
PVED-CLS communication protocol revision 3.36
OSPE Steering valve, SASA sensor, Technical information, 11068682
PVED-CLS KWP2000 protocol, revision 1.75 (L1412764)
PVED-CLS Technical Specification, BC00000355
PVED-CLS User Manual, 2.00
EHPS Steering Valve, PVE Actuation, OSPCX CN Steering Unit, 520L0521
PVED-CLS firmware release note, 2.00
OSPE steering valve service manual, L1506577
EHPS steering valve service manual, AX00000235

Definitions and Abbreviations

DTC	Diagnostic Trouble Code
ECU	Electronic Control Unit
EHPS	Electro-Hydraulic Power Steering
OSPE	Orbital Steering Product – Electro-hydraulic
SEHS	Safe Electro-Hydraulic Steering
MMI	Man-Machine Command Interface
XID	Extended Message Identifier
PVED-CLS	Proportional Valve Digital – Closed Loop - Safety – here the valve controller
SPN	Suspect Parameter Number
COV	Cut-Off Valve
SVB	Solenoid Valve Bridge
CAT	Safety category per ISO 13849 and ISO 25119
DC	Diagnostic Coverage
MTTFd	Mean time to potentially dangerous failure
CCF	Common Cause Failure
SIL	Safety Integrity Level
PL	Performance level per ISO 13849
AgPL	Agricultural Performance Level per ISO 25119
SFF	Safe Failure Fraction
PFH	Probability for dangerous failure per hour
PFD	Probability of dangerous failure on Demand
FMEA	Failure Mode and Effects Analysis
FMEDA	Failure Mode and Effects and Diagnostic Analysis
SC	Systematic capability
WAS	Wheel Angle Sensor
SASA	Steering Angle Sensor Absolute
AUX	Auxiliary
PSAC	Parameter Sector Access Code
IR	Internal Resolution [-1000;1000]
OEM	Original Equipment Manufacturer
EHi-E	Electro-Hydraulic Inline Valve – Electronic Override
EHi-H	Electro-Hydraulic Inline Valve – Hydraulic Override
EH	Electro-Hydraulic
SVC	Solenoid Valve Control – Control algorithm for PVED-CLS

Table of Contents

1 Introduction

This Safety manual explains how the PVED-CLS can be used for realizing functional safety and safety functions up to Safety Integrity Level 2 (SIL 2), Performance Level d (PL d) and Agricultural Performance Level d (AgPL d) for off-road applications and Safety Integrity Level 3 (SIL 3), Performance Level e (PL e) and Agricultural Performance Level e (AgPL e) for safe on-road operation mode. It describes the safety functions, requirements, safety related parameters, application verification and provides information on installing, configuring, and troubleshooting the PVED-CLS.

The PVED-CLS can be used together with four different valve sub-systems:

OSPE

The OSPE valve sub-system is a one-piece steering unit, comprised by an orbital steering unit and an electro-hydraulic steering valve. With the PVED-CLS powered, the OSPE can steer either by summing the flow from the orbital steering unit and the electro-hydraulic steering valve, this steering mode requires a steering wheel sensor, or by the electro-hydraulic steering valve alone, this steering mode requires an AUX steering device or auto-guidance system. If the PVED-CLS is depowered, the OSPE will steer solely by the orbital steering unit. The number of available safety functions and functionality provided by the PVED-CLS used with an OSPE valve sub-system, is depending on inputs from sensor sub-systems. However, as a minimum a steering wheel sensor, vehicle speed sensor and a Man-Machine Interface is required.

EHPS

The EHPS valve sub-system is a pilot operated steering valve, which can be controlled either by a pilot steering unit, the PVED-CLS or both. If the PVED-CLS is depowered the EHPS will be controlled by the pilot steering unit only. With the PVED-CLS powered, the EHPS can either be controller by both the pilot steering unit and the PVED-CLS, this steering mode requires a steering wheel sensor, or by the PVED-CLS alone, this steering mode requires an AUX steering device or auto-guidance system. The number of available safety functions and functionality provided by the PVED-CLS used with an EHPS valve sub-system, is depending on inputs from sensor sub-systems. However, as a minimum a steering wheel sensor, a wheel angle sensor, vehicle speed sensor and a Man-Machine Interface is required.

EHi-E

The EHi-E valve sub-system is an inline electro-hydraulic steering valve, which can be inserted in a steering system, between a traditional orbital steering unit and the steering cylinder. The EHi-E valve sub-system together with a traditional orbital steering unit resembles the OSPE valve sub-system, so with the PVED-CLS powered, the EHi-E can steer either by summing the flow from the traditional orbital steering unit and the electro-hydraulic steering valve, this steering mode requires a steering wheel sensor, or by the electro-hydraulic steering valve alone, this steering mode requires an AUX steering device or auto-guidance system. If the PVED-CLS is depowered, the steering will rely solely on the traditional orbital steering unit. The number of available safety functions and functionality provided by the PVED-CLS used with an OSPE valve sub-system, is depending on inputs from sensor sub-systems. However, as a minimum a steering wheel sensor, vehicle speed sensor and a Man-Machine Command Interface is required.

EHi-H

The EHi-H valve sub-system in an inline electro-hydraulic steering valve, which can be inserted in a steering system, between a traditional orbital steering unit and the steering cylinder. The EHi-H valve sub-system is a variant of the EHi-E valve sub-systems, which does not require a steering wheel sensor. With the PVED-CLS powered, the EHi-H valve sub-system can utilize electro-hydraulic steering features like, AUX steering or auto-guidance steering. These electro-hydraulic steering features will be disengaged using the hydraulic override functionality, build-in partly in the PVED-CLS and partly in the EHi-H. Since the system does not comprise a steering wheel sensor, variable steering cannot be obtained with an EHi-H valve sub-system. With the PVED-CLS depowered, the steering will rely solely on the traditional orbital steering unit. The number of available safety functions and functionality provided by the PVED-CLS used with an EHi-H valve sub-system, is depending on inputs from sensor sub-systems. However, as a minimum a vehicle speed sensor and a Man-Machine Interface is required.

Important

Use this Safety manual if you are responsible for designing, installing, configuring, or troubleshooting safety applications that use the PVED-CLS. Please read section 2.2 before using this safety manual.

1.1 TRACEABILILTY TAGS

Unique tags in the form of SSM_<number> are associated to the functional safety realized in the PVED-CLS for traceability purposes.

Future changes to this document will be described by changes to tags in the revision history to enable end-users to perform an impact analysis.

The document layout and section numbers may change without notice.

1.2 PVED-CLS SOFTWARE CONFIGURATION SSM_000

The content of this safety manual is valid for the following PVED-CLS software configuration.

Software component	Version	Software name	Program date	Program Time
PVED-CLS firmware (.hex)				
Boot-loader software version	3.85	BOOT_CLS-_M_R385_KWP2000-_11153472_-rrr	13.03.15	04:38 PM
Main application software version	2.00	APP-_CLS-_M_R200_SEHS----_11153340_-B14	25.10.17	06:14PM
Safety application software version		APP-_CLS-_S_R200_SEHS----_11153341_-B14		06:17PM
Service tool				
PLUS+1 service tool	9.1.6			
PLUS+1 service tool pages P1D	2.00	PVED-CLS_2.00_rev_D	NA	NA
PLUS+1 service tool PLG	2.00	APP-_CLS-_M_R200_SEHS----_11153340_-B14	25.10.17	06:14PM
		APP-_CLS-_S_R200_SEHS----_11153341_-B14		06:17PM

See PVED-CLS 2.00 firmware release note for revision history.
The software configuration can be read out by the PLUS+1 service tool.

2 Safety Concept

2.1 SAFETY CERTIFICATION SSM_001

The PVED-CLS steering valve controller is certified for use in off-road safety applications up SIL2 according to IEC 61508, PL d according to ISO 13849 and AgPL d according to ISO 25119.

The certificate for the PVED-CLS valve controller can be found in the document PVED-CLS Functional Safety Annex. The PVED-CLS Functional Safety Annex can be found on the Danfoss homepage via following link:
HTTP://POWERSOLUTIONS.DANFOSS.COM/PRODUCTS/STEERING/PVED-CLS-INTELLIGENT-STEERING-SUB-SYSTEM/

The certificate scope is for the generic PVED-CLS valve controller for use in safety-related applications as follows; for off-road applications, safe electro-hydraulic steering is ensured by metering out a safe steering flow as a function of selected steering mode, input steering command, vehicle speed and steered wheel angle.
For on-road operation, the safe state is achieved by de-energizing the PVED-CLS valve controller.

Important

- The certificate does not cover safe on-road system to SIL 3, PL e and AgPL e as it requires external circuitry, which is not in scope of the assessment.
- The certification is not a guarantee for that the realized functional safety is sufficient for any machine. The OEM system integrator is responsible for analyzing the hazard and risks for a particular machine and evaluate if the risks are sufficiently reduced by the provided safety functions. The application of the PVED-CLS and valve sub-system is subject for a separate safety life-cycle.

2.2 IMPORTANT SAFETY CONSIDERATIONS SSM_002

Attention

⚠

The OEM system integrator is responsible for:

- Having an organization that is responsible for functional safety of the system.
- Ensuring that only authorized and trained personnel perform functional safety related work.
- Choosing reliable components.
- Completing a system hazard & risk analysis.
- Reassessing the hazard & risk every time the system is changed.
- Ensuring that the derived risks are properly reduced by the safety functions provided by the PVED-CLS.
- Certification and homologation of the entire system to the desired risk reduction level.
- Installation, set-up, safety assessment and validation of the interfacing sensor sub-systems.
- Parameter configuration of the application software in accordance with this safety manual.
- Validating that the safety functions reduce the risks as expected.
- Any related non-safety standards should be fulfilled for the application and its components.
- Verify the environmental robustness suitability of the PVED-CLS to installation in the final system in its surrounding environment.
- Periodically inspect for errata information updates, see section 3.

3 Errata information

The latest errata information is always available on the Danfoss homepage via following link:
HTTP://POWERSOLUTIONS.DANFOSS.COM/PRODUCTS/STEERING/PVED-CLS-INTELLIGENT-STEERING-SUB-SYSTEM/

It contains errata information for:

- PVED-CLS boot loader
- PVED-CLS application
- Documentation
- PLUS+1 Service tool
- Other topics related to the steering system

If further information to any errata is required, please contact your nearest Danfoss Product Application Engineer

Attention ⚠	• **The system integrator and/or responsible for the target system is advised to periodically observe the errata information as new information will be added as needed.** • **Optionally, the system integrator and responsible for the system, after commissioning, may sign up for the email notification service.**

4 Safety related specifications for PVED-CLS and valve sub-systems

The safety related specifications for safety loop calculations are given for three different modes of operation:

- PVED-CLS and valve sub-system operational mode for safe off-road functionality
- PVED-CLS and valve sub-system operational mode for safe on-road functionality
- PVED-CLS and valve sub-system de-energized for safe on-road functionality

4.1 OFF-ROAD MODE - SYSTEM OPERATIONAL SSM_003

- The probabilistic calculations are based on FMEDA calculations according to IEC 61508.
- The calculations are valid for off-road application mode and related safety functions.
- All safety functions and related hardware are included.
- The road switch for on-road mode is not included in this calculation.
- Any sensor sub-systems are not included as it depends on the system. See section 8.
- The CAN bus contributes less than 1 % of SIL2 due to the applied safety protocol and is thus omitted in safety related calculations.

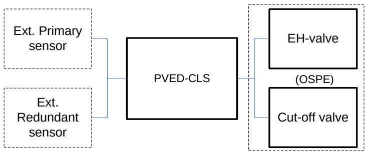


Figure 1: Simplified block diagram of system utilizing PVED-CLS and OSPE valve sub-system.

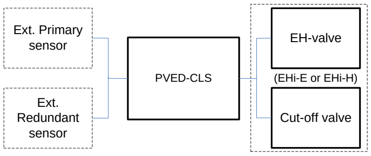


Figure 2: Simplified block diagram of system utilizing PVED-CLS and EHi-E or EHi-H valve sub-system.

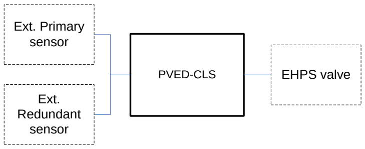


Figure 3: Simplified block diagram of system utilizing PVED-CLS and EHPS valve sub-system.

Safety parameter	Specification	Description
SIL	2	IEC 61508 ed. 1 The FMEDA calculation assumes the use of redundant analogue WAS with inverted characteristics.
PFH	$5.77 \cdot 10^{-8}$ [1/h]	
Component type	B	
SFF	98 %	
DC	97 %	
Architecture /category (IEC 61508)	1002	
Proof test interval/mission time	20 years	
Reliability handbook	Siemens SN29500	Calculations are performed at an average temperature equal to 80 °C
Fault exclusion	Mechanical valve parts (EH-valve, EH-main spool, cut-off valve, cut-off spool)	On demanding the safe state, both valves do not fail simultaneously. At least one valve will always block the EH steering flow to the cylinder. Fault accumulation is addressed by OSPE EH-valve and OSPE Cut-off valve test.
OSPE EH-valve test	On-line testing	Direct monitoring by a LVDT sensor.
OSPE Cut-off valve test	Intermittent full stroke test.	Indirect monitoring by test pilot pressure test. Test performed on changing to off-road mode and prior to executing off-road steering functionality.
AgPL/PL	d	Maximum achievable performance level
MTTFd per channel	36 years	ISO 13849, ISO 25119
DCavg per channel	97 % / (95 %)	ISO 13849 / (ISO 25119, lowest of the two channels)
Category PVED-CLS and valve sub-system	3	When using with OSPE, EHi-E or EHi-H valve. ISO 13849, ISO 25119
	2	When using with EHPS valve. ISO 13849, ISO 25119
CCF analysis	>65	ISO 13849, ISO 25119
Software Requirement Level	SIL2 / SRL3	IEC 61508, ISO 13849 / ISO 25119
Systematic Capability (SC)	2	IEC 61508

Source: Danfoss PVED-CLS/OSPE/EHPS/EHi FMEDA.

4.2 SAFE ON-ROAD MODE - SYSTEM OPERATIONAL SSM_004

The electro-hydraulic steering functionalities provided by the PVED-CLS and valve sub-systems are not designed for on-road use. The PVED-CLS and valve sub-system shall therefore be brought in a safe state while the vehicle is being used on public roads.

- The probabilistic calculations are based on FMEDA calculations according to IEC 61508.
- Non-relevant safety parts in the PVED-CLS are excluded in the calculation of the safety related specifications.
- Higher safety integrity levels can be achieved by adding additional components.
- See section 14 for different architectures for on-road modes.

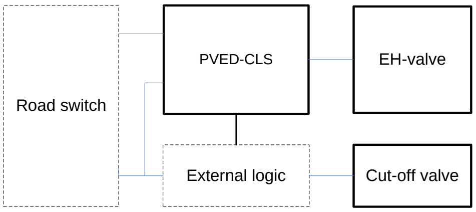


Figure 4: Simplified block diagram of system utilizing PVED-CLS and OSPE, EHi-E or EHi-H valve sub-system.

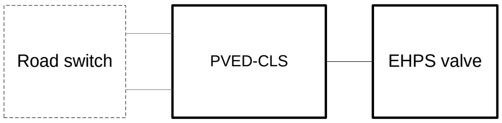


Figure 5: Simplified block diagram of system utilizing PVED-CLS and EHPS valve sub-system.

The below data is valid for the safe on-road switch channel containing the PVED-CLS and solenoid valve bridge. For specification on the electro-mechanical channel see section 14.

Safety parameter	Specification	Description
SIL	2	IEC 61508 ed. 1 The FMEDA calculation assumes the use of redundant analogue WAS with inverted characteristics. All circuitry including circuitry for diagnostics is included except LED, temperature sensor and JTAG interface.
PFH	$6.08 \cdot 10^{-8}$ [1/h]	
Component type	B	
SFF	98 %	
DC	97 %	
Architecture /category (IEC 61508)	1002	
Proof test interval/mission time	20 years	
Reliability handbook	Siemens SN29500	Calculations are performed at an average temperature equal to 80 °C
Fault exclusion	Mechanical valve parts (EH-valve, EH-main spool, cut-off valve, cut-off spool)	On demanding the safe state, both valves do not fail simultaneously. At least one valve will always block the EH steering flow to the cylinder. Fault accumulation is addressed by OSPE EH-valve and OSPE Cut-off valve test.
OSPE EH-valve test	On-line testing	Direct monitoring by a LVDT sensor.
OSPE Cut-off valve test	Intermittent full stroke test.	Indirect monitoring by test pilot pressure test. Test performed on changing to off-road mode and prior to executing off-road steering functionality.
AgPL/PL	d	Maximum achievable performance level
MTTFd per channel	57 years	Optimized value for this Safety function. ISO 13849, ISO 25119.
DCavg per channel	97 % / (95 %)	ISO 13849 / (ISO 25119, lowest of the two channels)
Category PVED-CLS and valve sub-system	3	When using with OSPE, EHi-E or EHi-H valve. ISO 13849, ISO 25119
	2	When using with EHPS valve. ISO 13849, ISO 25119
CCF analysis	>65	ISO 13849, ISO 25119
Software Requirement Level	SIL2 / SRL3	IEC 61508, ISO 13849 / ISO 25119
Systematic Capability (SC)	2	IEC 61508

Source: Danfoss PVED-CLS/OSPE/EHPS/EHi FMEDA.

Important

- The safety related specifications are only valid for safe on-road application.

- The safety related specifications are only valid for the PVED-CLS and valve sub-system and shall be included when composing an architecture achieving higher safety integrity levels.

4.3 SAFE ON-ROAD MODE - DE-ENERGIZE SSM_005

The electro-hydraulic steering functionalities provided by the PVED-CLS and valve sub-systems are not designed for on-road use.

- De-powering the PVED-CLS and valve sub-systems by disconnection battery power supply will bring the system in a safe state which is suitable for on-road operation by OSP control.
- No functional safety is present when the PVED-CLS is de-energized.

Set-up

The below architecture de-energizes the PVED-CLS and valve sub-systems by disconnecting any battery power to the PVED-CLS and valve sub-system.

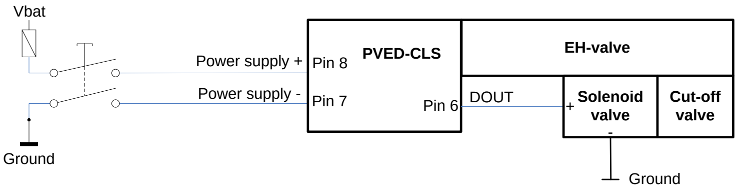


Figure 6: OSPE, EHi-E and EHi-H valve sub-system

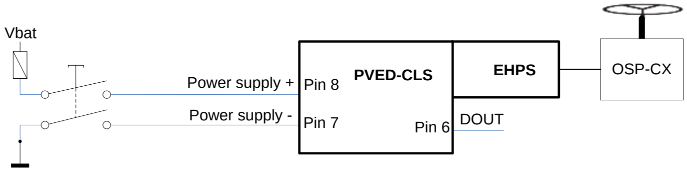


Figure 7: EHPS valve sub-system

Important

The system integrator shall:

- Take responsibility for choosing reliable cables and switch/circuit breaking components.
- Regard the standards ISO25119, ISO 13849-2 appendix A and D, IEC 60947-5-1 and IEC 60204.
- Ensure that the road switch performs the safety function i.e. disconnecting battery power to AgPL/PL e.
- Ensure that the switch is suitable for the purpose and meets the target SIL.
- Perform an FMEA to address dangerous failures and common cause failure modes.
- For OSPE valve systems, fault exclusion applies as follows. On disconnecting battery power to the PVED-CLS and valves, both valves do not fail simultaneously. At least one valve will always block the EH steering flow to the cylinder.
- The EH-valve is tested at power-up and on-line when the PVED-CLS is used in off-road mode.
- The cut-off valve is tested intermittently on every PVED-CLS mode change to off-road functionality.
- For EHPS valve systems, fault exclusion applies as follows; on disconnection battery power to the PVED-CLS and EHPS valve, the OSP-CX does not fail in piloting the EHPS main spool with a pilot pressure up to 40 Bar.
- Faults in the PVED-CLS cannot prohibit the OSP-CX from controlling the EHPS main spool.
- Refer to PVED-CLS Technical Specification for information on electrical characteristics for the PVED-CLS.

Warning ⚠	**The system integrator shall ensure that the PVED-CLS and valve sub-system are brought into a safe state while the vehicle is being used on public roads.**

4.4 SAFE STATE SSM_006

Achieving the safe state relies on a de-energize principle and is achieved when the EH-steering flow is isolated from the steering cylinder and steering is solely controlled by the steering orbital. In the safe state, all safety controlled outputs, i.e. solid state power switches, are in their safe state (de-energized).

OSPE

For systems using an OSPE valve sub-system, the safe state is achieved by one or both of the following states:

- The EH-valve main spool of the EH steering valve is in neutral position.
- Cut-off valve spool is in blocked position.

EHPS

For systems using an EHPS valve sub-system, the safe state is achieved by one or both of the following states:

- Battery supply for Solenoid Valve Bridge is switched off.
- Hydraulically override the PVED-CLS SVB pilot flows by stroking the EHPS main spool with a hydraulic pilot pressure up to 40 Bar produced by activating the OSP-CX steering unit.

EHi

For systems using an EHi-E or EHi-H valve sub-system, the safe state is achieved by one or both of the following states:

- The EH-valve main spool of the EH steering valve is in neutral position.
- Cut-off valve spool is in blocked position.

If the PVED-CLS hardware or software detects a failure or fails to function, the safe state will be demanded. One or more diagnostic trouble codes related to the detected failure will be broadcast on the CAN bus. Refer to the PVED-CLS User manual for information on diagnostic trouble codes.

Important

- If the PVED-CLS enters safe state, the operator will only be able operate the vehicle with the steering wheel.
- If a steering wheel program is active when the PVED-CLS enters the safe state, the steering wheel ratio lock-to-lock will increase immediately to lock-to-lock ratio given by the orbital displacement. The system integrator shall evaluate if an immediately change in lock-to-lock ratio can lead to a hazard.
- Give audible and visible alarm to operator when the safe state is entered, to inform the operator that the vehicle can exclusively be steered by the steering wheel.

4.4 RESET - RECOVERING FROM THE SAFE STATE SSM_007

The PVED-CLS cannot leave the safe state by normal application interaction. Resetting the PVED-CLS from safe state can be done by any of the below methods:

- Power-cycling battery supply to the PVED-CLS
- Performing a soft-reset by J1939 CAN command (see PVED-CLS communication protocol documentation)
- Perform a jump to and out of boot-loader via KWP2000 start and stop diagnostic session services (see PVED-CLS KWP2000 protocol documentation).

All the above-mentioned methods to reset the PVED-CLS from safe state, will force a full Power-on-Self-Test (POST) of the PVED-CLS.

4.5 SAFETY FUNCTION RESPONSE TIME SSM_008

The safety response time is defined as the period of time between a fault is first observed by the diagnostics and the time by which the safe state has been achieved, e.g. de-energizing the solenoid valves to bring the valve spool(s) within the hydraulic deadband (no valve output).

Safety function	Fault reaction/risk mitigation	Safety response time	
		OSPE valve	EHPS valve
Safe EH steering shut-off (entering safe state)	Safe state	160 ms	200 ms
Vehicle speed triggered EH steering shut-off		70 ms	110 ms
Safe on-road mode (switch to safe on-road mode)	Safe on-road mode	70 ms	110 ms
Safe EH-steering	n.a.	10 ms	

Table 1: Safety response time – Safety functions

- The 'Safe EH steering shut-off' (entering safe state) includes a 100ms detection confidence interval.
- The response time for 'Vehicle speed triggered EH steering shut-off' is comprised of:
  a) a 10ms control loop period (react and switch off valve drivers)
  b) the time it takes for the valve spools to close the steering flows (maximum spool stroke)
- The safety related control function 'Safe EH-steering' is executed every 10ms.
- The 'Safe on-road mode' is demanded by the road switch and switches to safe on-road mode within
  a) a 10ms control loop period (react and switch off valve drivers)
  b) the time it takes for the valve spool to close the steering flows (maximum spool stroke).
- The reaction time for the OSPE valve spool to reach neutral position (safe state) from full stroke is typically 60ms for normal working temperature/viscosity.
- The reaction time for the OSPE cut-off valve to reach blocked state (safe state) from full stroke is typically 60ms for normal working temperature/viscosity.
- The reaction time for the EHPS valve spool to reach blocked state (safe state) from full stroke is typically 100ms for normal working temperature/viscosity.

4.6 MONITORING FUNCTION RESPONSE TIME SSM_009

Monitoring	Fault reaction/risk mitigation	Safety response time	
		OSPE valve	EHPS valve
Internal hardware and software	Safe state	160 ms	200 ms
External sensor monitoring (note 1)		160 ms	200 ms
Valve main spool monitoring		250 ms (note 3)	290 ms (note 3)
Fault Detection Algorithm (note 2)		500-1000 ms	
Solenoid valve connection monitoring		560 ms	n.a.
Guidance Machine Command time-out	Disengage auto-guidance	200 ms	

Table 2: Safety response time – Monitoring functions

Note 1: Sensor CAN message time-outs are configurable which has a direct impact on the fault reaction time.
Note 2: FDA is configurable. The resulting fault detection time depends on the parameter settings.
Note 3: The spool monitoring fault reaction times are valid when the hydraulics has reached normal working temperature/viscosity.

5 PVED-CLS Safety Function Overview

5.1 SAFETY FUNCTIONS SSM_010

The PVED-CLS valve controller features the below safety functions which can be employed and configured by the system integrator. Only elements required for the realization is shown. Elements or signals required for a given steering functionality to work and which is impacted by a safety function is not included in the overview.

	Operator interface						Sensor		Valve sub-system						
Safety function of the PVED-CLS valve controller	Road switch	Man-Machine Command Interface (MMI)	Steering wheel sensor sub-system / SASA sensor	Auxiliary steering device (mini-wheel)	Auxiliary steering device (joystick)	Auto-guidance controller	Wheel Angle Sensor sub-system (CAN, analogue)	Vehicle speed sensor sub-system	EHPS valve sub-system	OSPE valve sub-system	EHi-E valve sub-system	EHi-H valve sub-system	Relay / circuit breaking arrangement	SIL 2, PL d, AgPL d	SIL 3, PL e, AgPL e
SSM_023 Safe on-road mode (OSPE, EHi-E and EHi-H)	•								-	•	•	•	•		x
SSM_024 Safe on-road mode (EHPS)	•								•	-	-	-	o	x	
SSM_030 Fault Detection Algorithm – FDA			•	o	o		•	•	o	o	o	-		x	
SSM_032 Auto-guidance and auxiliary steering disengage by steering wheel / SASA sensor			•						o	o	o	-		x	
SSM_033 Auto-guidance disengage at low speed/parking								•	o	o	o	o		x	
SSM_034 Vehicle speed dependent flow limitation (auto-guidance)								•	o	o	o	o		x	
SSM_035 Vehicle speed dependent wheel angle limitation (auto-guidance)							•	•	o	o	o	o		x	
SSM_036 Auto-guidance disengage by auxiliary steering device (mini-steering wheel)				•					o	o	o	o		x	
SSM_037 Auto-guidance disengage by auxiliary steering device (joystick)					•				o	o	o	o		x	
SSM_038 Vehicle speed dependent flow limitation (auxiliary mini-steering wheel)				•				•	o	o	o	o		x	
SSM_039 Safe auto-calibration stop			•						o	o	o	-		x	
SSM_055 Safe EH steering shut-off (safe state)									o	o	o	o		x	
SSM_056 Vehicle speed EH steering shut-off								•	o	o	o	o		x	
SSM_057 Safe EH steering flow command		•	•	o	o	o	o	•	o	o	o	o		x	
SSM_058 MMI steering program change lock-out		•						•	o	o	o	o		x	
SSM_059 Steering device change lock-out								•	o	o	o	o		x	
SSM_060 Vehicle speed dependent flow limitation (steering wheel)			•					•	o	o	o	-		x	
SSM_061 Vehicle speed dependent flow scaling (open loop auxiliary joystick)					•			•	o	o	o	o		x	
SSM_062 Vehicle speed dependent wheel angle limitation (Auxiliary closed loop joystick)					•		•	•	o	o	o	o		x	
SSM_063 Safe Closed loop joystick engage					•		•		o	o	o	o		x	
SSM_067 Hydraulic override									-	-	-	•		x	
SSM_068 Hydraulic override disengage									-	-	-	•		x	
SSM_069 Hydraulic override of auto-calibration									-	-	-	•		x	
SSM_070 Hydraulic override of auto-guidance and auxiliary steering									-	-	-	•		x	

•	Element of the safety function.
o	Optional/system dependent for the realization of the safety function.
x	The maximum achievable risk reduction.
-	Not applicable for the given valve sub-system.

Important

- A hazard and risk analysis must be conducted before using the safety functions.

- The system integrator must evaluate if the safety functions are suitable for reducing a certain risk.
- The system integrator must configure and validate the safety function in the final installation.
- Not all safety functions are available when the wheel angle sensor is disabled.

5.2 HAZARDOUS SCENARIOS – SAFETY FUNCTION MAPPING

The below table can be used for mapping the available safety functions to risk scenarios. All safety functions which may be used for addressing a certain risk scenarios are marked. Not all safety functions may be needed for addressing a certain risk scenario. The system integrator shall ensure that all risk scenarios are adequately addressed.

	Available safety functions																						
Risk scenarios	SSM_023 Safe on-road mode (OSPE system)	SSM_024 Safe on-road mode (EHPS system)	SSM_032 Auto-guidance and auxiliary steering disengage by steering wheel / SASA sensor	SSM_033 Auto-guidance disengage at low speed/parking	SSM_034 Vehicle speed dependent flow limitation (auto-guidance)	SSM_035 Vehicle speed dependent wheel angle limitation (auto-guidance)	SSM_036 Auto-guidance disengage by auxiliary steering device (mini-steering wheel)	SSM_037 Auto-guidance disengage by auxiliary steering device (joystick)	SSM_038 Vehicle speed dependent flow limitation (auxiliary mini-steering wheel)	SSM_039 Safe auto-calibration stop	SSM_055 Safe EH steering shut-off (safe state)	SSM_056 Vehicle speed EH steering shut-off	SSM_057 Safe EH steering flow command	SSM_058 MMI steering program change lock-out	SSM_059 Steering device change lock-out	SSM_060 Vehicle speed dependent flow limitation (steering wheel)	SSM_061 Vehicle speed dependent flow scaling (open loop auxiliary joystick)	SSM_062 Vehicle speed dependent wheel angle limitation (Auxiliary closed loop joystick)	SSM_063 Safe Closed loop joystick engage	SSM_067 Hydraulic override	SSM_068 Hydraulic override disengage	SSM_069 Hydraulic override of auto-calibration	SSM_070 Hydraulic override of auto-guidance and auxiliary steering
Related to Auto-guidance mode																							
Loss of steering/unintended steering	○	○	○								●	●	●							○	○		○
Auto-guidance controller engages unintentionally	○	○	○	●	●	●	○	○			●	●			●					○	○		○
Auto-guidance controller disengages unintentionally	No risk reduction by PVED-CLS/software/valve. See ISO 10975.																						
Auto-guidance cannot be disengaged	○	○	○				○	○			●	●								○	○		○
Auto-guidance controller changes curvature command unintentionally	○	○	○	●	●	●	○	○			●	●								○	○		○
Auto-guidance controller unintentionally transmits oscillating curvature command	○	○	○	●	●	●	○	○			●	●								○	○		○
Operator is not awake	No risk reduction by PVED-CLS/Software/valve. See ISO 10975.																						
Operator is not in the cabin																							
Related to variable steering/fast-steering mode (steering wheel)																							
Loss of steering/unintended steering	○	○									●	●	●			●							
Variable steering cannot be changed to ON	No risk reduction by PVED-CLS/Software/valve.																						
Variable steering cannot be changed to OFF	○	○									●	●	●	●		●							
Variable steering changes to ON unintentionally (sudden change of steering behavior)	○	○									●	●	●	●		●							
Variable steering changes to OFF unintentionally (sudden change of steering behavior)	No risk reduction by PVED-CLS/Software/valve. See section 15.3																						
Variable steering changes between ON and OFF in an oscillating pattern unintentionally (sudden change of steering behavior)	○	○									●	●	●	●		●							

	Available safety functions																						
Risk scenarios	SSM_023 Safe on-road mode (OSPE system)	SSM_024 Safe on-road mode (EHPS system)	SSM_032 Auto-guidance and auxiliary steering disengage by steering wheel / SASA sensor	SSM_033 Auto-guidance disengage at low speed/parking	SSM_034 Vehicle speed dependent flow limitation (auto-guidance)	SSM_035 Vehicle speed dependent wheel angle limitation (auto-guidance)	SSM_036 Auto-guidance disengage by auxiliary steering device (mini-steering wheel)	SSM_037 Auto-guidance disengage by auxiliary steering device (joystick)	SSM_038 Vehicle speed dependent flow limitation (auxiliary mini-steering wheel)	SSM_039 Safe auto-calibration stop	SSM_055 Safe EH steering shut-off (safe state)	SSM_056 Vehicle speed EH steering shut-off	SSM_057 Safe EH steering flow command	SSM_058 MMI steering program change lock-out	SSM_059 Steering device change lock-out	SSM_060 Vehicle speed dependent flow limitation (steering wheel)	SSM_061 Vehicle speed dependent flow scaling (open loop auxiliary joystick)	SSM_062 Vehicle speed dependent wheel angle limitation (Auxiliary closed loop joystick)	SSM_063 Safe Closed loop joystick engage	SSM_067 Hydraulic override	SSM_068 Hydraulic override disengage	SSM_069 Hydraulic override of auto-calibration	SSM_070 Hydraulic override of auto-guidance and auxiliary steering
Operator forgets that Variable steering is ON when disengaging auto-steering with steering wheel											●	●	●			●							
Operator loses steering control when Variable steering is ON because the vehicle speed is too high											●	●	●	●		●							
Operator switches to a too aggressive steering program at too high vehicle speed	○	○									●		●	●									
Related to on-road usage																							
Loss of steering/unintended steering	○	○																					
Road switch cannot change to ON (on-road mode)											●	●	●			●							
Road switch changes to ON (on-road mode) unintentionally	No risk reduction by PVED-CLS/Software/valve. See section 15.3																						
Road switch changes to OFF (off-road mode) unintentionally or due to misuse											●	●	●	●		●							
Operator does not switch to on-road mode when driving on public road											●	●	●			●							
Related to auxiliary (mini-steering wheel) steering																							
Loss of steering/unintended steering	○	○	○						●		●	●	●							○	○		○
Mini-wheel steering cannot be deselected	○	○	○						●		●	●	●							○	○		○
Steering mode changes to mini-wheel steering unintentionally	○	○	○						●		●	●	●		●					○	○		○
Operator loses steering control when using mini-wheel steering because the vehicle speed is too high	○	○	○						●		●	●	●		●					○	○		○
Related to auxiliary open loop joystick steering																							
Loss of steering/unintended steering	○	○	○								●	●	●				●			○	○		○
Joystick steering mode cannot be deselected	○	○	○								●	●	●				●			○	○		○
Steering mode changes to joystick steering mode unintentionally	○	○	○								●	●	●		●		●			○	○		○

	Available safety functions																						
Risk scenarios	SSM_023 Safe on-road mode (OSPE system)	SSM_024 Safe on-road mode (EHPS system)	SSM_032 Auto-guidance and auxiliary steering disengage by steering wheel / SASA sensor	SSM_033 Auto-guidance disengage at low speed/parking	SSM_034 Vehicle speed dependent flow limitation (auto-guidance)	SSM_035 Vehicle speed dependent wheel angle limitation (auto-guidance)	SSM_036 Auto-guidance disengage by auxiliary steering device (mini-steering wheel)	SSM_037 Auto-guidance disengage by auxiliary steering device (joystick)	SSM_038 Vehicle speed dependent flow limitation (auxiliary mini-steering wheel)	SSM_039 Safe auto-calibration stop	SSM_055 Safe EH steering shut-off (safe state)	SSM_056 Vehicle speed EH steering shut-off	SSM_057 Safe EH steering flow command	SSM_058 MMI steering program change lock-out	SSM_059 Steering device change lock-out	SSM_060 Vehicle speed dependent flow limitation (steering wheel)	SSM_061 Vehicle speed dependent flow scaling (open loop auxiliary joystick)	SSM_062 Vehicle speed dependent wheel angle limitation (Auxiliary closed loop joystick)	SSM_063 Safe Closed loop joystick engage	SSM_067 Hydraulic override	SSM_068 Hydraulic override disengage	SSM_069 Hydraulic override of auto-calibration	SSM_070 Hydraulic override of auto-guidance and auxiliary steering
Operator loses steering control when using joystick steering because the vehicle speed is too high	○	○	○								●	●	●		●		●			○	○		○
Related to auxiliary closed loop joystick steering																							
Loss of steering/unintended steering	○	○	○								●	●	●					●		○	○		○
Joystick steering mode cannot be deselected	○	○	○								●	●	●							○	○		○
Steering mode changes to joystick steering mode unintentionally	○	○	○								●	●	●		●			●	●	○	○		○
Operator loses steering control when using joystick steering because the vehicle speed is too high	○	○	○								●	●	●					●		○	○		○
Related to auto-calibration (spool, WAS)																							
Loss of steering/unintended steering	○	○								○	●									○	○	○	
Unintended start of auto-calibration	○	○								○	●		●							○	○	○	

●	Possible safety function for risk reduction
○	System dependent safety function for risk reduction

Warning ⚠	**The system integrator shall ensure that all identified risk scenarios are adequately addressed. The above list of risk scenarios are typical cases.** **The list may not be complete.** **The available safety functions may be used for reducing risks for scenarios which are not listed.**

6 Operations Modes SSM_011

When the PVED-CLS is powered, it can operate in the following modes:

- Boot-loader mode
- Application mode
- Safe On-road mode
- Service mode
- Safe state

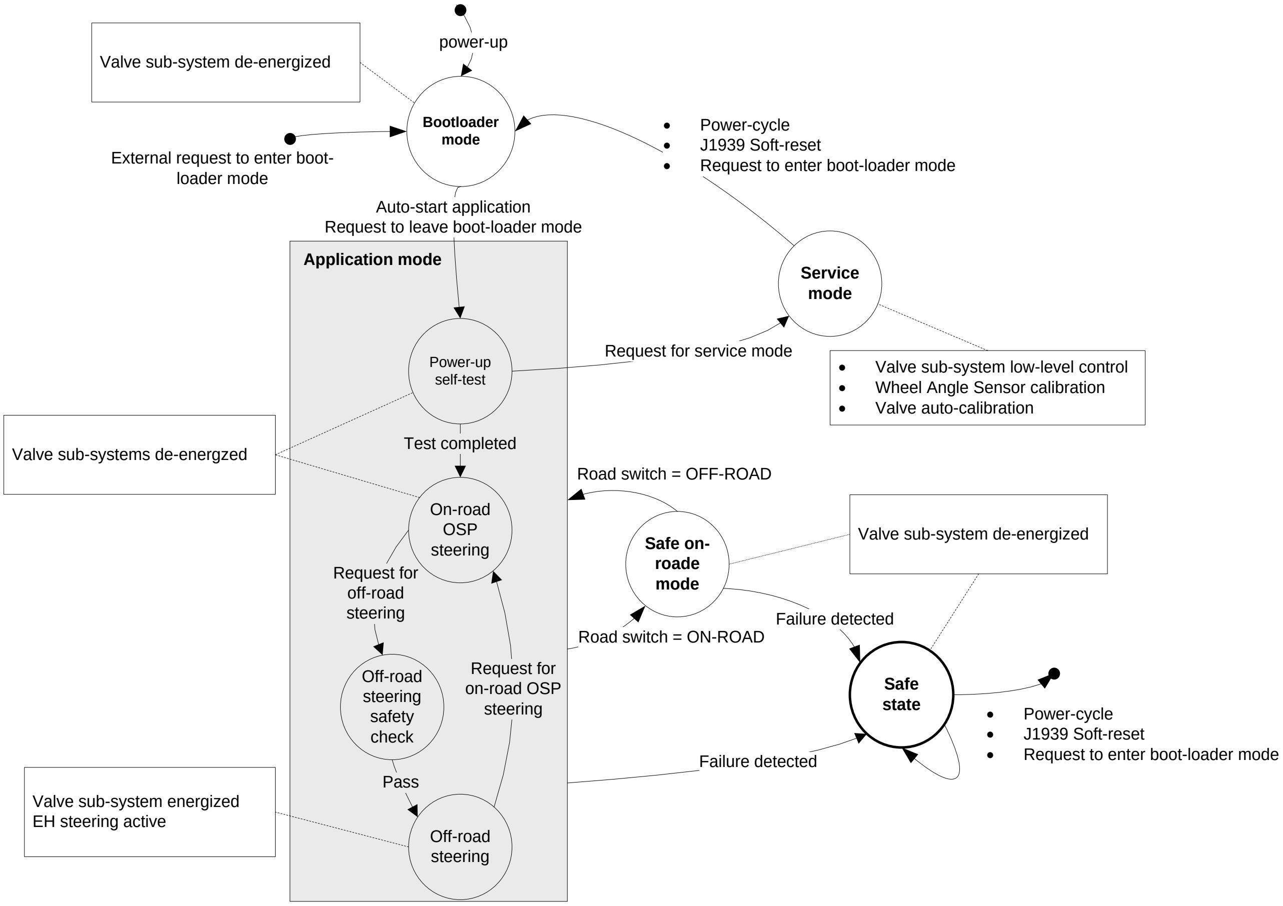

Valve sub-system de-energized
power-up
Bootloader mode
External request to enter boot-loader mode
Power-cycle
J1939 Soft-reset
Request to enter boot-loader mode
Auto-start application
Request to leave boot-loader mode
Application mode
Service mode
Power-up self-test
Request for service mode
Valve sub-system low-level control
Wheel Angle Sensor calibration
Valve auto-calibration
Valve sub-systems de-energzed
Test completed
Road switch = OFF-ROAD
On-road OSP steering
Safe on-roade mode
Valve sub-system de-energized
Request for off-road steering
Road switch = ON-ROAD
Failure detected
Off-road steering safety check
Request for on-road OSP steering
Safe state
Power-cycle
J1939 Soft-reset
Request to enter boot-loader mode
Failure detected
Pass
Valve sub-system energized
EH steering active
Off-road steering

Figure 8: PVED-CLS operation mode state machine.

6.1 BOOT-LOADER MODE

When the PVED-CLS is powered, boot-loader mode is entered. If the boot-loader detects that an application firmware is installed and there is no request to stay in boot-loader mode, it will auto-start the application 50ms later. It is possible to request a transition to boot-loader mode from any mode at any time. See PVED-CLS KWP2000 protocol documentation.

6.2 APPLICATION MODE

After entering application mode, a Power-on-Self-Test (POST) is executed. If the POST is passed, the address claim message is sent on the CAN bus. A 200ms time-window is opened for entering service mode. See PVED-CLS communication protocol for information on how to enter service mode.

If a road switch sub-system is not present in the system, the software enters On-road OSP steering state.
If a road switch is present in the system and it is in 'off-road position', then the software jumps to the on-road OSP steering state. If the road switch is in 'on-road position, the software enters safe on-road mode.

6.1 CONFIGURATION SSM_013

Parameter configuration can only be performed when the PVED-CLS is in boot-loader mode.

In this mode, all peripherals are de-energized. No EH-steering algorithms or safety related software is executed.

7 System diagrams

7.1 PVED-CLS CONNECTOR SSM_015

The PVED-CLS will only be available with connector variant: 12 pin Deutsch DT04-12PA-B016 connector.

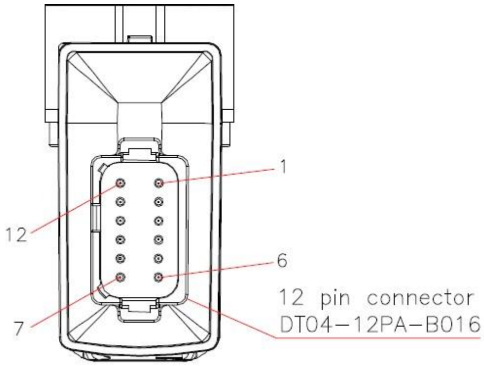


Figure 9: PVED-CLS Pinout layout.

PVED-CLS Pinout			
Deutsch Connector			
1	AD2	7	Power ground (-)
2	AD3	8	Power supply (+)
3	Sensor power ground (-)	9	CAN Low MAIN
4	CAN High SAFETY	10	CAN High MAIN
5	CAN Low SAFETY	11	5V sensor supply (+)
6	Digital output	12	AD1

Table 3: PVED-CLS Pinout description.

For information regarding technical specification, please see PVED-CLS Technical Specification.

7.2 WIRING SCHEMATICS

The following wiring schematics are general. Variants are possible as long as the installation guidelines are respected.

7.2.1 De-energized on-road mode – OSPE, EHi-E and EHi-H valve sub-system SSM_031

Both CAN-based and analogue wheel angle sensor sub-systems are illustrated in the schematic below, in order to obtain a certain level of completeness. However, the system can be designed either with a CAN-based, an analogue or no wheel angle sensor.

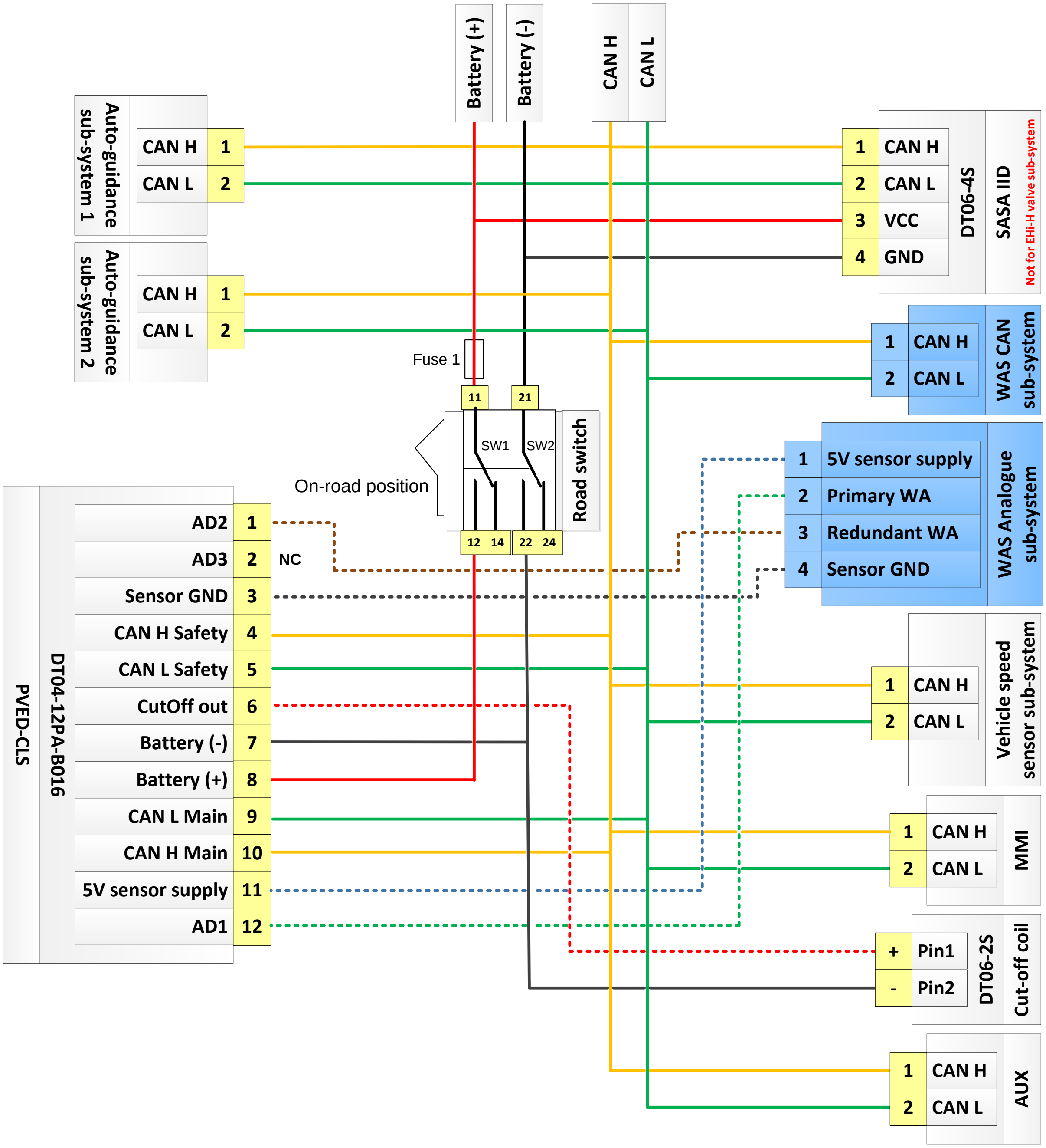


Figure 10: Schematic for de-energized on-road mode for OSPE, EHi-E and EHi-H valve sub-system.

- The interfacing sub-systems may be powered by other power sources.
- The output of the sub-systems must be present and stable no later than 10 seconds after PVED-CLS power-up.

7.2.2 Safe On-road mode – OSPE, EHi-E and EHi-H valve sub-system SSM_023

Both CAN-based and analogue wheel angle sensor sub-systems are illustrated in the schematic below, in order to obtain a certain level of completeness. However, the system can be designed either with a CAN-based, an analogue or no wheel angle sensor.

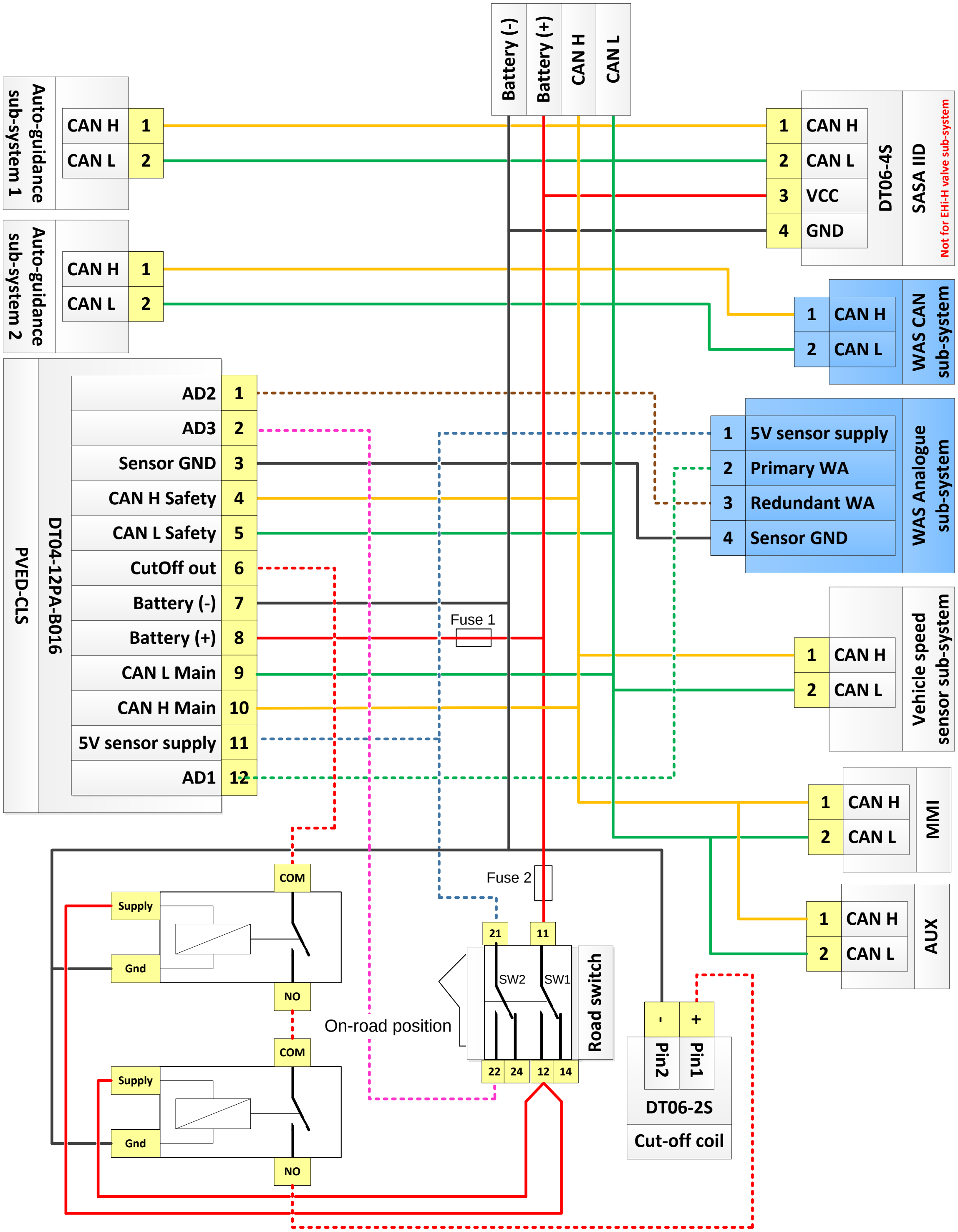


Figure 11: Schematic for safe on-road mode for OSPE, EHi-E and EHi-H valve sub-system.

- The interfacing sub-systems may be powered by other power sources.
- The output of the sub-systems must be present and stable no later than 10 seconds after PVED-CLS power-up.

7.2.3 safe on-road mode – EHPS valve sub-system SSM_024

Both CAN-based and analogue wheel angle sensor sub-systems are illustrated in the schematic below, in order to obtain a certain level of completeness. However, the system can be designed either with a CAN-based or an analogue wheel angle sensor. It is also possible to apply the de-energize on-road mode for the EHPS valve sub-system, by using a road switch in the same manner as system diagram shown in Figure 10.

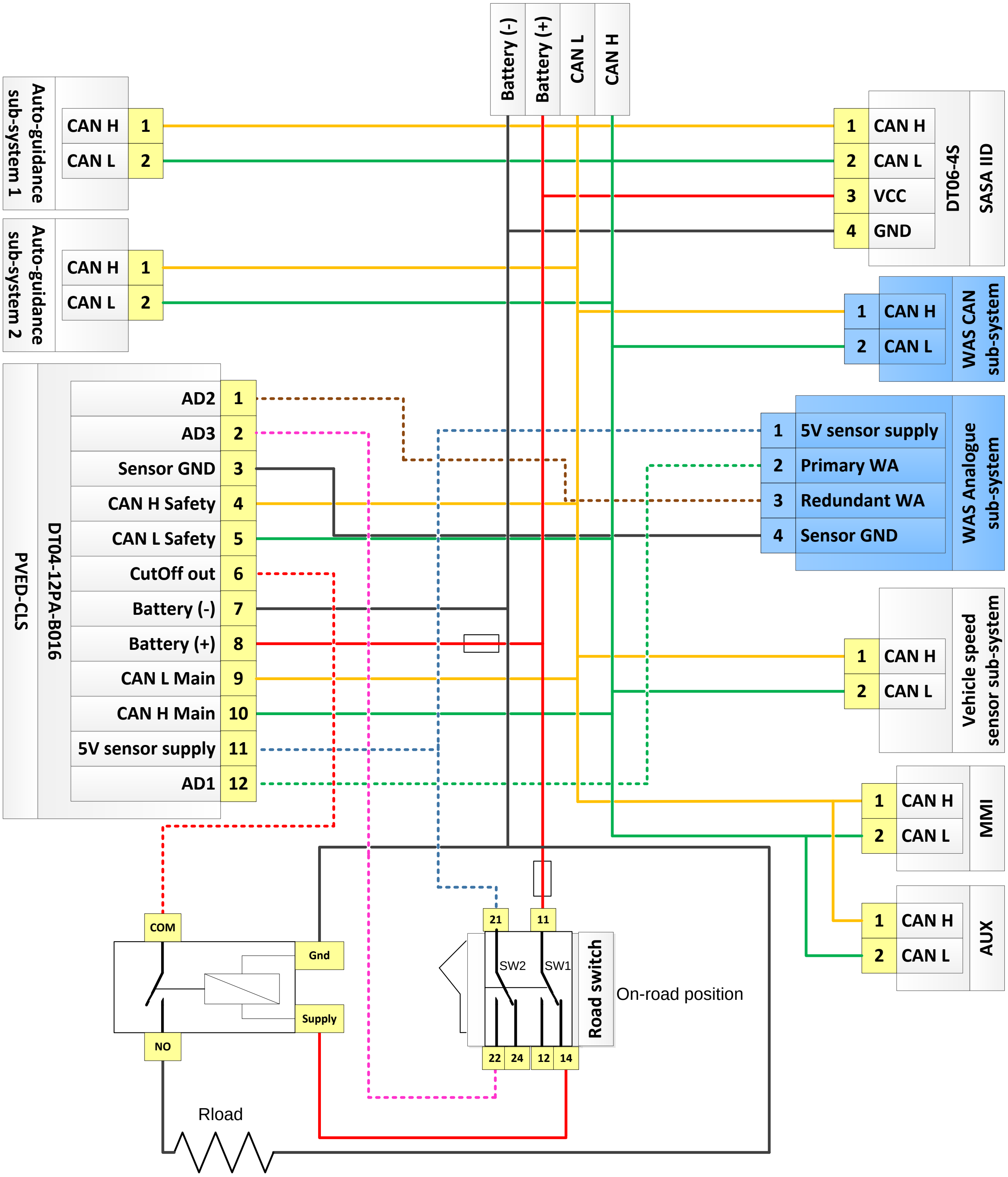


Figure 12: Schematic for safe on-road mode for EHPS valve sub-system.

- The interfacing sub-systems may be powered by other power sources.
- The output of the sub-systems must be present and stable no later than 10 seconds after PVED-CLS power-up.

8 Sensor sub-systems and Monitoring

The PVED-CLS requires one or more sensor sub-systems to be present. This section describes the requirements to each sensor sub-system.

Warning	
⚠	**It is strongly recommended that the system integrator performs a System level Failure Mode Effects Analysis (FMEA) on the sub-systems and the system in its entireness.**

8.1 STEERING WHEEL SENSOR SUB-SYSTEM SSM_016

The steering wheel position and rotational speed must be input to the PVED-CLS, when used together with an OSPE, EHPS or EHi-E valve sub-system. The architecture seen below shows how the PVED-CLS can be used as part of a steering wheel sensor sub-system. The sub-system design supports realizing safety function designed to meet SIL2/PL d/AgPL d by designing the sub-system to a category 3 architecture.

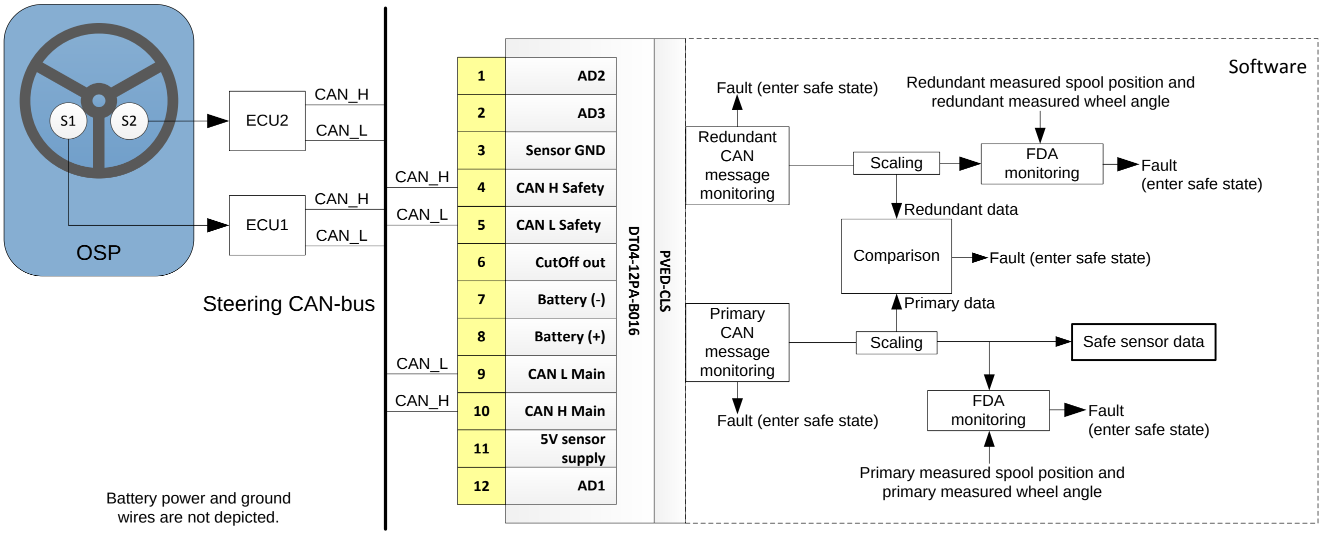


Figure 13: Steering wheel sensor architecture.

Primary steering wheel sensor (S1, ECU1) and redundant steering wheel sensor (S2, ECU2) shall be two channels which both acquire the steering wheel angle position and calculates the steering angle speed and direction. ECU1 acquires the steering wheel angle via sensor element S1 and scales it to representing steering wheel angle and calculates a steering angle speed. Both the angle and speed is transmitted onto the CAN bus via a safe protocol as the STW primary message. The same applies for the redundant steering wheel message, where ECU2 transmits the STW redundant message. The main and safety controller receive, monitor and scale the input to the internal resolution range. See PVED-CLS communication protocol for details on the steering wheel message protocol.

Attention

⚠

The system integrator shall:

- Design and supply the steering wheel sensor sub-system.
- Ensure that the sub-system components are fit for the purpose.
- Conduct an FMEA to uncover dangerous failures.
- Implement measures against dangerous failures.
- Perform a CCF analysis.
- Document the sub-system as part of the safety case.

8.1.1 CAN interface

The PVED-CLS main controller receives the STW primary message and the PVED-CLS safety controller receives the STW redundant message. The default values are valid for the compatible Danfoss steering wheel (SASA) sensor (see section 8.1.3).

Parameter	Description	Default value	
		Main controller	Safety controller
P3296	Steering wheel sensor source address	77	77
P3319	Steering wheel sensor PGN offset	16	17

Important

- The applied safety protocol allows omitting the CAN bus from the safety loop calculation as it contributes less than 1 % of the safety integrity level.
- The applied safety protocol allows the presence of both safety and non-safety related CAN messages.
- P3296 may be equal for both STW primary and redundant message if they are transmitted by one CAN node.
- The sub-system shall begin transmitting CAN messages no later than 10 seconds after the PVED-CLS is powered.

8.1.2 Monitoring

The PVED-CLS provides monitoring functions for the sensor sub-system.
For both STW primary and redundant message, the following monitoring is in place in both the PVED-CLS main and safety controller:

- Receive timing check of CAN messages. Single failure leads to safe state.
- Sequence number check on CAN message. Single failure leads to safe state.
- End-to-end CRC on messages. Single failure leads to safe state.
- Data validity check (range check). Valid range for angle is 0° to 359,912°. Valid range for angular velocity is -300 RMP to 300 RPM. Single failure leads to safe state.
- Primary and redundant data are cross-checked as follows: If the absolute primary and redundant difference is > P3355 degrees for more than P3354 x10ms, then enter safe state.
- Primary and redundant data are cross-checked as follows: If the absolute primary and redundant difference is > P3358 RPM for more than P3357 x10ms, then enter safe state.
- See PVED-CLS User Manual for CAN bus diagnostic trouble codes related to detecting different failures on the sensor sub-system.
- Fault Detection Algorithm (FDA), see section 9.5.

Parameter	Description	Default value
P3355	Channel cross-check monitoring. Maximum steering wheel angle [Degrees]	15
P3358	Channel cross-check monitoring. Maximum steering wheel angle velocity [dRPM]	50
P3354	Channel cross-check monitoring. Maximum steering wheel angle divergence time [x10ms]	10
P3357	Channel cross-check monitoring. Maximum steering wheel angle velocity divergence time [x10ms]	10
P3287	Maximum message timeout [x10ms]	8

Default values are recommended values when a SASA sensor is utilized.

Important

- Setting the value for P3355, P3358, P3354, P3357, P3287 too high will reduce the monitoring performance.
- Set value of P3287 to 1.5 · nominal transmission rate.
- Design the sensor sub-system channels to output as equal data as possible.
- Record sensor data in different scenarios and use simulation for optimum monitoring performance tuning.
- The monitoring technique is based on a comparison and reference sensors. A diagnostic coverage in the range 90-99 % may be claimed provided that the sub-system is integrated according to the specification.

Fault Detection Algorithm – FDA

The cross-checked steering wheel sensor data is monitored by the Fault Detection Algorithm (FDA) which checks the correlation plausibility between the a) wheel angle changes, b) the EH-valve main spool position and c) steering wheel movement. If an inconsistency is detected, the safe state is entered.

FDA can detect the following common cause faults related to the steering wheel sensor:

- Loss of mechanical connection between the steering wheel sensor and the steering wheel column
- Steering wheel sensor dual-channel electrical "stuck-at" faults

For further information, see section 9.5.

8.1.3 SASA sensor

Danfoss supplies an integrated steering wheel sensor (SASA sensor) which is designed for the PVED-CLS and seamless installation of the OSP. Refer to OSPE Steering valve, SASA sensor, Technical information, 11068682 for information on the SASA sensor.

Safety parameter	Specification	Description
MTTFd	73 years	Per SASA sensor channel. Calculated at 80 ˚C.
DC	99 %	Internal SASA sensor monitoring. PVED-CLS monitoring for steering wheel sensor input.
CCF analysis	>65 %	Performed for SASA sensor design.
Category	3	Ensured by SASA sensor design.

8.2 OPEN LOOP AUXILIARY STEERING DEVICE SENSOR SUB-SYSTEM SSM_017

It is possible to connect an open loop auxiliary steering device to the PVED-CLS. An open loop auxiliary steering device is basically a steering device which outputs a flow command. It is possible to select the open loop auxiliary steering device to be a mini-steering wheel, a CAN based joystick or an analogue joystick. However, only one type of auxiliary steering device can be present in the system, see section 7.3.

8.2.1 Mini-steering wheel sub-system

The auxiliary mini-steering wheel position and rotational speed is input to the PVED-CLS. The architecture seen below shows how the PVED-CLS can be used as part of an auxiliary mini-steering wheel sensor sub-system. The sub-system design supports realizing safety function designed to meet SIL2/PL d/AgPL d by designing the sub-system to a category 3 architecture.

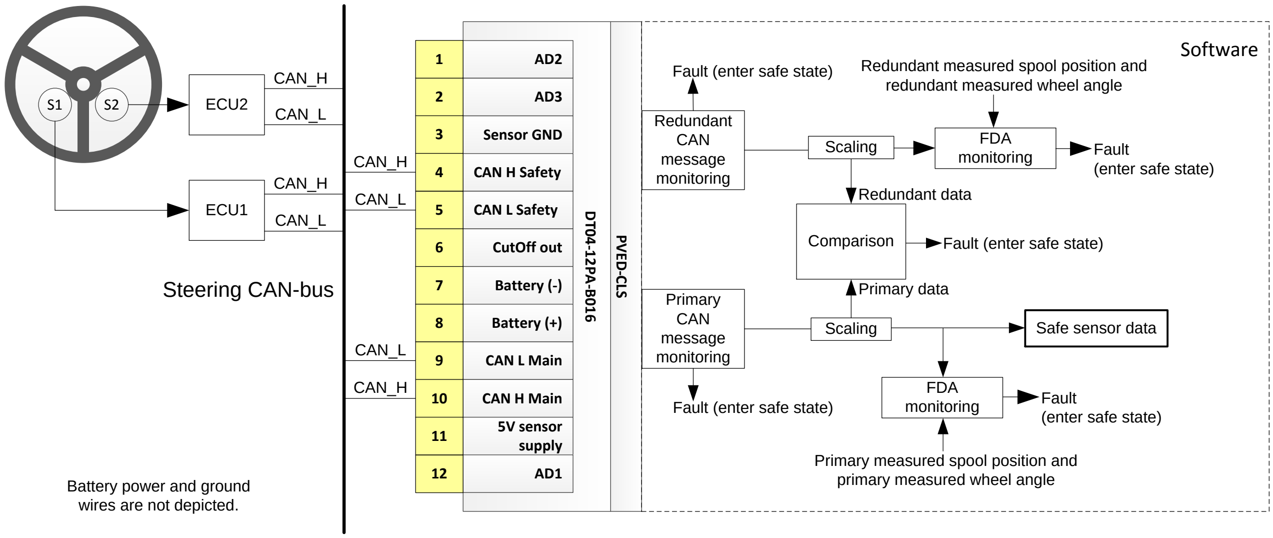


Figure 14: Mini-steering wheel architecture

Primary mini-steering wheel sensor (S1, ECU1) and redundant mini-steering wheel sensor (S2, ECU2) shall be two channels which both acquire the mini-steering wheel angular position and calculates the mini-steering wheel angular speed and direction. ECU1 acquires the mini-steering wheel angle via sensor element S1 and scales it to representing steering wheel angle and calculates a steering angular velocity. Both the angle and speed are transmitted onto the CAN bus via a safe protocol as the AUX sensor mini-steering wheel message. The same applies for the redundant mini-steering wheel message, where ECU2 transmits the AUX sensor mini-steering wheel message. The main and safety controller receive, monitor and scale the input to the internal resolution range. See PVED-CLS communication protocol for details on the steering wheel message protocol.

8.2.1.1 Interface – Auxiliary mini-steering wheel

The PVED-CLS main controller receives the primary message and the PVED-CLS safety controller receives the redundant message.

Parameter	Description	Main controller	Safety controller
P3299	Auxiliary mini-steering wheel source address	79 (Default)	79 (Default)
P3321	Auxiliary mini-steering wheel PGN offset	20 (Default)	21 (Default)
P3239	Auxiliary steering device present in the system (0 = Not present, 255 = Present)	255	255
P3240	Auxiliary steering device type (0 = Open loop joystick, 1 = Closed loop joystick, 2 = Mini-steering wheel, 3 = Analogue open loop joystick, 20 = Elobau® joystick)	2 (Default)	2 (Default)

8.2.1.2 MMI steering device lock-out - Auxiliary mini-steering wheel

The MMI CAN command signal 'AUX steering device lockout' shall indicate if the PVED-CLS is allowed to follow commands from the auxiliary mini-steering wheel or not. When the auxiliary mini-steering wheel is locked out, the PVED-CLS awaits a steering command from any other present steering device. The PVED-CLS will suspend auxiliary mini-steering wheel as soon as the MMI command prohibit auxiliary steering. If an auxiliary steering device is configured to be present, the data from the AUX device will always be validated. Monitoring will only be suspended if the AUX steering device is configured as "not present" in the system. See PVED-CLS Communication protocol.

Important

- The applied safety protocol allows omitting the CAN bus from the safety loop calculation as it contributes less than 1 % of the SIL2.
- The applied safety protocol allows the presence of both safety and non-safety related CAN messages.
- P3299 may be equal for both auxiliary steering device primary and redundant message if they are transmitted by one CAN node.
- The sub-system shall begin transmitting CAN messages no later than 10 seconds after the PVED-CLS is powered.
- At power on, it is recommended that the MMI CAN command signal 'AUX steering device lockout' is set to 'AUX steering prohibited'.

8.2.1.3 Monitoring - Auxiliary mini-steering wheel

The PVED-CLS provides monitoring functions for the auxiliary mini-steering wheel sub-system.
For both auxiliary steering device primary and redundant message, the following monitoring is in place in both the PVED-CLS main and safety controller:

- Receive timing check of CAN messages. Single failure leads to safe state.
- Sequence number check on CAN message. Single failure leads to safe state.
- End-to-end CRC on messages. Single failure leads to safe state.
- Data validity check (range check). Valid range for angle is 0° to 359,912°. Valid range for angular velocity is -300 RMP to 300 RPM. Single failure leads to safe state.
- Primary and redundant data are cross-checked as follows: If the absolute primary and redundant steering speed difference is > P3366 RPM for more than P3365 x10ms, then enter safe state.
- Primary and redundant data are cross-checked as follows: If the absolute primary and redundant steering angle difference is > P3372 degrees for more than P3371 x10ms, then enter safe state.
- See PVED-CLS User Manual for CAN bus diagnostic trouble codes related to detecting different failures on the sensor sub-system.

- Fault Detection Algorithm (FDA), see section 9.5.

Parameter	Description	Default value
P3365	Channel cross-check monitoring. Maximum auxiliary mini-steering wheel angle velocity divergence time [x10ms]	10
P3366	Channel cross-check monitoring. Maximum auxiliary mini-steering wheel angle velocity difference [dRPM]	50
P3371	Channel cross-check monitoring. Maximum auxiliary mini-steering wheel angle divergence time [x10ms]	10
P3372	Channel cross-check monitoring. Maximum auxiliary mini-steering wheel angle difference [Degrees]	15
P3291	Maximum auxiliary device message timeout [x10ms]	8

Important

- Setting the value for P3365, P3366, P3354, P3371, P3272, P3291 too high will reduce the monitoring performance.
- Set value of P3291 to 1.5 · nominal transmission rate.
- Design the auxiliary steering device sub-system channels to output as equal data as possible.
- Record sensor data in different scenarios and use simulation for optimum monitoring performance tuning.
- The monitoring technique is based on a comparison and reference sensors. A diagnostic coverage in the range 90-99 % may be claimed provided that the sub-system is integrated according to the specification.

Fault Detection Algorithm – FDA

The cross-checked auxiliary steering device data is scaled to EH-valve main spool set-point and is monitored by the Fault Detection Algorithm (FDA). The Fault Detection Algorithm (FDA) checks the correlation plausibility between the a) wheel angle changes, b) the EH-valve main spool position and c) steering wheel movement. If an inconsistency is detected, the safe state is entered. For further information, see section 9.5.

8.2.2 CAN based open-loop joystick sub-system

Alternatively, the open loop auxiliary steering device can be a CAN based joystick. In this case the joystick position must be input to the PVED-CLS. The architecture seen on the next page shows how the PVED-CLS can be used as part of a CAN based open-loop auxiliary joystick sensor sub-system. The sub-system design supports realizing safety function designed to meet SIL2/PL d/AgPL d by designing the sub-system to a category 3 architecture.

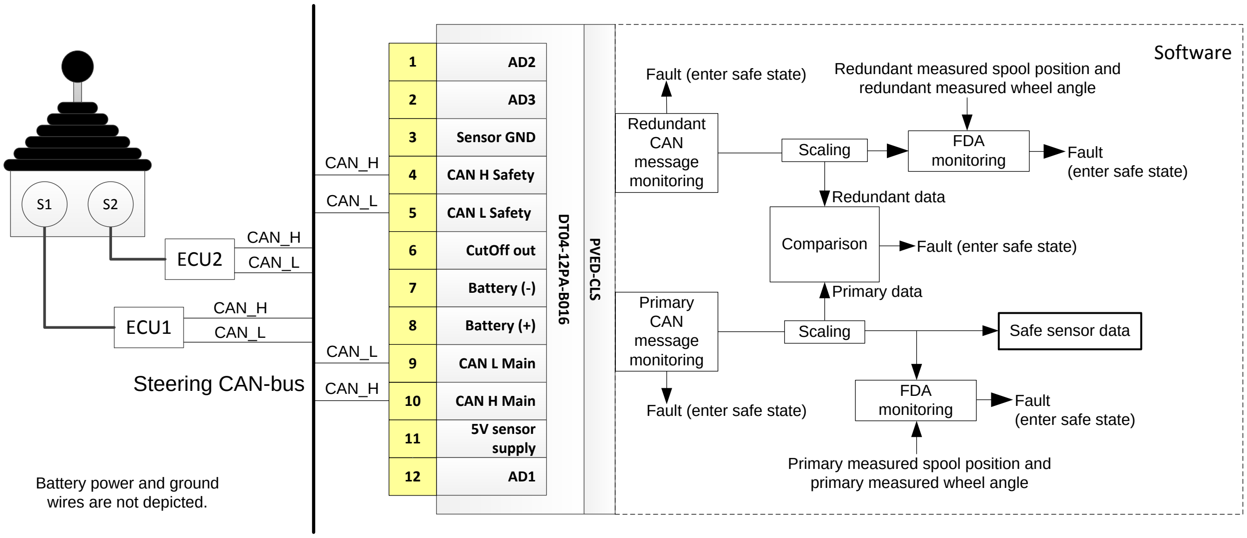


Figure 15: CAN based open-loop joystick architecture.

Primary joystick position sensor (S1, ECU1) and redundant joystick position sensor (S2, ECU2) shall be two channels which both acquire the joystick position. Both the primary and redundant joystick position is transmitted onto the CAN bus via a safe protocol as the AUX sensor joystick messages. In this case the messages contain a flow command relative to the maximum steering flow. The main and safety controller receive, monitor and scale the input to the internal resolution range.
The PVED-CLS software is compatible with the Elobau® J4F with 351JCM joystick which can be used as the CAN based open-loop joystick in a sensor sub-system.
See PVED-CLS communication protocol for details on the steering wheel message protocol.

8.2.2.1 Interface - CAN based open loop joystick

The PVED-CLS main controller receives the primary message and the PVED-CLS safety controller receives the redundant message.

Parameter	Description	Main controller	Safety controller
P3300	Auxiliary joystick source address	78 (Default)	78 (Default)
P3322	Auxiliary joystick PGN offset	22 (Default)	23 (Default)
P3239	Auxiliary steering device present in the system (0 = Not present, 255 = Present)	255	255
P3240	Auxiliary steering device type (0 = Open loop joystick, 1 = Closed loop joystick, 2 = Mini-steering wheel, 3 = Analogue open loop joystick, 20 = Elobau® joystick)	0	0

8.2.2.2 MMI steering device lock-out - CAN based open loop joystick

The MMI CAN command signal 'AUX steering device lockout' shall indicate if the PVED-CLS is allowed to follow commands from the CAN based open loop joystick or not. When the CAN based open loop joystick is locked out, the PVED-CLS awaits a steering command from any other present steering device. The PVED-CLS will suspend CAN based open loop joystick steering as soon as the MMI command prohibit auxiliary steering. If an auxiliary steering device is configured to be present, the data from the AUX device will always be validated. Monitoring will only be suspended if the AUX steering device is configured as "not present" in the system. See PVED-CLS Communication protocol.

Important

- The applied safety protocol allows omitting the CAN bus from the safety loop calculation as it contributes less than 1% of the SIL2.
- The applied safety protocol allows the presence of both safety and non-safety related CAN messages.
- P3299 and P3300 may be equal for both auxiliary steering device primary and redundant message if they are transmitted by one CAN node.
- The sub-system shall begin transmitting CAN messages no later than 10 seconds after the PVED-CLS is powered.
- At power on, it is recommended that the MMI CAN command signal 'AUX steering device lockout' is set to 'AUX steering prohibited'.

8.2.2.3 Monitoring - CAN based open loop joystick

The PVED-CLS provides monitoring functions for the CAN based open loop auxiliary joystick sub-system.
For both auxiliary steering device primary and redundant message, the following monitoring is in place in both the PVED-CLS main and safety controller:

- Receive timing check of CAN messages. Single failure leads to safe state.
- Sequence number check on CAN message. Single failure leads to safe state.
- End-to-end CRC on messages. Single failure leads to safe state.
- Data validity check (range check). Single failure leads to safe state.
- Primary and redundant data are cross-checked as follows: If the absolute primary and redundant steering flow command difference is > P3369 [IR] for more than P3368 ms, then enter safe state.
- See PVED-CLS User Manual for CAN bus diagnostic trouble codes related to detecting different failures on the sensor sub-system.
- Fault Detection Algorithm (FDA), see section 9.5.

Parameter	Description	Default value
P3368	Channel cross-check monitoring. Maximum auxiliary joystick position divergence time [x10ms]	10
P3369	Channel cross-check monitoring. Maximum auxiliary joystick position difference [IR]	5
P3291	Maximum auxiliary device message timeout [x10ms]	8

Important

- Setting the value for P3368, P3369, P3291 too high will reduce the monitoring performance.
- Set value of P3291 to 1.5 · nominal transmission rate.
- Design the auxiliary steering device sub-system channels to output as equal data as possible.
- Record sensor data in different scenarios and use simulation for optimum monitoring performance tuning.
- The monitoring technique is based on a comparison and reference sensors. A diagnostic coverage in the range 90-99% may be claimed provided that the sub-system is integrated according to the specification.

Fault Detection Algorithm – FDA

The cross-checked auxiliary steering device data is scaled to EH-valve main spool set-point and is monitored by the Fault Detection Algorithm (FDA). The Fault Detection Algorithm (FDA) checks the correlation plausibility between the a) wheel angle changes, b) the EH-valve main spool position and c) steering wheel movement. If an inconsistency is detected, the safe state is entered. For further information, see section 9.5.

8.2.2.4 Interface - Elobau® open loop joystick

The PVED-CLS supports interfacing to an Elobau® J4F joystick (with 351JCM), right or left hand joystick. The steering related information can be transmitted in the basic joystick message (BJM) and the inverted basic joystick message (invBJM), were the basic joystick message is the primary message and the inverted basic joystick message is the redundant message. Alternatively the steering related information can be transmitted in the extended joystick message (EJM) and the inverted extended joystick message (invEJM), where the extended joystick message is the primary message and the inverted extended joystick message is the redundant message. The PVED-CLS main controller receives the primary messages and the PVED-CLS safety controller receives the redundant messages. The inverted messages, invBJM and invEJM, are bitwise inverted by the PVED-CLS safety controller.

Parameter	Description	Main controller	Safety controller
P3300	Auxiliary joystick source address: Right hand Elobau® joystick source address	235	237
	Auxiliary joystick source address: Left hand Elobau® joystick source address	236	238
P3329	Elobau® PGN: Right hand joystick BJM and invBJM	64982 (Default)	64982 (Default)
	Elobau® PGN: Left hand joystick BJM and invBJM	64984	64984
	Elobau® PGN: Right hand joystick EJM and invEJM	64983	64983
	Elobau® PGN: Left hand joystick EJM and invEJM	64985	64985
P3239	Auxiliary steering device present in the system (0 = Not present, 255 = Present)	255	255
P3240	Auxiliary steering device type (0 = Open loop joystick, 1 = Closed loop joystick, 2 = Mini-steering wheel, 3 = Analogue open loop joystick, 20 = Elobau® joystick)	20	20

8.2.2.5 MMI steering device lock-out - Elobau® open loop joystick

The MMI CAN command signal 'AUX steering device lockout' shall indicate if the PVED-CLS is allowed to follow commands from the Elobau® open loop joystick or not. When the Elobau® open loop joystick is locked out, the PVED-CLS awaits a steering command from any other present steering device. The PVED-CLS will suspend Elobau® open loop joystick steering as soon as the MMI command prohibit auxiliary steering. If an auxiliary steering device is configured to be present, the data from the AUX device will always be validated. Monitoring will only be suspended if the AUX steering device is configured as "not present" in the system. See PVED-CLS Communication protocol.

Important

- The applied safety protocol allows omitting the CAN bus from the safety loop calculation as it contributes less than 1% of the SIL2.
- The applied safety protocol allows the presence of both safety and non-safety related CAN messages.
- The sub-system shall begin transmitting CAN messages no later than 10 seconds after the PVED-CLS is powered.
- At power on, it is recommended that the MMI CAN command signal 'AUX steering device lockout' is set to 'AUX steering prohibited'.

8.2.2.6 Monitoring - Elobau® open loop joystick

The PVED-CLS provides monitoring functions for the Elobau® open loop auxiliary joystick sub-system.
For basic joystick message (BJM) and inverted joystick message (invBJM) or extended joystick message (EJM) and inverted extended joystick message (invEJM), the following monitoring is in place in both the PVED-CLS main and safety controller:

- Receive timing check of CAN messages. Single failure leads to safe state.
- Data validity check (range check). Single failure leads to safe state.
- Primary (BJM) and redundant (invBJM) data are cross-checked as follows: If the absolute primary and redundant steering flow command difference is > P3369 [IR] for more than P3368 ms, then enter safe state.
- See PVED-CLS User Manual for CAN bus diagnostic trouble codes related to detecting different failures on the sensor sub-system.
- Fault Detection Algorithm (FDA), see section 9.5.

The table below describes how the parameters related to the CAN monitoring shall be configured in order to be compliant with the guidelines given by Elobau® in the document Operating/Safety Manual for J4F with351JCM version 01.04.

Parameter	Description	Value for BJM and invBJM	Value for EJM and invEJM
P3368	Channel cross-check monitoring. Maximum auxiliary joystick position divergence time [x10ms]	15	15
P3369	Channel cross-check monitoring. Maximum auxiliary joystick position difference [IR]	75	120
P3291	Maximum auxiliary device message timeout [x10ms]	6	6

Attention ⚠	**The integrator shall have read the document Operating/Safety Manual for J4F with351JCM version 01.04, before configuration an Elobau joystick as input device for the PVED-CLS.**

Important

The monitoring technique is based on a comparison and reference sensors. A diagnostic coverage in the range 90-99 % may be claimed provided that the sub-system is integrated according to the specification.

Fault Detection Algorithm – FDA

The cross-checked auxiliary steering device data is scaled to EH-valve main spool set-point and is monitored by the Fault Detection Algorithm (FDA). The Fault Detection Algorithm (FDA) checks the correlation plausibility between the a) wheel angle changes, b) the EH-valve main spool position and c) steering wheel movement. If an inconsistency is detected, the safe state is entered. For further information, see section 9.5.

8.2.3 Analogue open-loop joystick sub-system

Finally, the open loop auxiliary steering device can be an analogue joystick. The input to the PVED-CLS is the joystick position, expressed as an analogue signal. The architecture seen below shows how the PVED-CLS can be used as part of an analogue open loop auxiliary joystick sensor sub-system. The sub-system design supports realizing a safety function designed to meet SIL2/PL d/AgPL d by designing the sub-system to a category 3 architecture.

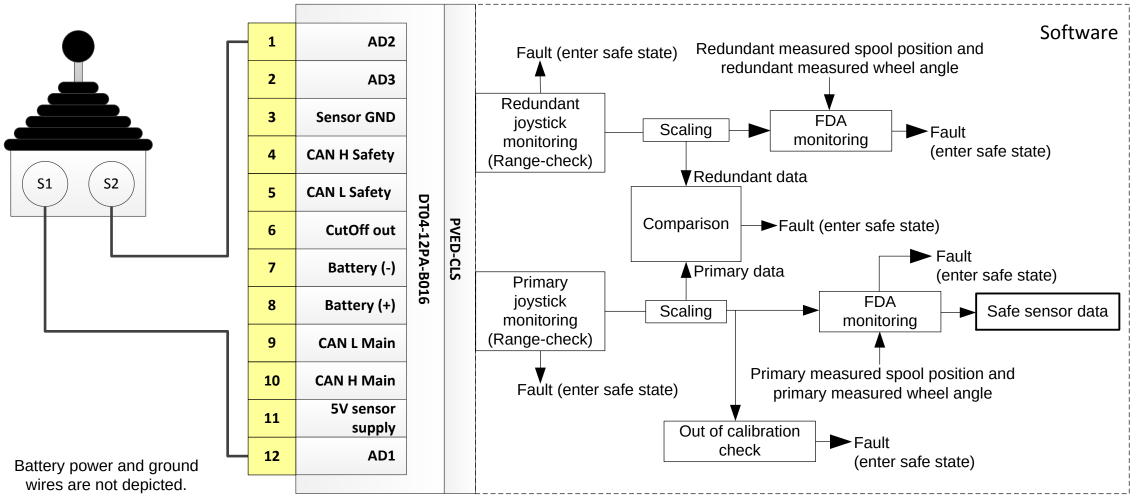


Figure 16: Analogue joystick architecture.

Primary joystick position sensor (S1) and redundant joystick position sensor (S2) shall be two channels which both acquire the joystick position. The main and safety controller receive, monitor and scale the input to the internal resolution range. The analogue joystick can be powered by any stabilized supply or from the PVED-CLS 5V sensor supply. The PVED-CLS 5V sensor supply is internally monitored and adjusts for output drift and short-circuits faults. See PVED-CLS User Manual for further information on the 5V sensor supply.

Refer to the PVED-CLS user manual for AD1 and AD2 calibration for the analogue joystick.

Attention

The system integrator shall:

- Design and supply the open loop auxiliary steering device sub-system.
- Ensure that the sub-system components are fit for the purpose.
- Conduct an FMEA to uncover dangerous failures.
- Implement measures against dangerous failures.
- Perform a CCF analysis.
- Document the sub-system as part of the safety case.

8.2.3.1 Interface – Analogue open loop joystick

The analogue joystick signals on AD1 and AD2 shall be in the range 500 mV to 4500 mV. The parameters related to dual channel analogue joystick are:

Parameter	Description	Main controller	Safety controller
P3239	Auxiliary steering device is present in the system (0 = Not present, 255 = Present)	255	255
P3240	Auxiliary steering device type (0 = Open loop joystick, 1 = Closed loop joystick, 2 = Mini-steering wheel,	3	3

	3 = Analogue open loop joystick, 20 = Elobau® joystick)		

8.2.3.2 MMI steering device lock-out - Analogue open loop joystick

The MMI CAN command shall indicate if the PVED-CLS is allowed to follow commands from the analogue open loop auxiliary steering device or not. When the auxiliary steering device is locked out, the PVED-CLS awaits a steering command from any other present steering device. The PVED-CLS will suspend analogue open loop auxiliary steering as soon as the MMI command prohibit analogue open loop auxiliary steering. If an auxiliary steering device is configured to be present, the data from the AUX device will always be validated. Monitoring will only be suspended if the AUX steering device is configured as "not present" in the system. See PVED-CLS Communication protocol.

Important

- The sub-system shall begin transmitting the analogue signals no later than 10 seconds after the PVED-CLS is powered.
- The joystick position angle-to-signal characteristic shall be mutually inverted for the PVED-CLS to monitor a common 5V sensor supply.
- If the joystick position outputs are not mutually inverted and a single joystick position output is unintendedly connected to both AD1 and AD2, the PVED-CLS cannot detect the failure. In this situation the sub-system does not meet the requirements for a category 3 architecture.
- The voltage representing neutral shall be in the middle of the achieved voltage range.
- At power on, it is recommended that the MMI CAN command signal 'AUX steering device lockout' is set to 'AUX steering prohibited'.

Refer to the PVED-CLS user manual for AD1 and AD2 calibrating for the analogue joystick.

8.2.3.3 Monitoring - Analogue open loop joystick

The PVED-CLS provides monitoring function for the analogue joystick sub-system.

- Input range check
- Joystick channel cross-check
- Micro-controller cross-check of scaled joystick position
- Fault Detection Algorithm
- Out of calibration check

Input range check
AD1 and AD2 input values below 100 mV and above 4900 mV are detected as short-circuit to ground and supply respectively.

Analogue joystick channel cross-check
The PVED-CLS will perform cross-check monitoring on the joystick position signal from the primary and redundant joystick sensor. This check is performed in both micro-controllers.

Parameter	Description	Default value	
		Main controller	Safety controller
P3375	Analogue sensor cross-check monitoring. Maximum analogue sensor divergence. Unit is internal resolution [IR] i.e. after scaling.	100	100

If the difference is greater than the threshold specified by P3375 for more than 100ms in one of the micro-controllers, safe state is triggered.

Micro-controller cross-check of scaled joystick position

After the joystick channel internal cross-check, the primary joystick position is scaled and cross-checked by the micro-controllers.

Parameter	Description	Default value	
		Main controller	Safety controller
P3368	Channel cross-check monitoring. Maximum analogue joystick position divergence time [x10ms]	10	10
P3369	Channel cross-check monitoring. Maximum analogue joystick position divergence [IR]	100	100

If the difference is greater than the threshold specified by P3369 for more than P3368ms, safe state is triggered.

Important

- Setting the value for P3375, P3368 or P3369 too high will reduce the monitoring performance.
- The monitoring technique is based on a comparison and uses a reference sensor. A diagnostic coverage in the range 90-99 % may be claimed provided that the sub-system is integrated according to the specification.
- Danfoss recommends setting P3351 to 100ms for consistency to the fixed 100 ms joystick channel internal cross-check divergence time.
- Record sensor data in different scenarios and use simulation for optimum monitoring performance tuning of P3375.

Fault Detection Algorithm – FDA

The cross-checked auxiliary steering device data is scaled to EH-valve main spool set-point and is monitored by the Fault Detection Algorithm (FDA). The Fault Detection Algorithm (FDA) checks the correlation plausibility between the a) wheel angle changes, b) the EH-valve main spool position and c) steering wheel movement. If an inconsistency is detected, the safe state is entered. For further information, see section 9.5.

Out of calibration check

The out of calibration check is checking that the safe sensor data from the analogue joystick, is within the calibrated range added a threshold specified in the table below. The out of calibration check is testing if the safe sensor data from the analogue joystick is exceeding the nominal range. This may happen due to changes (wear, tear, stress) in the mechanical or electrical installation of the analogue joystick.

Parameter	Description	Default value	
		Main controller	Safety controller
P3384	Maximum value which the safe sensor data from the analogue joystick is allowed to be out of the calibrated range [IR]	50	50

If the safe sensor data from the analogue joystick, is outside the calibrated range, by more than specified by P3384 for longer than 120ms, safe state is triggered.

8.3 CLOSED LOOP AUXILIARY STEERING DEVICE SENSOR SUB-SYSTEM SSM_064

The PVED-CLS offers the possibility to be use together with a closed loop joystick. A closed loop joystick is a steering device where the joystick position is directly related to the wheel angle. Based on the closed loop error, being the difference between the wheel angle set point and the actual wheel angle, the PVED-CLS calculates and outputs a flow command. The closed loop steering functionality in the PVED-CLS can only be used together with a CAN based joystick. Only one type of auxiliary steering device can be present in the system, see section 7.2.

The architecture shows how the PVED-CLS can be used as part of a closed loop auxiliary steering device sensor sub-system. The sub-system design supports realizing safety function designed to meet SIL2/PL d/AgPL d by designing the sub-system to a category 3 architecture.

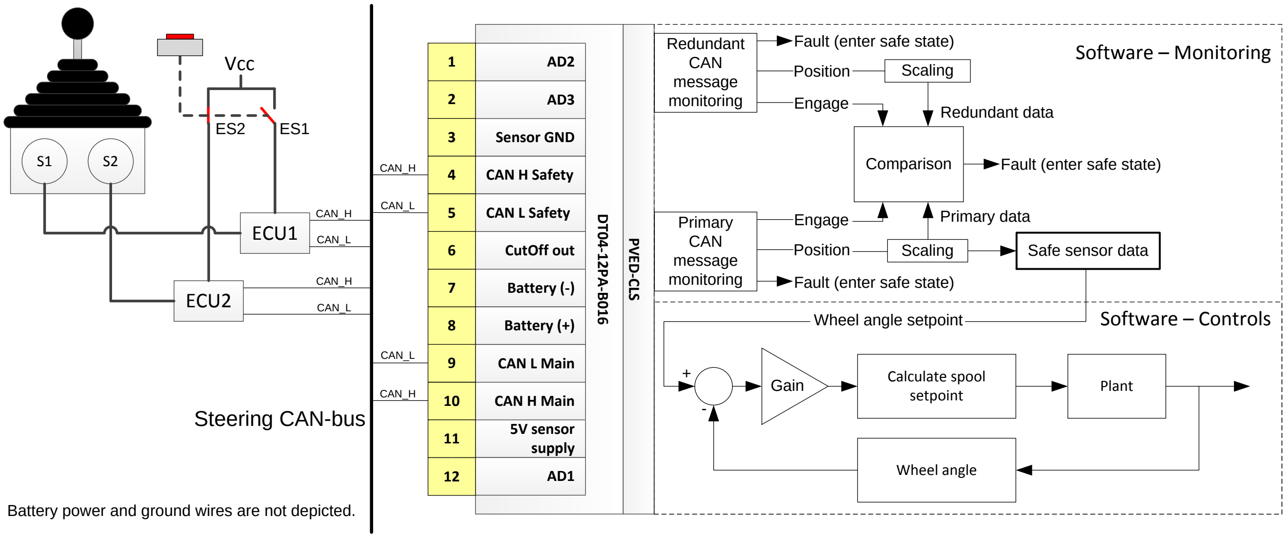


Figure 17: Closed loop joystick architecture.

Note 1: In the above diagram the blocked marked 'plant' represents EH-valve, hoses, steering cylinder and wheels.

Note 2: The wheel angle is measured by a wheel angle sensor, please refer to section 7.4, 7.5 and 7.6 which all deals with wheel angle sensors.

Note 3: In the above diagram the switches named ES1 and ES2 might both be normally closed or normally opened, as ISO 13849 states that a DC of 90 % might be claimed for such a configuration, however the system integrator shall ensure that the configuration of the engage button is fit for purpose. Please refer to ISO 13849-2 annex A and D, IEC 60947-5-1 and IEC 60204 for additional specifications.

Note 4: Other engage switch architectures may be used. The system integrator is responsible for the design, functionality and validation.

Primary joystick position sensor (S1, ECU1) and redundant joystick position sensor (S2, ECU2) shall be two channels which both acquire the joystick position. The main and safety controller receive, monitor and scale the input to the internal resolution range. Both the primary and redundant joystick position is transmitted onto the CAN bus via a safe protocol as the AUX sensor joystick messages.
Primary engage sensor (ES1, ECU1) and redundant engage sensor (ES2, ECU2) shall be a two channel switch which signals that engaging closed loop joy steering is requested. Both the primary and redundant engage signal is transmitted onto the CAN bus via a safe protocol and is also a part of the AUX sensor joystick messages.
See PVED-CLS communication protocol for details on the AUX sensor joystick message protocol.

Attention

The system integrator shall:

- Design and supply the closed loop auxiliary steering device sub-system.
- Ensure that the sub-system components are fit for the purpose.

- Conduct an FMEA to uncover dangerous failures.
- Implement measures against dangerous failures.
- Perform a CCF analysis.
- Document the sub-system as part of the safety case.

8.3.1.1 Interface - Closed loop joystick

The PVED-CLS main controller receives the primary message and the PVED-CLS safety controller receives the redundant message.

Parameter	Description	Main controller	Safety controller
P3239	Auxiliary steering device is present in the system (0 = Not present, 255 = Present)	255	255
P3240	Auxiliary steering device type (0 = Open loop joystick, 1 = Closed loop joystick, 2 = Mini-steering wheel, 3 = Analogue open loop joystick, 20 = Elobau® joystick)	1	1
P3300	Auxiliary joystick source address	78 (Default)	78 (Default)
P3322	Auxiliary joystick PGN offset	22 (Default)	23 (Default)

The MMI CAN command shall indicate if the PVED-CLS is allowed to follow the command from the closed loop auxiliary steering device or not. When the auxiliary steering device is locked out, the PVED-CLS awaits a steering command from any other present steering device. The PVED-CLS will suspend closed loop auxiliary steering as soon as the MMI command prohibit closed loop auxiliary steering. If an auxiliary steering device is configured to be present, the data from the AUX device will always be validated. Monitoring will only be suspended if the AUX steering device is configured as “not present” in the system. See PVED-CLS Communication protocol.

Important

- The applied safety protocol allows omitting the CAN bus from the safety loop calculation as it contributes less than 1 % of the SIL2.
- The applied safety protocol allows the presence of both safety and non-safety related CAN messages.
- The sub-system shall begin transmitting CAN messages no later than 10 seconds after the PVED-CLS is powered.
- At power on, it is recommended that the MMI CAN command signal ‘AUX steering device lockout’ is set to ‘AUX steering prohibited’.

8.3.1.2 Monitoring - Closed loop joystick

The PVED-CLS provides monitoring functions for the auxiliary joystick sub-system.
For both auxiliary steering device primary and redundant message, the following monitoring is in place in both the PVED-CLS main and safety controller:

- Receive timing check of CAN messages. Single failure leads to safe state.
- Sequence number check on CAN message. Single failure leads to safe state.
- End-to-end CRC on messages. Single failure leads to safe state.
- Data validity check (range check). Single failure leads to safe state.
- Primary and redundant data are cross-checked as follows:
  - If the absolute primary and redundant joystick position difference is > P3369 [IR] for more than P3368 x10ms, then enter safe state.
  - If the absolute primary and redundant engage signal is different is for more than P3387 [x10ms], then enter safe state.
  - If the absolute primary and redundant joystick trim signal difference is > P3389 [IR] for more than P3388 x10ms, then enter safe state.
- See PVED-CLS User Manual for CAN bus diagnostic trouble codes related to detecting different failures on the sensor sub-system.
- Fault Detection Algorithm (FDA), see section 9.5.

Parameter	Description	Default value
P3368	Channel cross-check monitoring. Maximum auxiliary joystick position divergence time [x10ms]	10
P3369	Channel cross-check monitoring. Maximum auxiliary joystick position difference [IR]	5
P3291	Maximum auxiliary device message timeout [x10ms]	8
P3387	Channel cross-check monitoring. Maximum closed loop joystick engage divergence time [x10ms]	10
P3388	Channel cross-check monitoring. Maximum auxiliary joystick trim divergence time [x10ms]	10
P3389	Channel cross-check monitoring. Maximum auxiliary joystick trim difference [IR]	50

Important

- Setting the value for P3368, P3369, P3291, P3387, P3388 and P3389 too high will reduce the monitoring performance.
- Set value of P3291 to 1.5 · nominal transmission rate.
- Design the auxiliary steering device sub-system channels to output as equal data as possible.
- Record sensor data in different scenarios and use simulation for optimum monitoring performance tuning.
- The monitoring technique is based on a comparison and reference sensors. A diagnostic coverage in the range 90-99 % may be claimed provided that the sub-system is integrated according to the specification.

Fault Detection Algorithm – FDA

The cross-checked auxiliary steering device data is scaled to EH-valve main spool set-point and is monitored by the Fault Detection Algorithm (FDA). The Fault Detection Algorithm (FDA) checks the correlation plausibility between the a) wheel angle changes, b) the EH-valve main spool position and c) steering wheel movement. If an inconsistency is detected, the safe state is entered. For further information, see section 9.5.

8.3.1.3 Safety channel calculation - Closed loop joystick

The wheel angle sensor, vehicle speed sensor and CAN based joystick shall be supplied by a third-party supplier and the architectures of these must conform to category 3. Identical channels are assumed, so for reliability calculation the following safety related block diagram shows an EH-steering system for closed loop joystick steering.

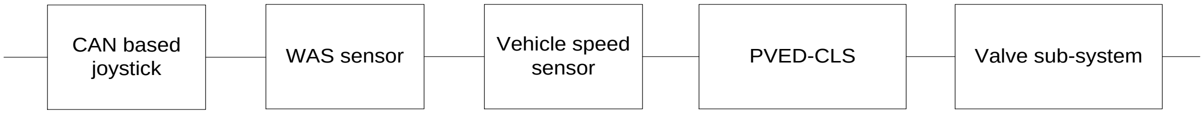


Figure 18 Safety related block diagram for CAN based joystick

- The target AgPLr is d
- The MTTFd,ch for the entire channel must be better than 10 years (medium) for a category 3 architecture.
- The DCavg must be ≥ 90% (for ISO25119 DCavg must be ≥ 60%).
- The MTTFd for the vehicle speed sub-system, wheel angle sensor and CAN based joystick are example value. Refer to the 3rd party supplier for precise values.
- The CAN bus takes less than 1% of SIL2 due to the applied safety protocol and is thus omitted for all sensors.

Sub-system monitoring	DC	Description
PVED-CLS, OSPE valve	95 %	Resulting DC per PVED-CLS FMEDA. Lowest number is applied for both channels.
CAN based joystick	99 %	The CAN based joystick is monitored by a comparison cross-check of channel 1 and 2
Vehicle speed sensor	99 %	The vehicle speed sensor sub-system is monitored by a comparison cross-check of vehicle speed channel 1 and 2.
Dual WAS	99 %	Monitoring for dual WAS is described in section 8.5.2 and 8.6.2.

The PVED-CLS safety related specifications are described in section 4.1.

Channel 1,2 elements	MTTFd [years]	DC [%]
CAN based joystick (example)	42	99
Dual WAS (example)	42	99
Vehicle speed sensor (example)	42	99
PVED-CLS, OSPE valve	36	95
MTTFd,ch	**10**	
DCavg		**97**

Refer to ISO 13849 for calculation of MTTFd,ch and DCavg.

The MTTFd,ch and the DCavg fulfills the requirement for meeting AgPL d with a category 3 architecture.

Attention

The system integrator shall:

- Design the auxiliary steering device sub-system.
- Ensure that the sub-system components are fit for the purpose.
- Conduct an FMEA to uncover dangerous failures.
- Implement measures against dangerous failures.
- Perform a CCF analysis.
- Document the sub-system as part of the safety case if it analyzed to be part of the safety function.
- Perform safety validation on the architecture.
- Ensure that the safety response time is acceptable.

Important

The safety response time is defined as the period of time between a fault is first observed by the diagnostics and the time by which the system is brought to a safe state, i.e. de-energizing the solenoid valves to bring the valve spool(s) within the hydraulic deadband (no valve output).

8.3.1.4 Safety channel calculation - Closed loop engage button

The wheel angle sensor, vehicle speed sensor and safe engage button shall be supplied by a 3rd party and the architectures of these must conform to category 3. Identical channels are assumed, so for reliability calculation the following safety related block diagram shows an EH-steering system for closed loop joystick steering.

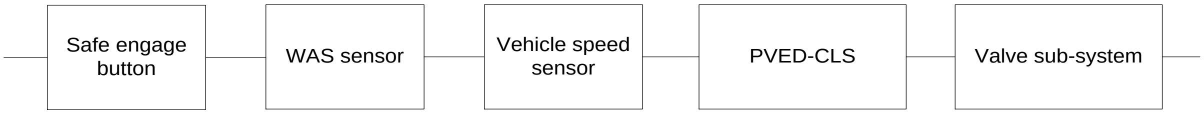


Figure 19: Safety related block diagram for safe engage button.

- The target AgPLr is d
- The MTTFd,ch for the entire channel must be better than 10 years (medium) for a category 3 architecture.
- The DCavg must be ≥ 90% (for ISO25119 DCavg must be ≥ 60%).
- The MTTFd for the vehicle speed sub-system, wheel angle sensor and safe engage button are example value. Refer to the 3rd party supplier for precise values.
- The CAN bus takes less than 1% of SIL2 due to the applied safety protocol and is thus omitted for all sensors.

Sub-system monitoring	DC	Description
PVED-CLS, OSPE valve	95 %	Resulting DC per PVED-CLS FMEDA. Lowest number is applied for both channels.
Safe engage button	90 %	The CAN based engage button is monitored by a comparison cross-check of channel 1 and 2
Vehicle speed sensor	99 %	The vehicle speed sensor sub-system is monitored by a comparison cross-check of vehicle speed channel 1 and 2.
Dual WAS	99 %	Monitoring for dual WAS is described in section 8.5.2 and 8.6.2.

The PVED-CLS safety related specifications are described in section 4.1.

Channel 1,2 elements	MTTFd [years]	DC [%]
Safe engage button (example)	42	90
Dual WAS (example)	42	99
Vehicle speed sensor (example)	42	99
PVED-CLS, OSPE valve	36	95
MTTFd,ch	**10**	
DCavg		**95**

Refer to ISO 13849 for calculation of MTTFd,ch and DCavg.

The MTTFd,ch and the DCavg fulfills the requirement for meeting AgPL d with a category 3 architecture.

Attention

The system integrator shall:

- Design the engage button sub-system.
- Ensure that the sub-system components are fit for the purpose.
- Conduct an FMEA to uncover dangerous failures.
- Implement measures against dangerous failures.
- Perform a CCF analysis.
- Document the sub-system as part of the safety case if it analyzed to be part of the safety function.
- Perform safety validation on the architecture.
- Ensure that the safety response time is acceptable.

Important

The safety response time is defined as the period of time between a fault is first observed by the diagnostics and the time by which the system is brought to a safe state, i.e. de-energizing the solenoid valves to bring the valve spool(s) within the hydraulic deadband (no valve output).

8.4 SAFE CLOSED LOOP JOYSTICK ENGAGE SSM_063

The safety related control function prevents unintended activation of the closed loop joystick steering.

Operation

Two criteria shall be fulfilled before the decision is taken to engage closed loop joystick steering:

1. The enable flag is set. The enable flag is set by activation of the engage button.
2. The absolute value of the closed loop error, being the difference between the wheel angle set point and the actual wheel angle, may not be greater than the specified limit (P3732).

Parameter	Description	Recommended value
P3732	Maximum closed loop error allowed to engage closed loop steering [IR]	100

Important

Setting P3732 too high may cause large unwanted wheel movement.

Attention ⚠	**When closed loop steering is requested the closed loop error must be minimized in order to prevent large unwanted wheel movement.**

8.5 WHEEL ANGLE SENSOR (WAS) – DUAL CHANNEL ANALOGUE SSM_018

A dual channel analogue wheel angle sensor can be connected to the PVED-CLS when a high diagnostic performance is required for reaching the highest possible safety integrity level or performance level. The architecture shows how the PVED-CLS can be used as part of a wheel angle sensor (WAS) sub-system. The sub-system design supports realizing safety function designed to meet SIL2/PL d/AgPL d by designing the sub-system to a category 3 architecture.

Attention

The system integrator shall:

- Design and supply the wheel angle sensor sub-system.
- Ensure that the sub-system components are fit for the purpose.
- Conduct an FMEA to uncover dangerous failures.
- Implement measures against dangerous failures.
- Perform a CCF analysis.
- Document the sub-system as part of the safety case.

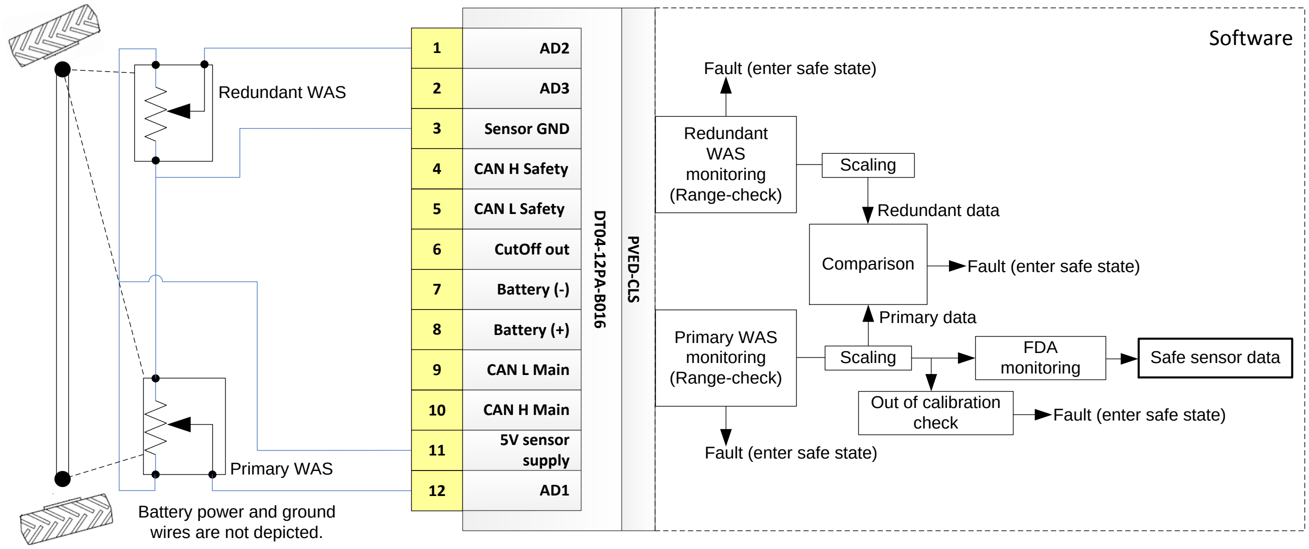


Figure 20: Dual channel analogue wheel angle sensor architecture.

The primary WAS and redundant WAS can be installed on the same kingpin or on each kingpin.

Two independent single-channel WAS sensors or an integrated dual channel WAS shall be installed to measure the steered wheel angle or articulation angle of the vehicle. The WAS sensors may be installed to measure the steered angle on one wheel or on both. The main and safety controller receive, monitor and scale the input to the internal resolution range. The WAS can be supplied by any stabilized 5V supply or from the PVED-CLS 5V sensor supply. The PVED-CLS 5V sensor supply is internally monitored and adjusts for output drift and short-circuits faults. See PVED-CLS User Manual for further information on the 5V sensor supply.

8.5.1 Analogue interface

The WAS signal on AD1 and AD2 shall be in the range 500 mV to 4500 mV. The safety related parameters related to dual channel WAS are:

Parameter	Description	Main controller	Safety controller
P3245	Redundant WAS present. (0= Not present, 255 = Present (Default))	255	255
P3244	WAS interface type. (0 = Analogue (Default), 1 = CAN, 2 = None)	0	0

Important

- The WAS steered angle-to-signal characteristic shall be mutually inverted for the PVED-CLS to monitor a common 5V sensor supply.
- The PVED-CLS cannot detect if a one WAS output is unintended connected to both AD1 and AD2. In this situation, the sub-system is not suitable as part of a category 3 architecture.
- Care must be taken by the system integrator when installing two identical WAS sensors, to avoid accidently connecting one output to both inputs.
- Use independent sensor supply sources if WAS with non-inverted output characteristics are used.
- The steered wheel or articulation angle sensor resolution shall be better than 20°/V.
- The voltage representing straight shall be approximately in the middle of the achieved voltage range.

Refer to the PVED-CLS user manual for AD1 and AD2 calibrating for the WAS

8.5.2 Monitoring

The PVED-CLS provides monitoring function for the WAS sub-system.

- Input range check
- WAS channel cross-check
- Micro-controller cross-check of scaled wheel angle
- Fault Detection Algorithm
- Out of calibration check

Input range check

AD1 and AD2 input values below 100mV and above 4900mV are detected as short-circuit to ground and supply respectively.

WAS channel cross-check

The PVED-CLS will perform cross-check monitoring on the wheel angle signal from the primary and redundant wheel angle sensor. This check is performed in both micro-controllers.

Parameter	Description	Default value	
		Main controller	Safety controller
P3375	Analogue sensor cross-check monitoring. Maximum analogue sensor divergence. Unit is internal resolution [IR] i.e. after scaling.	100	100

If the difference is greater than the threshold specified by P3375 for more than 100ms in one of the micro-controllers, safe state is triggered.

Micro-controller cross-check of scaled wheel angle

After the internal WAS channel cross-check, the primary wheel angle is scaled and cross-checked by the micro-controllers.

Parameter	Description	Default value	
		Main controller	Safety controller
P3351	Channel cross-check monitoring. Maximum steering wheel angle divergence time [x10ms]	10	10

P3352	Channel cross-check monitoring. Maximum wheel angle divergence [IR]	100	100

If the difference is greater than the threshold specified by P3352 for more than P3351ms, safe state is triggered.

Important

- Setting the value for P3375, P3351 or P3352 too high will reduce the monitoring performance.
- The monitoring technique is based on a comparison and uses a reference sensor. A diagnostic coverage in the range 90-99 % may be claimed provided that the sub-system is integrated according to the specification.
- P3375 is not relevant if the system is configured to use a single WAS.
- Danfoss recommends setting P3351 to 100 ms for consistency to the fixed 100 ms WAS channel internal cross-check divergence time.
- Danfoss recommends setting P3375 to 100 if a dual channel WAS is used on one kingpin.
- If two single channel WASs are mounted on each kingpin, Danfoss recommends P3375 to be set 150 due to the difference in angles steering left and right, with reference to the turning point.
- Record sensor data in different scenarios and use simulation for optimum monitoring performance tuning of P3375.

Fault Detection Algorithm – FDA

The cross-checked wheel angle sensor data is monitored by the Fault Detection Algorithm (FDA) which checks the correlation plausibility between the a) wheel angle changes, b) the EH-valve main spool position and c) steering wheel movement. If an inconsistency is detected, the safe state is entered.

FDA can detect the following common cause faults related to the wheel angle sensor:

- Loss of mechanical connection between the WAS and the kingpin.
- WAS electrical "stuck-at" faults
- Channel short-circuits if both channels output a valid voltage during this failure mode.

For further information, see section 9.5.

Out of calibration check

The out of calibration check is checking that the safe sensor data from the wheel angle sensor, is within the calibrated range added a threshold specified in the table below. The out of calibration check is testing if the safe sensor data from the wheel angle sensor is exceeding the nominal range. This may happen due to changes (wear, tear, stress) in the mechanical or electrical installation of the wheel angle sensor.

Parameter	Description	Default value	
		Main controller	Safety controller
P3384	Maximum value which the safe sensor data from the wheel angle sensor is allowed to be out of the calibrated range [IR]	50	50

If the safe sensor data from the wheel angle sensor, is outside the calibrated range, by more than specified by P3384 for longer than 120 ms, safe state is triggered.

8.6 WHEEL ANGLE SENSOR (WAS) – CAN BASED SSM_019

The steered wheel angle can be supplied via the CAN bus. The principle is identical to having a dual analogue wheel angle sensor except that sampling the angle sensors is now performed by external controllers. The sampled values in mV are transmitted via a safe protocol.

The architecture shows how the PVED-CLS can be used as part of a CAN based wheel angle sensor sub-system. The sub-system design supports realizing safety function designed to meet SIL2/PL d/AgPL d by designing the sub-system to a category 3 architecture.

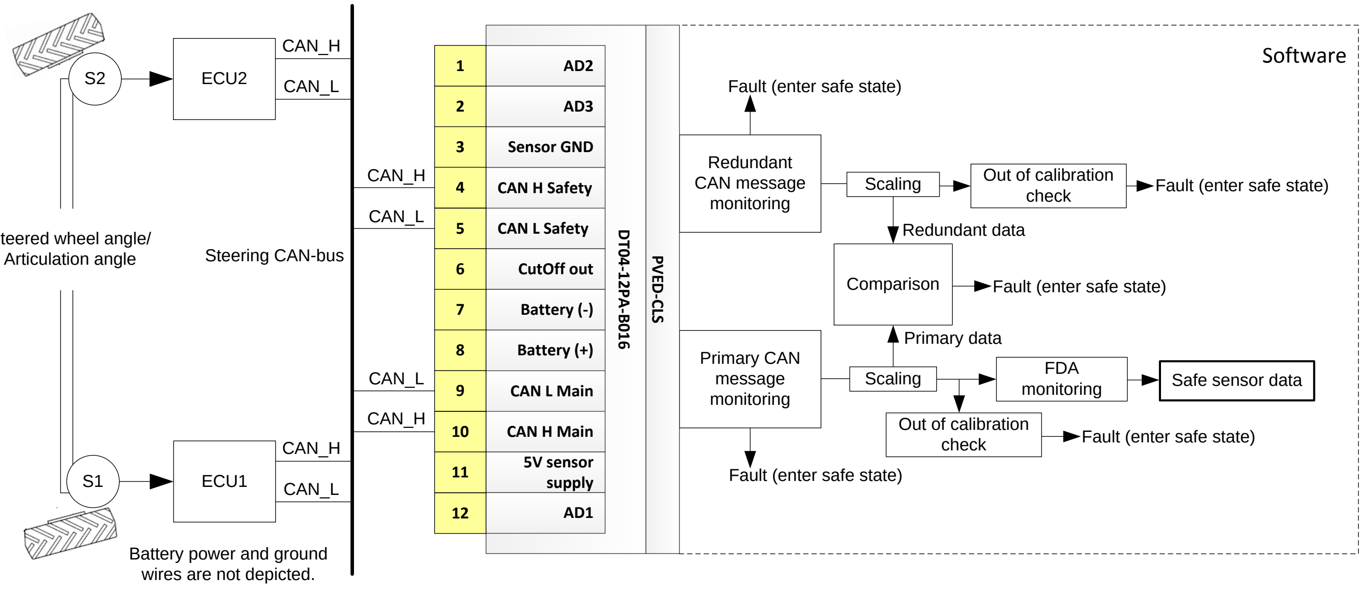


Figure 21: CAN based wheel angle sensor architecture.

S1 and S2 can be installed on the same kingpin or on separate kingpins.

Primary wheel angle sensor (S1, ECU1) and redundant wheel angle sensor (S2, ECU2) shall be two channels which both acquire the steered wheel angle. The ECU1 acquires the steered wheel position via sensor element S1 and scales it to a voltage. The voltage, representing a steered wheel angle, is transmitted onto the CAN bus via a safe protocol as the primary wheel angle sensor message. The same applies for the redundant wheel angle message, where ECU2 transmits the redundant wheel angle sensor message. See PVED-CLS communication protocol for details on the wheel angle sensor message protocol. The main and safety controller receive, monitor and scale the input to the internal resolution range.

Attention

The system integrator shall:

- Design and supply the steering wheel sensor sub-system.
- Ensure that the sub-system components are fit for the purpose.
- Conduct an FMEA to uncover dangerous failures.
- Implement measures against dangerous failures.
- Perform a CCF analysis.
- Document the sub-system as part of the safety case.

8.6.1 CAN interface

The PVED-CLS main controller receives the primary steering angle sensor message and the PVED-CLS safety controller receives the redundant steering angle message.

Parameter	Description	Main controller	Safety controller
P3244	WAS interface type. (0 = Analogue (Default), 1 = CAN, 2 = None)	1	1
P3298	Steering wheel angle sensor source address.	250	250
P3320	Steering wheel angle sensor PGN offset.	18	19

Important

- The applied safety protocol allows omitting the CAN bus from the safety loop calculation as it contributes less than 1% of the safety integrity level.
- The applied safety protocol allows the presence of both safety and non-safety related CAN messages.
- P3298 may be equal for both primary and redundant message if they are transmitted by one CAN node.
- For redundant WAS configurations P3298 for the main and safety controller shall be different.
- The sub-system shall begin transmitting CAN messages no later than 10 seconds after the PVED-CLS is powered.
- Single channel CAN based WAS configuration is not possible.
- The steered wheel or articulation angle sensor resolution shall be better than 0.023°/mV.

8.6.2 Monitoring

The PVED-CLS provides monitoring function for the WAS sub-system.

- Input range check
- Micro-controller WAS channel cross-check
- Fault Detection Algorithm
- Out of calibration check

Input range check

WAS signal values below 100 and above 4900 are detected as short-circuit to ground and supply respectively.

Micro-controller WAS channel cross-check

The PVED-CLS will perform cross-check monitoring on the wheel angle signal from the primary and redundant wheel angle sensor by an internal micro-controller data exchange and comparison.

Parameter	Description	Default value	
		Main controller	Safety controller
P3352	Wheel angle sensor cross-check monitoring. Maximum wheel angle divergence. Unit is internal resolution [IR] i.e. after scaling.	100	100
P3351	Channel cross-check monitoring. Maximum steering wheel angle divergence time [x10ms]	10	10
P3290	Maximum message timeout [x10ms]	8	8

If the difference is greater than the threshold specified by P3352 for more than P3351 ms, safe state is triggered.

Important

- Set value of P3290 to 1.5 · nominal transmission rate.
- Setting the value for P3352, P3351 or P3290 too high will reduce the monitoring performance.
- The monitoring technique is based on a comparison and uses a reference sensor. A diagnostic coverage in the range 90-99 % may be claimed provided that the sub-system is integrated according to the specification.
- Danfoss recommends setting P3352 to 100 if a dual channel WAS is used on one kingpin.

- If two single channel WASs are mounted, one on each kingpin, Danfoss recommends P3352 to be set 150 due to the difference in angles steering left and right, with reference to the turning point.
- Record sensor data in different scenarios and use simulation for optimum monitoring performance tuning.

Fault Detection Algorithm – FDA

The cross-checked wheel angle sensor data is monitored by the Fault Detection Algorithm (FDA) which checks the correlation plausibility between the a) wheel angle changes, b) the EH-valve main spool position and c) steering wheel movement. If an inconsistency is detected, the safe state is entered.
FDA can detect the following common cause faults related to the wheel angle sensor:

- Loss of mechanical connection between the WAS and the kingpin.
- WAS electrical "stuck-at" faults
- Channel short-circuits if both channels output a valid voltage during this failure mode.

For further information, see section 9.5.

Out of calibration check

The out of calibration check is checking that the wheel angle read from both the primary and redundant wheel angle message, is within the calibrated range added a threshold which is specified in the table below. The out of calibration check is testing if the safe sensor data from the wheel angle sensor is exceeding the nominal range. This may happen due to changes (wear, tear, stress) in the mechanical or electrical installation of the wheel angle sensor.

Parameter	Description	Default value	
		Main controller	Safety controller
P3390	Maximum value which the primary and redundant wheel angle signal are allowed to be out of the calibrated range [IR]	50	50

If the wheel angle read from the primary or the redundant wheel angle message is out of the calibrated range by more that threshold specified by P3384 for more than 120 ms, safe state is triggered.

8.7 WHEEL ANGLE SENSOR (WAS) – SINGLE CHANNEL ANALOGUE SSM_020

The steered wheel angle can be supplied as a single channel analogue signal to a PVED-CLS analogue input. The architecture shows how the PVED-CLS can be used as part of a wheel angle sensor (WAS) sub-system which meets architecture category 2 requirements.

Attention

The system integrator shall:

- Design and supply the wheel angle sensor sub-system.
- Ensure that the sub-system components are fit for the purpose.
- Conduct an FMEA to uncover dangerous failures.
- Implement measures against dangerous failures.
- Document the sub-system as part of the safety case.

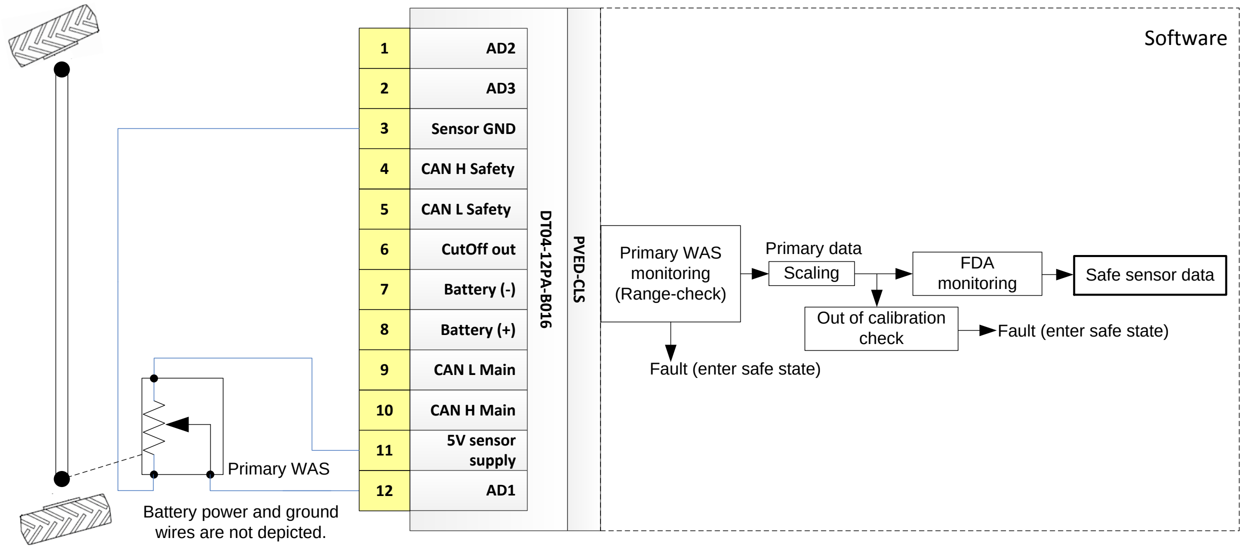


Figure 22: Single channel analogue wheel angle sensor architecture.

A single-channel WAS sensors shall be installed to measure the steered wheel angle or articulation angle of the vehicle. The main and safety controller both receive, monitor and scale the AD1 input to the internal resolution range. The software in both controllers performs monitoring on the WAS prior to passing it for further calculation.
The WAS can be supplied by any stabilized 5V supply or from the PVED-CLS 5 V sensor supply. The PVED-CLS 5 V sensor supply is internally monitored and can detect short-circuits.

8.7.1 Analogue interface

The WAS signal on AD1 shall be in the range 500 mV to 4500 mV. The safety related parameters related to single dual channel WAS are:

Parameter	Description	Main controller	Safety controller
P3245	Redundant WAS present. (0= Not present, 255 = Present (Default))	0	0
P3244	WAS interface type. (0 = Analogue (Default), 1 = CAN, 2 = None)	0	0

The AD2 input may be left unconnected. For single channel WAS configurations this input is ignored.

Important

- The voltage representing straight shall be approximately in the middle of the achieved voltage range.
- The steered wheel or articulation angle sensor resolution shall be better than 20°/V.

Refer to the PVED-CLS user manual for AD1 and AD2 calibration of the WAS

8.7.2 Monitoring

The PVED-CLS provides monitoring function for the WAS sub-system.

- Input range check
- Fault Detection Algorithm
- Out of calibration check

Input range check

AD1 input values below 100 mV and above 4900 mV are detected as short-circuit to ground and supply respectively.

Important

Input range checking is based on monitoring some characteristics of the sensor (range). No diagnostic coverage should be claimed by this principle.

Fault Detection Algorithm – FDA

The range checked wheel angle sensor data is monitored by the Fault Detection Algorithm (FDA) which checks the correlation plausibility between the a) wheel angle changes, b) the EH-valve main spool position and c) steering wheel movement. If an inconsistency is detected, the safe state is entered.

FDA can detect the faults related to the wheel angle sensor:

- Loss of mechanical connection between the WAS and the kingpin.
- WAS electrical "stuck-at" faults

For further information, see section 9.5.

Important

- Monitoring by FDA is an instance of fault detection by the process. It may also be regarded as a reference sensor to the WAS. A diagnostic coverage in the range 60-90 % may be claimed for this principle.
- Danfoss recommends that fault insertion testing is used on the final installation to validate the claimed diagnostic coverage.

Out of calibration check

The out of calibration check is checking that the safe sensor data from the wheel angle sensor, is within the calibrated range plus a threshold specified in the table below. The out of calibration check is testing if the safe sensor data from the wheel angle sensor is exceeding the nominal range. This may happen due to changes (wear, tear, stress) in the mechanical or electrical installation of the wheel angle sensor.

Parameter	Description	Default value	
		Main controller	Safety controller
P3384	Maximum value which the safe sensor data from the wheel angle sensor is allowed to be out of the calibrated range [IR]	50	50

If the safe sensor data from the wheel angle sensor, is outside the calibrated range, by more than specified by P3384 for longer than 120 ms, safe state is triggered.

8.8 VEHICLE SPEED SENSOR SSM_021

The architecture shows how the PVED-CLS can be used as part of a vehicle speed sub-system.
The sub-system design supports realizing safety function designed to meet SIL2/PL d/AgPL d by designing the sub-system to a category 3 architecture.

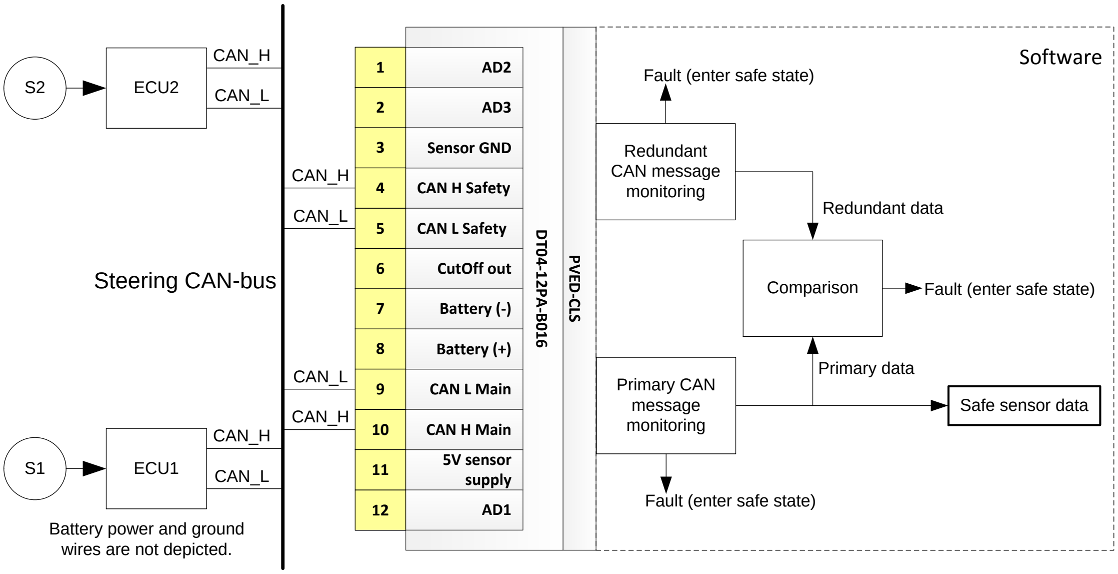


Figure 23: Vehicle speed sensor architecture.

Primary vehicle speed sensor (S1, ECU1) and redundant vehicle speed sensor (S2, ECU2) shall be two channels which both acquire the vehicle speed independently. The ECU1 acquires a speed signal via sensor element S1 and scales it to representing a vehicle speed. The vehicle speed data is transmitted onto the CAN bus via a safe protocol as the VSP primary message. The same applied for the redundant vehicle speed sensor, where ECU2 transmits the VSP redundant message. See PVED-CLS communication protocol for details on the vehicle speed message protocol.

The functional safety requirements to the primary and redundant vehicle speed sensor is that both channels shall have a systematic capability of 1. This can be achieved if both channels meet QM/SIL1 and the channels are sufficiently independent and functionally diverse. By applying the concept of 'synthesis of elements', a resulting systematic capability of 2 can be claimed accordance with safety standard IEC 61508 and thus meeting SIL2/AgPL/PL d requirements.

Attention ⚠	**The vehicle speed is a critical signal for the majority of the safety functions.**

The system integrator shall:

- Design and supply the vehicle speed sub-system.
- Ensure that the sub-system components are fit for the purpose.
- Conduct an FMEA to uncover dangerous failures.
- Implement measures against dangerous failures.
- Perform a CCF analysis.
- Document the sub-system as part of the safety case.
- Failing to supply the PVED-CLS with safe vehicle speed information will invalidate the functional safety concept.

8.8.1 CAN interface

The PVED-CLS main controller receives the VSP primary message and the PVED-CLS safety controller receives the VSP redundant message.

Parameter	Description	Default value	
		Main controller	Safety controller
P3294	Vehicle speed sensor source address	251	251
P3318	Vehicle speed sensor PGN offset	64	65

Important

- The applied safety protocol allows omitting the CAN bus from the safety loop calculation as it contributes less than 1% of the safety integrity level.
- The applied safety protocol allows the presence of both safety and non-safety related CAN messages.
- P3318 shall be different in the main and safety controller as two CAN nodes are not allowed to have the same source address.
- The sub-system shall begin transmitting CAN messages no later than 10 seconds after the PVED-CLS is powered.

8.8.2 Monitoring

The PVED-CLS provides monitoring functions for the vehicle speed sensor sub-system.
For both VSP primary and redundant message (see PVED-CLS communication protocol) the following monitoring is in place in both the PVED-CLS main and safety controller:

- Receive timing check of CAN messages. Single failure leads to safe state.
- Sequence number check on CAN message. Single failure leads to safe state.
- End-to-end CRC on messages. Single failure leads to safe state.
- Data validity check (range check on vehicle speed data). Single failure leads to safe state.
- Range check on 'Direction indication'. A single instance of 'Error condition' leads to safe state.
  Note: Setting the 'Direction indication' to 'Information not available' is regarded as 'Forward'.
- The forward and reverse flags are cross-checked as follows: The 'Direction indication' field determines the sign of the vehicle speed data which is cross-checked.
- Primary and redundant data are cross-checked as follows: If the absolute primary and redundant difference is > P3364 km/h for more than P3363 ms, then enter safe state.
- See PVED-CLS User Manual for CAN bus diagnostic trouble codes related to detecting different failures on the vehicle speed sensor sub-system.

Parameter	Description	Default value
P3364	Channel cross-check monitoring. Maximum vehicle speed divergence [km/h].	5
P3363	Channel cross-check monitoring. Maximum vehicle speed divergence time [x10msec].	10
P3288	Maximum message timeout [x10ms].	15

Important

- Setting the value for P3363, P3364 or P3288 too high will reduce the monitoring performance.
- The monitoring technique is based on a comparison and uses a reference sensor. A diagnostic coverage in the range 90-99% may be claimed provided that the sub-system is integrated according to the specification.
- Set value of P3288 to 1.5 · nominal transmission rate.
- Design the sensor sub-system channels to output as equal data as possible.
- Record vehicle speed sensor data in different scenarios and use simulation for optimum monitoring performance tuning.

8.9 AUTO-GUIDANCE SUB-SYSTEM SSM_022

It is possible to connect up to two independent and co-existing auto-guidance controllers to the PVED-CLS. Only one auto-guidance controller can be active at a time. An external ECU must via the MMI command interface inform the PVED-CLS which auto-guidance controller to take commands from. Both auto-guidance controllers shall transmit ISO11783 Guidance Machine Commands. See PVED-CLS Communication protocol. The PVED-CLS safety functions will work on the active auto-guidance controller input.

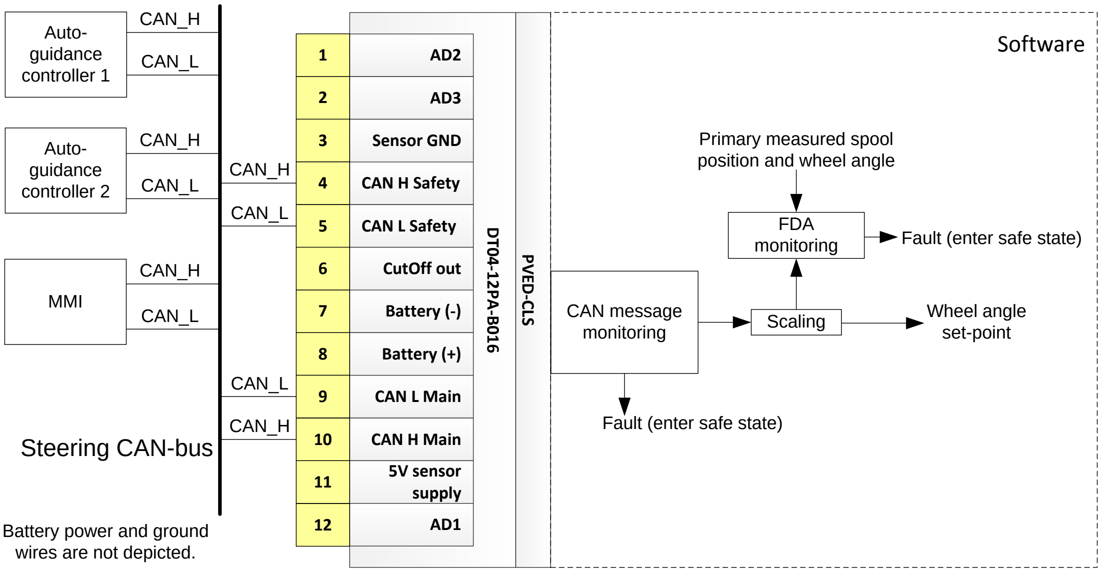


Figure 24: Auto-guidance sub-system architecture.

The guidance machine commands are received by the main controller which performs timing monitoring on the selected auto-guidance controller. No further validation is performed on the data before it is shared to the safety micro-controller via an internal communication link.

8.9.1 CAN interface

Parameter	Description	Main controller	Safety controller
P3237	Auto-guidance controller 1 present. (0 = not present, 255 = present (default))	255	255
P3238	Auto-guidance controller 2 present. (0 = not present, 255 = present (default))	255	255
P3292	Auto-guidance controller 1 source address	28	28
P3293	Auto-guidance controller 2 source address	29	29

The MMI CAN command indicates which auto-guidance controller the PVED-CLS shall be receive data from. See PVED-CLS Communication protocol. The MMI controller can de-select one or both auto-guidance controllers. The PVED-CLS will suspend auto-guidance steering as soon as the MMI command de-selects an auto-guidance controller from steering. When an auto-guidance controller is de-selected out, the PVED-CLS awaits a steering command from any configured steering device. Monitoring is suspended on disabled auto-guidance controller(s).

Important

At power on, it is recommended that the MMI CAN command signal 'Auto-guidance receiver selection and lockout' is set to 'No GPS receiver selected'.

8.9.2 Monitoring

The PVED-CLS provides monitoring functions for the received auto-guidance CAN commands. The ISO11783 guidance machine commands do not utilize a safety protocol. Monitoring is thus reduced to monitoring the receive timing. If t

Parameter	Description	Default value
P3289	Guidance Machine status time-out [x10ms]	28

If the time between two messages exceeds P3289ms, then the PVED-CLS will disengage auto-guidance and await a steering device request from any steering device.

8.10 ROAD-SWITCH FOR OSPE, EHI-E AND EHI-H VALVE SUB-SYSTEMS SSM_023

A road switch sub-system can be used for bringing the PVED-CLS and OSPE, EHi-E and EHi-H valve sub-systems into a state which is suitable for on-road operation while keeping the PVED-CLS operational. The below architecture is suitable for achieving SIL 3, PL e for shutting off of EH-steering flows for public road transportation. The PVED-CLS can remain powered in this state.

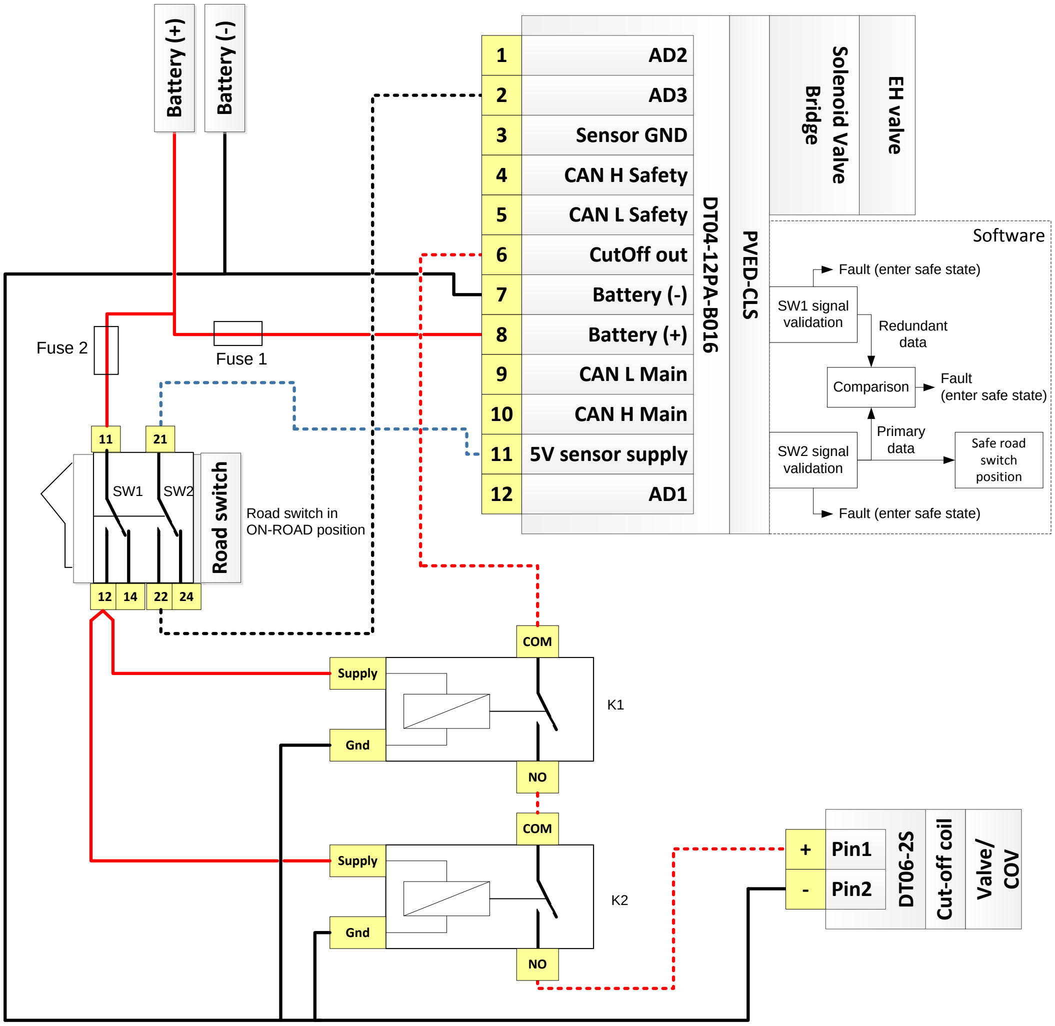


Figure 25: Road-Switch architecture for OSPE, EHi-E and EHi-H valve sub-systems.

To achieve SIL3/PL e with the PVED-CLS, an independent and diverse shut-down channel using two relays to disconnect the power to the cut-off valve, shall work in parallel with the PVED-CLS.

Operation

Input redundancy is achieved by using redundant switch, SW1 and SW2. Redundancy on the logic for de-powering the valves is achieved by using the PVED-CLS to control the EH-valve and relay logic for de-energizing the coil for the cut-off solenoid valve.

Redundancy on de-energizing the valves is achieved by de-energizing the solenoid valve bridge and the cut-off solenoid valve.

Important

- Reaching the target safety integrity requires a correct installation.
- Single faults may not be detected but the safety function is not lost.
- The safety function can be demanded in the presence of two undetected faults.

- Two undetected failures are detected on demanding the safety function.

To enable the road switch interface for a PVED-CLS and OSPE valve, the following parameter settings are required.

Parameter	Description	Main controller	Safety controller
P3072	External cut-off valve present. (0 = not present, 255 = present (default))	255	255
P3241	Road switch present. 255 = present. (0 = not present, 255 = present (default))	255	255
P3242	Road switch resistance check enabled. (0 = disabled (default), 255 = enabled)	0	0

Important

The safety function will only work for OSPE valve systems when the above parameters are set as specified.

Attention

⚠

The system integrator shall:

- Supply the road switch and relay components.
- Ensure that the switch, relay, wiring and installation enclosure satisfies the requirements in ISO 13849-2 annex A and D, IEC 60947-5-1 and IEC 60204.
- Ensure that the sub-system components are fit for the purpose.
- Conduct an FMEA to uncover dangerous failures.
- Implement measures against dangerous failures.
- Perform a CCF analysis.
- Carry out verification and validation of the architecture on commissioning and after maintenance.

8.10.1 Interface

The road switch SW2 controls the PVED-CLS power to the solenoid valve bridge. SW1 controls the power to the relay logic. The state of SW1 switch position is obtained by the PVED-CLS by measuring the relay contact state via a current measurement and test pulse monitoring.

Road switch position		PVED-CLS enable (AD3)	Relay supply	Relay contacts	Cut-off valve
Off-road	SW1 closed		Battery supply	Closed	Can be pressurized
	SW2 closed	EH-steering enabled 4700mV < AD3 input < 5300mV			
On-road	SW1 open		0V	Open	De-energized
	SW2 open	EH-steering disabled/prohibited AD3 input < 500mV			

Important

- The electrical requirements of the relay must be respected.
- The sub-system shall supply a valid input on AD3 no later than 10 seconds after the PVED-CLS is powered.

8.10.2 Monitoring

The SW2 signal supplied to AD3 is range checked. If the voltage is out of the on-road or the off-road voltage range for more than 100ms, then the PVED-CLS enters safe state.

The 5 V sensor supply line is monitored. If the supply voltage is overloaded or short-circuited causing it exceeds the nominal voltage, the PVED-CLS enters safe state.

Monitoring of the switch is performed by the PVED-CLS by comparing the output of SW1 and SW2.
SW2 switches the 5V supply voltage to the PVED-CLS AD3 input. The PVED-CLS validates the input voltage on AD3. If the voltage is in the range 5 V ±300 mV, then SW2 is determined to be in off-road mode. If the voltage is below 500 mV, then SW2 is determined to be on-road position. The PVED-CLS will enter safe state if the AD3 input voltage is outside the two voltage ranges for more than 100 ms.

SW2 is monitored via PVED-CLS cut-off output pin 6. When SW21 signals on-road mode, the PVED-CLS switches off the power to the solenoid valve (sourced from the Cut-off output) and 100 ms after AD3 has changed from off-road mode to on-road mode (see note 1), the PVED-CLS starts a low-power test pulse pattern to measure that no electrical connection exists to the solenoid valve. If the low-power test pulse leads to a current build-up, then the PVED-CLS enter safe state. The monitoring principle is equivalent to cross-monitoring SW1 and SW2. It cannot be determined if the failure is caused by SW1 or one of the relays.
The low-power test pulse cannot lead to pressuring the cut-off valve.

When SW2 signals off-road mode, the PVED-CLS cut-off output will stop outputting low-power test pulses and start to supply current to the solenoid valve to pressurize the cut-off valve. The PVED-CLS monitors the current that is supplied to the solenoid valve. If the supplied current does reach 50% of the current set-point, then the PVED-CLS will enter safe state. The PVED-CLS cannot detect a welded relay contacts while operating in off-road mode. On switching to on-road mode (demanding the safety function), the current supply to the solenoid valve will stop and the low-power test pulses will detect the two welded relays or SW1 stuck at off-road position.

Note 1: The delay of 100ms from the mode has changed to on-road mode until low-power test pulse pattern starts, has been introduced in order to prevent false errors caused by relay-contact bounce.

Important

- The monitoring technique is based on a comparison with a reference sensor technique. A diagnostic coverage in the range 90-99 % may be claimed provided that the sub-system is integrated according to the specification.
- Some single faults cannot be detected until a second fault occurs.
- Two undetected faults may be present but the safety function is not lost.
- The two undetected faults will be detected when the safety function is demanded (on-road mode).

8.11 ROAD-SWITCH FOR EHPS VALVE SUB-SYSTEMS SSM_024

A road switch sub-system can be used for bringing the PVED-CLS and EHPS valve sub-system into a state which is suitable for on-road operation while keeping the PVED-CLS operational. The solenoid valve bridge is de-energized in on-road mode. The below architecture category 2 is suitable for achieving SIL 2, PL d and AgPL d for the shut off of EH-steering flows for public road transportation.

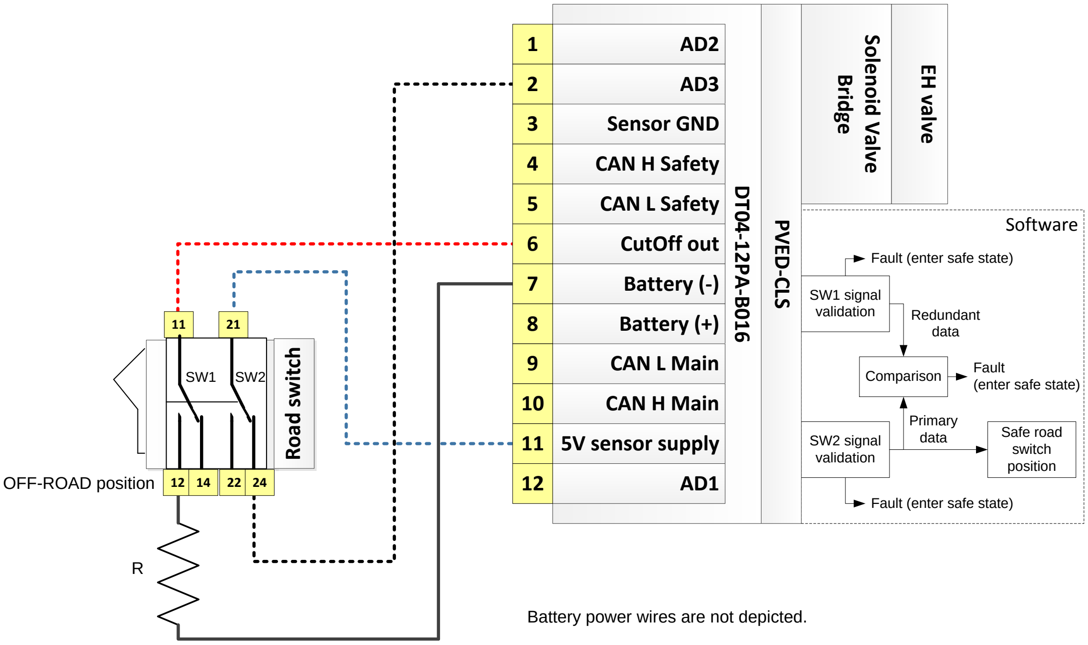


Figure 26: Road-Switch architecture for EHPS valve sub-systems.

Operation

Input redundancy is achieved by using redundant switch, SW1 and SW2.
SW2 switches a 5 V supply to the PVED-CLS AD3 input. SW1 switches the output of PVED-CLS cut-off valve output to a resistor. The cut-off valve output, supplies power via a high side switch with internal current monitoring. The internal current measurement is used to calculate the load resistance which yields the measured output of the SW1 output. A load resistor, R, is required to establish a well-defined current when SW1 is closed.

Both the main and safety controller energize and de-energize the solenoid valve bridge depending on SW1 and SW2 respectively.

To enable the road switch interface for a PVED-CLS and EHPS valve, the following parameter settings are required.

Parameter	Description	Main controller	Safety controller
P3072	External cut-off valve present. (0 = not present, 255 = (default))	0	0
P3241	Road switch present. (0 = not present, 255 = present (default))	255	255
3242	Road switch resistance check enabled. (0 = disabled (default), 255 = enabled)	255	255

Important
The safety function will only work for EHPS valve systems when the above parameters are set as specified.

Attention

The system integrator shall ensure:

- Supply the road switch, relay and load resistor.

- Ensure that the switch, relay, wiring and installation enclosure satisfies the requirements in ISO 13849-2 annex A and D, IEC 60947-5-1 and IEC 60204.
- Failing to enable the road switch resistance check will lead to ignoring the input from SW2.
- Ensure that the sub-system components are fit for the purpose (see ISO13849)
- Conduct an FMEA to uncover dangerous failures.
- Implement measures against dangerous failures.
- Perform a CCF analysis.
- The resistor shall be dimensioned to reduce the current to nominally 300 mA at 12 V battery supply when SW1 is closed.
- The current must not be lower than 175 mA.

8.11.1 Interface

Road switch SW1 and SW2 shall supply input signals to the PVED-CLS according to the below table.

Road switch position		PVED-CLS SW1 input (cut-off valve output)	PVED-CLS SW2 input (AD3)
Off-road	SW1 Open	measured resistance > 200 Ω	
	SW2 closed		4700 mV < AD3 input < 5300 mV
On-road	SW1 Closed	20 Ω < measured resistance < 100 Ω (Note 1)	
	SW2 open		AD3 input < 500 mV

SW1 and SW2 position are cross-checked. If the measures position differs, the PVED-CLS enter safe state.

Note 1: It is advised that the impedance for SW1 Closed is between 20 Ω and 70 Ω, in order to increase the robustness of the implementation.

Important

The sub-system shall supply a valid input on AD3 no later than 10 seconds after the PVED-CLS is powered.

8.11.2 Monitoring

SW2 switches the 5V supply voltage to the PVED-CLS AD3 input. AD3 is pulled to sensor ground if nothing is connected to the input. The PVED-CLS validates the input voltage on AD3. If the voltage is in the range 5V ±300mV, then SW2 is determined to be in off-road mode. If the voltage is below 500mV, then SW2 is determined to be on-road position. The PVED-CLS will enter safe state if the AD3 input voltage is outside the two voltage ranges for more than 100ms.

The SW1 signal (resistance) supplied to the PVED-CLS is range checked. If the measured resistance is in the undefined range (100-200 Ω) for more than 100ms, then the safe state is entered. The PVED-CLS will enter safe state if the current exceeds 2A. Short-circuits to ground are detected by the hardware.

Monitoring of the switch is performed by the PVED-CLS by comparing the range checked SW1 and SW2 inputs. If the SW1 and SW2 state differs for more than 100ms, the safe state is entered.

Important

- The monitoring technique is based on a comparison and uses a reference sensor. A diagnostic coverage in the range 90-99 % may be claimed provided that the sub-system is integrated according to the specification.
- Some faults cannot be detected before the road switch position is changed.

8.12 MAN-MACHINE INTERFACE (MMI) SSM_025

The MMI sub-system shall measure the systems or operators request for different steering modes and transmit the information to the PVED-CLS. The architecture shows how the PVED-CLS can be used as part of the Man Machine Interface (MMI) sub-system.

The basic architecture assumes two MMI messages, one destined for the main controller and one for the safety controller. Depending on the target system, two different sub-system architecture variants are possible:

- The steering mode request is measured redundantly by two separate sensor and ECUs.
- The steering mode request is measured by a single sensor and ECU.

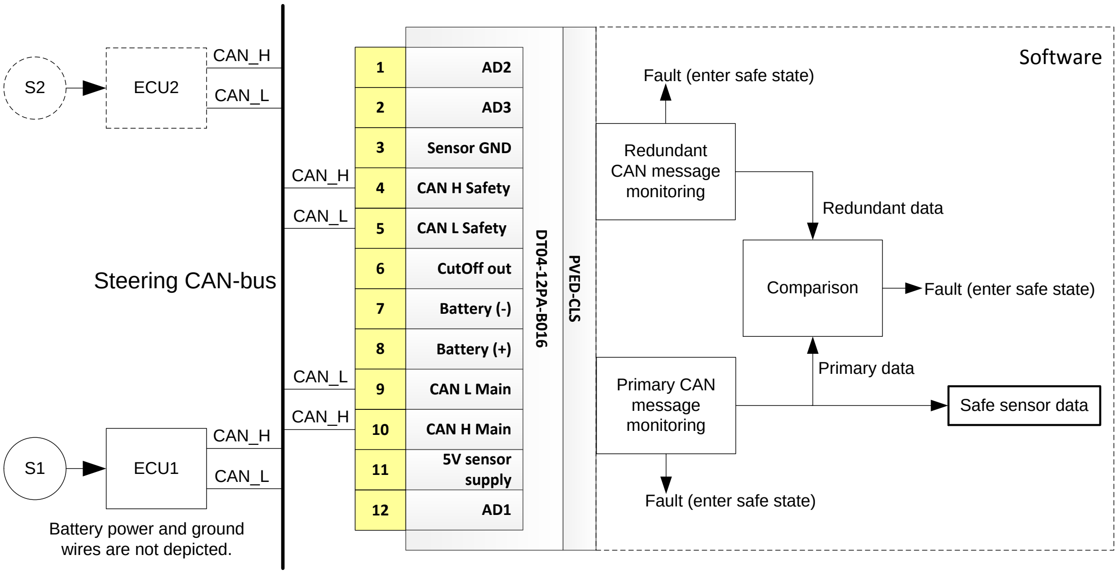


Figure 27: Man-Machine Interface architecture.

For implementing a sub-system which supports achieving an overall architecture category 3, primary MMI (S1, ECU1) and redundant MMI (S2, ECU2) are two channels which independently acquire the requested steering mode. ECU1 acquires the desired steering mode via sensor element S1. The desired steering mode is transmitted onto the CAN bus via a safe protocol as the primary MMI message. The same applied for the redundant MMI, where ECU2 transmits the redundant MMI message. See PVED-CLS communication protocol for details on the MMI message protocol.

The PVED-CLS provides a MMI program change lock-out functionality which can assist in excluding the MMI from becoming safety related functionality. By careful utilizing this method the MMI sub-system may be realized by a single MMI ECU (S1, ECU1) which senses the desired steering mode and outputs both MMI messages.

MMI program change lock-out

A safe vehicle speed range where MMI program changes are allowed can be configured. The PVED-CLS will lock the current steering program when the vehicle speed exceeds the speed threshold defined by parameter P3251. Any steering mode request will be ignored above the threshold.

Parameter	Description	Default value
P3251	Maximum vehicle speed for program changes [km/h].	15

Attention

⚠

The system integrator shall:

- Design and supply the vehicle speed sub-system.
- Ensure that the sub-system components are fit for the purpose.
- Conduct an FMEA to uncover dangerous failures.
- Implement measures against dangerous failures.

- Perform a CCF analysis.
- Document the sub-system as part of the safety case if it analyzed to be part of the safety function
- Ensure that a steering mode change will not lead to an unsafe situation.
- Do not use the MMI to change to on-road mode to achieve a steering mode suitable for on-road operation. The road switch shall be used for this purpose.

Important

The following must be considered for deciding if steering mode changes via the MMI CAN interface can be said to be not safety related:

- Any steering mode change may not result in a steering behavior difference i.e. change in steering wheel ratio which can lead to a hazard.
- Configure all steering wheel STW programs safely i.e. increasing steering ratio for increasing speed.
- Configure unused STW programs to maximum steering ratio at all vehicle speeds.
- Evaluate the behavioral effect of changing between STW programs with differently configured steering ratios.
- Configure P3251 to a vehicle speed where STW program behavior differences can be easily controlled by the operator.

8.12.1 CAN interface

The PVED-CLS main controller receives the primary MMI message and the PVED-CLS safety controller receives the redundant MMI message. See PVED-CLS communication protocol for details on the MMI message protocol.

Attention

⚠

- The applied safety protocol allows omitting the CAN bus from the safety loop calculation as it contributes less than 1% of the safety integrity level.
- The applied safety protocol allows the presence of both safety and non-safety related CAN messages.
- The sub-system shall begin transmitting CAN messages no later than 10 seconds after the PVED-CLS is powered.

8.12.2 Monitoring

The PVED-CLS provides monitoring functions for the MMI sub-system. For both primary and redundant message, the following monitoring is in place in both the PVED-CLS main and safety controller:

- Receive timing check of CAN messages. Nominal transmit rate is 500 ms. Time guard is fixed to 750 ms.
- Single receive timing failure leads to safe state.
- Sequence number check on CAN message. Single failure leads to safe state.
- End-to-end CRC on messages. Single failure leads to safe state.
- Data validity check (range check). Single failure leads to safe state.
- Primary and redundant steering mode requests are cross-checked as follows: If the absolute primary and redundant steering mode differ for more than P3374 ms, then enter safe state.
- See PVED-CLS User Manual for CAN bus diagnostic trouble codes related to detecting different failures on the vehicle speed sensor sub-system.

Parameter	Description	Default value
P3374	Channel cross-check monitoring. Maximum allowed time for which MMI steering mode requests are allowed to be different [x10ms]	10

Important

- Setting the value for P3374 too high will reduce the monitoring performance.
- If it is assessed that the MMI is part of the safety loop, then the monitoring technique for the category 3 architecture, is based on a comparison and uses a reference sensor. A diagnostic coverage in the range 90-99% may be claimed provided that the sub-system is integrated according to the specification.

8.13 BOOTLOADER VERSION CHECK SSM_066

At power-on the PVED-CLS checks that the application software has been downloaded to a target with the right bootloader. If the bootloader version is other than 3.85, the PVED-CLS enters safe state immediately.

9 Output sub-systems and Monitoring

9.1 CUT-OFF VALVE FOR OSPE, EHI-E AND EHI-H VALVE SUB-SYSTEMS SSM_026

The OSPE has an integrated cut-off valve (COV) which blocks the L and R steering flows to the steering cylinder. The COV is piloted by the COV solenoid valve which is opened by supplying power to the cut-off coil.

The COV spool has a dual function. In blocked state, it blocks L and R steering flow as well as hydraulic pilot pressure supply to the solenoid valve bridge (SVB).

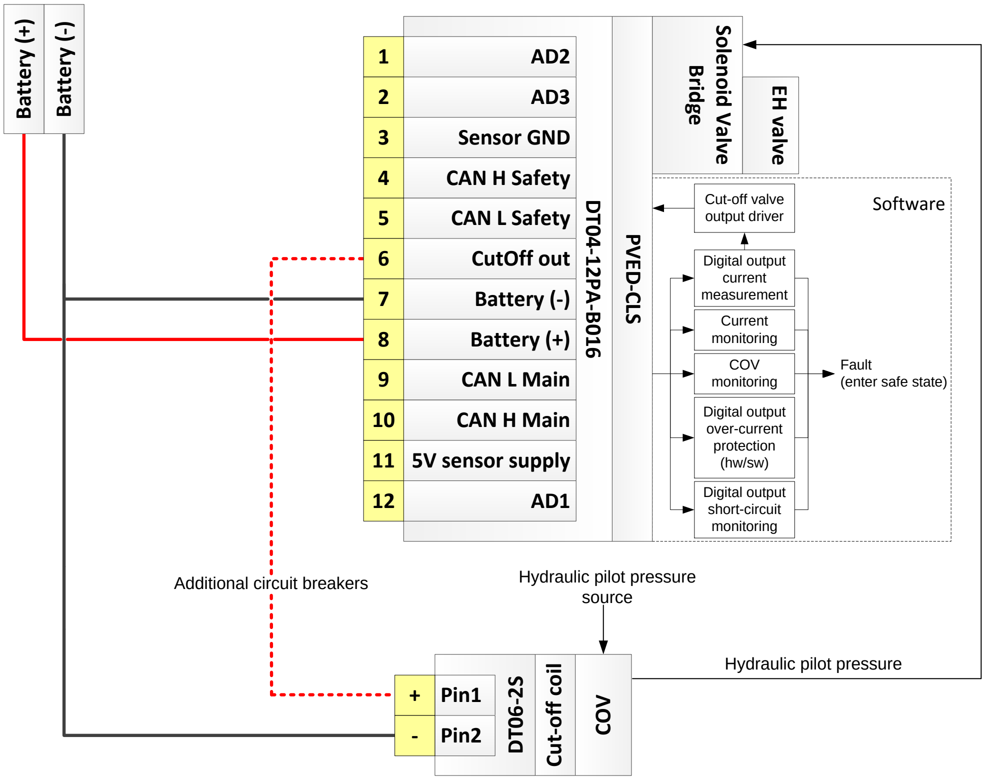


Figure 28: Cut-off valve architecture for OSPE, EHi-E and EHi-H valve sub-system.

9.1.1 Interface

The COV solenoid valve shall be connected to the monitored PVED-CLS high-side switch output (pin 6) and battery – (ground). It is recommended to establish the COV solenoid valve ground connection as close the PVED-CLS ground (pin 7) as possible to avoid voltage drops and current loops.

9.1.2 Configuration for OSPE and EHi-E valve sub-systems

Cut-off valve related configuration parameters and recommended values, for systems using an OSPE or EHi-E valve sub-systems can be seen below.

Parameter	Description	Value
P3072	Cut-off valve present. (0 = not present (EHPS), 225 = present (default)(OSPE, EHi-E and EHi-H)) Note: For OSPE, EHi-E and EHi-H valve sub-systems, P3072 shall be 255 to achieve the maximum safety integrity.	255
P3073	Cut-off valve control mode. (0 = Open loop current control, 255 = Closed loop current control (default))	255
P3074	Cut-off valve pull current (closed-loop current control).	1100 mA
P3076	Cut-off valve hold current (closed-loop current control).	500 mA
P3078	Cut-off valve monitoring POST time-out. The COV check will fail if started and not succeeded within the set time-out period. Note: Setting P3078 = 0 will disable COV monitoring.	900 ms
P3081	Valve type. (0 = OSPE or EHi-E (default), 1 = EHPS, 2 = EHi-H)	0
P3097	Cut-off solenoid valve PWM preload. The current build-up can be preloaded when the solenoid valve is powered, this speeds up the time it takes to pull the armature. P3097 = 100 % is recommended for OSPE, EHi-E and EHi-H valve sub-systems.	100 %

9.1.3 Monitoring for OSPE and EHi-E valve sub-systems

By utilizing the SVB and the EH-valve main spool position sensor, the following monitoring is achieved:

- Full-stroke testing of the COV.
- Full-stroke testing of the cut-off solenoid valve.

The test checks that the COV can enter blocked state. No EH-steering functionality is possible until the test has passed.

The COV solenoid valve and COV is tested every time the MMI commands the PVED-CLS from on-road mode into off-road mode. The monitoring function is designed to work in the full operational temperature range. The test will time out if it cannot complete within 10 seconds (high oil viscosity). Some examples of test execution times, using oil type Tellus 32, are:

- Oil temp -25 °C (6000 cSt) results in test duration: ~6.0 s
- Oil temp -20 °C (4500 cSt) results in test duration: ~3.1 s
- Oil temp -10 °C (1700 cSt) results in test duration: ~1.3 s
- Oil temp 0 °C (761 cSt) results in test duration: ~0.7 s
- Oil temp 20 °C (203 cSt) results in test duration: ~0.6 s
- Oil temp 40 °C (75 cSt) results in test duration: ~0.6 s

Important

- The monitoring technique is based on an intermittent test pulse principle.
- A diagnostic coverage in the range 90-99 % may be claimed, provided that the sub-system is integrated according to the specification.

9.1.4 Configuration for EHi-H valve sub-systems

Cut-off valve related configuration parameters and recommended values, for systems using an EHi-H valve sub-systems can be seen below.

Parameter	Description	Value
P3072	Cut-off valve present. (0 = not present (EHPS), 225 = present (default)(OSPE, EHi-E and EHi-H)) Note: For OSPE, EHi-E and EHi-H valve sub-systems, P3072 shall be 255 to achieve the maximum safety integrity.	255
P3073	Cut-off valve control mode. (0 = Open loop current control, 255 = Closed loop current control (default))	255
P3074	Cut-off valve pull current (closed-loop current control).	1100 mA
P3076	Cut-off valve hold current (closed-loop current control).	500 mA
P3078	Cut-off valve monitoring POST time-out. The COV check will fail if started and not succeeded within the set time-out period. Note: Setting P3078 = 0 will disable COV monitoring.	900 ms
P3081	Valve type. (0 = OSPE or EHi-E (default), 1 = EHPS, 2 = EHi-H)	2
P3097	Cut-off solenoid valve PWM preload. The current build-up can be preloaded when the solenoid valve is powered, this speeds up the time it takes to pull the armature. P3097 = 100 % is recommended for OSPE, EHi-E and EHi-H valve sub-systems.	100 %
P3098	Maximum rise time, i.e. time from switching the COV solenoid valve on until movement of the EH-valve main spool is observed. [x10msec]	30
P3099	Maximum fall time, i.e. time from switching the COV solenoid valve off until movement of the EH-valve main spool is observed. [x10msec]	20
P3100	Number of consecutive rise and fall times measured within limits to conclude the test as passed. (Must be concluded as passed once for both a positive and negative EH-valve main spool set-point)	2
P3101	If the EH-spool does not return to neutral, after switching the COV solenoid valve off, within this timeout, the cut-off solenoid is concluded to be stuck open. [x10msec]	100

9.1.5 Monitoring for EHi-H valve sub-systems

By utilizing the SVB and the EH-valve main spool position sensor, the following monitoring is achieved:

- Full-stroke testing of the COV.
- Full-stroke testing of the cut-off solenoid valve.

The test checks that the COV can enter blocked state. No EH-steering functionality is possible until the test has passed. The COV solenoid valve and COV is tested every time the MMI commands the PVED-CLS from on-road mode into off-road mode.

The monitoring function will set the EH-valve main spool set-point to a positive value inside the hydraulic deadband and alternately turn the COV solenoid valve on and off. Each time the COV solenoid valve is toggled, the time is measured from it is toggled until the EH-valve main spool has been observed moving. The measured time is then evaluated against the value of P3098 and P3099, for the rise time (COV solenoid turned on) and the fall time (COV solenoid turned off) respectively. Once the consecutive number of test passed, both rise times and fall times, is equal to the value of P3100, the test is evaluated as passed and it will be repeated with a negative EH-valve main spool set-point inside the hydraulic deadband. Once this test has passed as well, the PVED-CLS will be allowed to go into off-road mode.

Important

- If the fall time is observed longer than specified by P3101, the COV solenoid will be concluded as stuck open and the safe state will be entered.
- If the consecutive number of test passed never reaches the value specified by P3100, the test will continue endlessly, or until either the safe state is triggered as mentioned above or on-road mode is requested.
- There is no limit on how long the rise time can be.
- Turning the steering wheel during the test will extent the duration of the test, eventually to infinity.
- A diagnostic coverage in the range 90-99 % may be claimed provided that the sub-system is integrated according to the specification.

9.2 5V DC POWER SUPPLY SSM_028

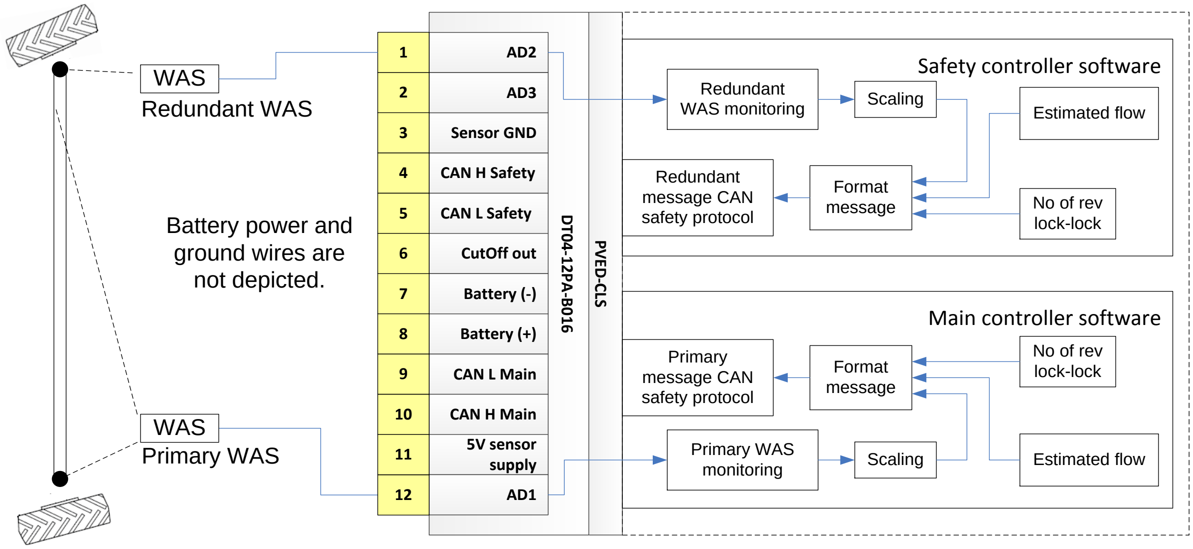
The PVED-CLS can supply external sensors with a regulated 5V supply voltage. The voltage is internally monitored by a range check. The PVED-CLS enters the safe state if the voltage exceeds the monitored sensor voltage thresholds.
A diagnostic coverage of 60 % can be claimed by the range check method. For a higher diagnostic coverage, use the 5V sensor supply for a two channel sensor with inverted characteristics and monitor the supply voltage indirectly by cross-checking the two sensor channels.
For more details refer to PVED-CLS Technical Specification.

9.3 STEERING STATUS CAN MESSAGE SSM_029

The PVED-CLS can be configured to output a steering CAN message with status information on:

- Estimated steered wheel angle (scaled to the internal resolution)
- Estimated EH-valve flow (scaled to internal resolution)
- Number of desired steering wheel revolution lock-to-lock

The steering status data may be used by other ECUs for various purposes.



9.3.1 CAN interface

A primary and redundant message is generated by the main and safety controller respectively. See PVED-CLS communication protocol for details on the MMI message protocol.

Attention

- The applied safety protocol allows omitting the CAN bus from the safety loop calculation as it contributes less than 1 % of the safety integrity level.
- The applied safety protocol allows the presence of both safety and non-safety related CAN messages.
- The sub-system shall begin transmitting CAN messages no later than 10 seconds after the PVED-CLS is powered.

9.4 EH-VALVE MAIN SPOOL MONITORING SSM_053

The PVED-CLS features an integrated EH-valve main spool position sensor (LVDT-sensor) which is used for 1) closed-loop EH-valve main spool positioning and for 2) EH-valve main spool monitoring.

9.4.1 EH-valve main spool control principle

The main controller calculates a EH-valve main spool set-point every 10ms. The set-point is input to the Solenoid Valve Bridge (SVB) which pilots the EH-valve main spool towards the calculated spool set-point. The actual EH-valve main spool position is measured via the LVDT sensor and fed back to the software for closed-loop spool position control. When the spool position control error is zero the EH-valve main spool is kept at the set-point.

9.4.2 EH-valve main spool monitoring – OSPE, EHi-E and EHi-H valve sub-systems

The principle of spool monitoring is depicted in Figure 29. The criterion for safe spool control is:

1. The EH-valve main spool shall be within the mechanical neutral position threshold (P3090) when the SVB is de-energized.
2. The spool is positioned at or less than the set-point (green dots) and
3. The spool is positioned no further than the |set-point + spool monitoring max threshold (P3377)|.
   The spool monitoring max threshold range are marked with orange arrows.

A spool monitoring fault is detected when the EH-valve main spool position is in the red enclosed region for more than 'Spool out of control' tolerance time equal to 150 ms (P3378). At power-up, the initial tolerance time is 1000 ms (P3379). The Spool out of control tolerance time is oil viscosity dependent and will decrease and settle at 150 ms as the spool dynamics reflects normal operation conditions. The tolerance time decline rate is determined by an initial tolerance time constant (P3381) and the observed spool dynamics measured over a 10 ms interval.

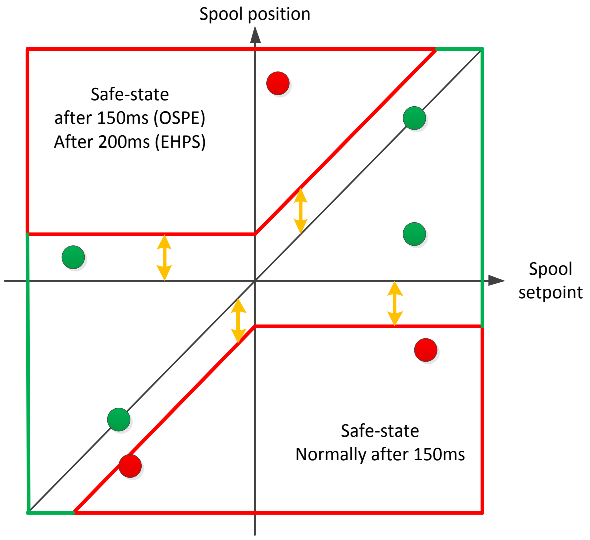


Figure 29 Spool monitoring

Parameter	Description	Recommended value
P3090	Absolute spool neutral position threshold. At power-up and when the SVB is de-energized the spool position shall be 0±0.25mm.	0.25 mm
P3377	Max difference between spool set-point and spool position	0.8 mm
P3378	Minimum 'spool out of control' tolerance time	150 ms
P3379	Initial 'spool out of control' tolerance time	1000 ms
P3381	'Spool out-of control' time constant. The effective tolerance time is in the range given by P3379 and P3378.	8000 ms

Attention

Do not modify the above parameters.
Contact Danfoss PAE for questions to the above parameters.

9.4.3 EHPS main spool monitoring - EHPS valve sub-system

Spool monitoring for steering systems using an EHPS valve is based on the same principle as for the OSPE valve but with compensation for the following known EHPS operation modes which will all lead to a spool out of control false alarms:

- The OSP-CX steering unit can hydraulically override the PVED-CLS SVB pilot flows and thus push the EHPS main spool away from the PVED-CLS spool set-point.
- Insufficient pump pressure situations causes the EHPS valve to switch into emergency steering mode and stroke the EHPS main spool to maximum deflection.
- Steering the steered wheels against the end-lock will stroke the EHPS main spool to maximum deflection.
- Resting/holding the steering wheel in auto-guidance mode may restrict the steering unit neutral springs to fully return the spool-sleeve set to neutral to relief the EHPS main spool chambers. This may result in a small OSP-CX generated pilot flow which pilots the EHPS main spool and thus hold/stroke the EHPS main spool position due to its higher steering priority/pressure. The PVED-CLS will detect a spool out of control failure when the EHPS main spool set-point is calculated to be at the opposite side as shown in Figure 29.

To handle the above EHPS valve specific features and to not generate false alarms, an additional spool movement check is added to work in parallel with spool monitoring for steering systems using the EHPS valve. Both the check in Figure 29 and Figure 30 shall indicate a failure to detect a spool-out-of-control failure.

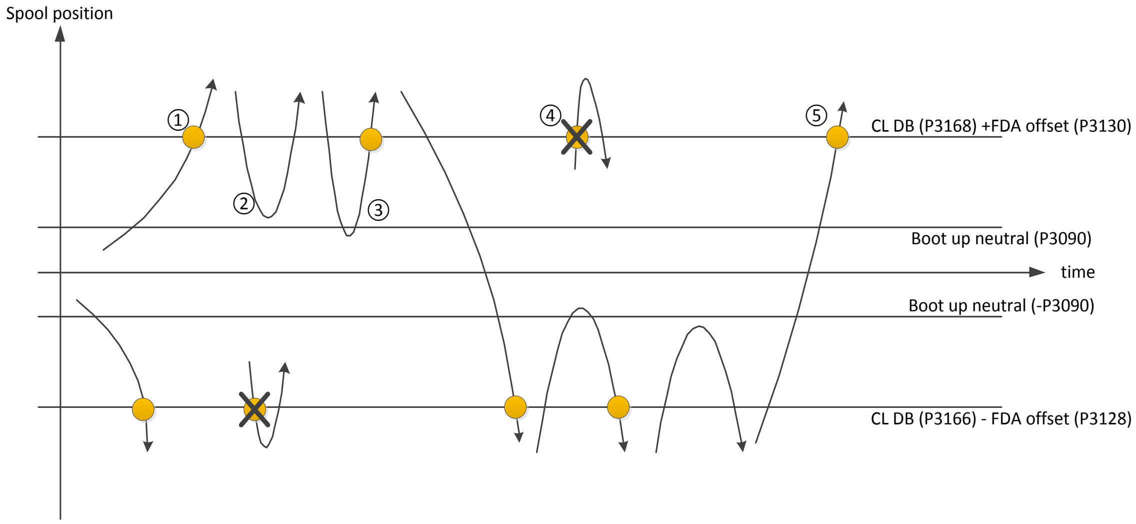


Figure 30 Spool movement check (EHPS)

The spool movement check at any point in time infers checking if the steering wheel activation in a ±100ms time-window is correlating with the spool movement.

Example

In Figure 30 the yellow dots show when the spool movement check is executed. In scenario ① it is checked if the steering wheel caused the spool to travel from mechanical neutral position threshold (P3090) and crossed the closed-loop deadband position (P3166/P3168) + FDA offset (P3128/P3130). If this is not the case and a spool-out-of-control failure is detected by spool monitoring, then the PVED-CLS enters safe state. ② does not trigger a spool movement check as the valve chambers have not been fully relieved as result of an ongoing steering activity to the same direction. ④ shows the example where spool movement check is started but suspended as the spool exhibits correct behavior within a 100ms window. Scenario ③ and ⑤ also triggers a spool movement check.

The combination of spool monitoring and spool movement check is executed for EHPS valve systems as a function of configuration, application mode, steering angle and vehicle speed as outlined in Figure 31 and explained in table

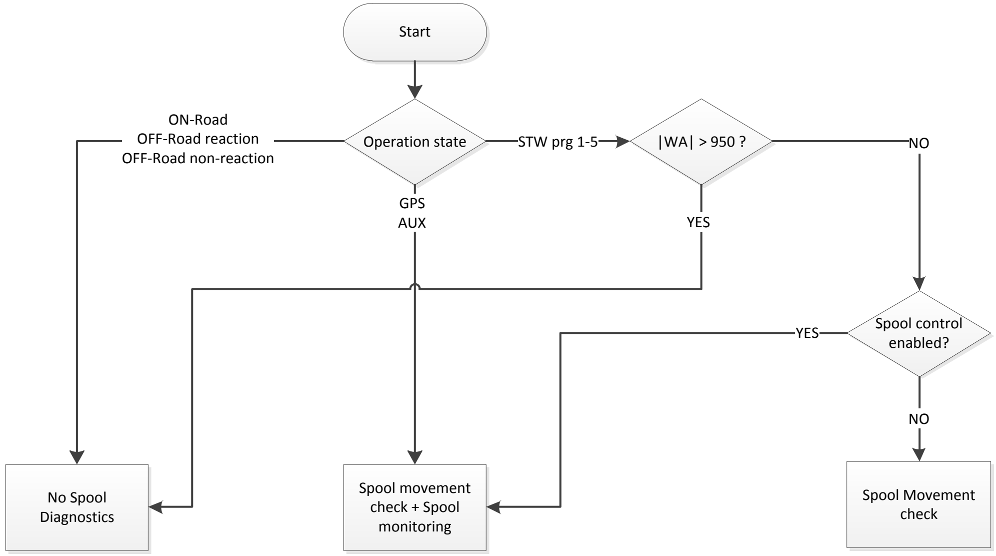


Figure 31: EHPS spool monitoring and spool movement check

Operation mode	Spool monitoring active	Spool movement check active	Residual false alarms sources
Auto-guidance	yes	Yes	
Auxiliary steering	yes	Yes	
On-road *or* Off-road reaction *or* Off-road non-reaction	No	No	
STW program 1-5, |WA|<950 IR	No	No	
STW program 1-5, |WA|<950 IR *and* Spool control enabled = true *and* Vehicle speed > FDA Vehicle Speed threshold (P3134)	Yes	yes	If system pressure is reached away from the end-stop region and the EHPS main spool moves without a detectable steering wheel movement
STW PRG 1-5, |WA| < 950 IR *and* Spool control enabled = false *and* Vehicle speed > FDA Vehicle speed threshold (P3134)	No	yes	If the EHPS main spool moves without detectable steering wheel movement
STW PRG 1-5, |WA| < 950 IR *and* Spool control enabled = true *and* Vehicle speed < FDA Vehicle speed threshold (P3134)	Yes	yes	If system pressure is reached away from the end-stop region and the EHPS main spool moves without a detectable steering wheel movement
STW PRG 1-5, |WA| < 950 IR *and* Spool control enabled = false *and* Vehicle speed < FDA Vehicle speed threshold (P3134)	No	yes	If the EHPS main spool moves without a detectable steering wheel movement

Table 4 EHPS main spool monitoring and spool movement check operation map

Note 1: Spool control enabled = true:
OSP-CX Flow command ≤ PVED-CLS Flow command AND PVED-CLS Flow command ≠0.

Note 2: Spool control enabled = false:
OSP-CX Flow command > PVED-CLS Flow command OR PVED-CLS Flow command = 0.

9.5 FAULT DETECTION ALGORITHM - FDA SSM_030

This section describes the Fault Detection Algorithm – FDA.

Attention

- In order for the Fault Detection Algorithm to work a steering wheel sensor and a wheel angle sensor must be present in the system. If either a steering wheel sensor or a wheel angle sensor is not present in the system, the Fault Detection Algorithm must be set to passive mode, i.e. P3132 shall be set to 0, otherwise the safe state will be triggered.
- As a SASA sensor cannot be used together with an EHi-H valve sub-system, the Fault Detection Algorithm is not applicable for the EHi-H valve sub-system, and must be set to passive mode, i.e. P3132 shall be set to 0. Therefore, a single channel wheel angle sensor is not suitable for an EHi-H valve sub-system, as FDA cannot be used for diagnostic.

9.5.1 FDA operation

The PVED-CLS is executing the Fault Detection Algorithm (FDA) in operation mode and in safe state. FDA monitors the system correlation between the wheel angle movement (direction), the steering wheel activation (direction) and the EH-valve main spool position (flow direction) and validates the inputs as outlined in FDA truth table.

The FDA parameters are highly vehicle design dependent and will vary from vehicle type to vehicle type. Tuning of the below parameters and field testing the configuration is essential for ensuring operation with no false alarms.

Parameter	Description	Recommended value
P3122	Steering wheel activation threshold required to detect a left or right steering motion. [dRPM]	50
P3123	Wheel angle difference indicating no steering, left or right steering. The difference is calculated as difference between current wheel angle and the wheel angle observed P3124·10ms ago. [IR]	50
P3124	Wheel angle history pointer. Selects a delayed wheel angle value for the wheel angle difference calculation. [x10ms]	1
P3125	Confidence time decrease rate. When the FDA detects correct system correlation, the fault confidence counter is decreased by P3125·10ms every control loop. This enables configuration of more forgiving fault confidence build-ups. [x10ms]	1
P3126	Confidence time increase rate. When the FDA detects incorrect system correlation, the confidence time is increased with P3126·10ms every control loop. [x10ms]	50
P3128	The threshold for defining steering to the left is defined by the spool exceeding the spool position given by: Left closed-loop deadband position (P3166) - FDA left spool position offset in (P3128). [10µm]	0
P3130	The threshold for defining steering to the right is defined by the spool exceeding the spool position given by: Right closed-loop deadband position (P3168) - FDA left spool position offset in (P3128). [10µm]	0
P3132	FDA active or passive mode. 0=Passive. FDA is operational but does not enter safe state if a fault is detected (tuning mode). FDA operation shall be observed via status message 5 (PVED-CLS communication protocol) 255=active. FDA is operational and enters safe state if a fault is detected.	255
P3134	Vehicle speed dependent FDA mute. If the measured vehicle speed < P3134 km/h, then the FDA is muted and the confidence counter is cleared. Use this parameter if	0

	case insufficient steering pump pressure is available at park or low-speed conditions.	
P3166	Left closed-loop deadband position. [10µm]	See PVED-CLS User Manual
P3168	Right closed-loop deadband position. [10µm]	See PVED-CLS User Manual

Attention

Contact Danfoss PAE for questions on how to tune the above parameters.

9.5.2 FDA truth table

The truth table outlines when FDA begins to count up or decrease the confidence in the existence of a system fault. In steering wheel mode the correlation of all three inputs is regarded. In auto-guidance mode, the steering wheel direction is 'neutral' and FDA regards only three columns in the table.

Spool position	Left	Left	Left	Neutral	Neutral	Neutral	Right	Right	Right
Steering wheel direction	Left	Neutral	Right	Left	Neutral	Right	Left	Neutral	Right
Wheel angle difference = Left	Yes	Yes	No	Yes	No	No	No	No	No
(WA difference = Neutral) and (Wheel angle < -975 [IR])	Yes	Yes	No	Yes	Yes	No	No	No	No
(WA difference = Neutral) and (|Wheel angle| <= 975 [IR])	No	No	No	No	Yes	No	No	No	No
(WA difference = Neutral) and (Wheel angle > 975 [IR])	No	No	No	No	Yes	Yes	No	Yes	Yes
Wheel angle difference = Right	No	No	No	No	No	Yes	No	Yes	Yes

9.5.3 FDA parameter tuning

The FDA parameters are highly vehicle design dependent and will vary from vehicle type to vehicle type. Tuning of the FDA parameters and field testing the configuration is essential for ensuring operation with no false alarms.
Refer to the PVED-CLS User Manual for a guideline on tuning.

Important

- Failing to configure the FDA algorithm correctly will lead to loss of diagnostic capability.
- In order to prevent the Fault Detection Algorithm from giving false errors due to high frequent wheel angle oscillations, the Fault Detection Algorithm will ignore wheel angle oscillations above 6.7Hz.

Attention

The system integrator shall:

- FDA tuning shall be followed by system validation by testing the diagnostic capability of the FDA configuration by vehicle fault insertion test method.

10 Hydraulic override for EHi-H valve sub-systems

The EHi-H valve sub-system is developed to address the aftermarket for auto-guidance systems. In many of these aftermarket applications, a steering wheel sensor, like the SASA sensor, is not mounted and will be difficult to install. Therefore, an alternative method for realizing auto-guidance disengage, by steering wheel activation, has been developed for the EHi-H valve sub-system.

The hydraulic override is not limited to disengage of auto-guidance, but can be used to disengage any EH-steering mode. The safety function for disengaging EH-steering using the EHi-H valve sub-sytem, is performed by two safety functions:

Hydraulic override SSM_067

1) Internal Monitored DisengageInternal Monitored Disengage SSM_068

The total risk reduction is achieved by both safety functions as explained in the figure below.

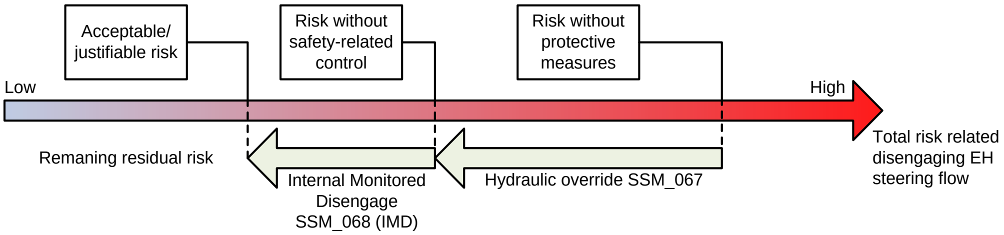

Acceptable/ justifiable risk
Risk without safety-related control
Risk without protective measures
Low
High
Total risk related disengaging EH steering flow
Remaning residual risk
Internal Monitored Disengage SSM_068 (IMD)
Hydraulic override SSM_067

Figure 32: Risk reduction strategy for hydraulic override for the EHi-H valve sub-system.

The safety function named

Hydraulic override SSM_067 performs the first risk reduction, only by including hydraulic parts of the valve sub-system, meaning that the PVED-CLS valve controller is not a part of this safety function. This safety function will not disengage EH-steering, but override it. The safety function

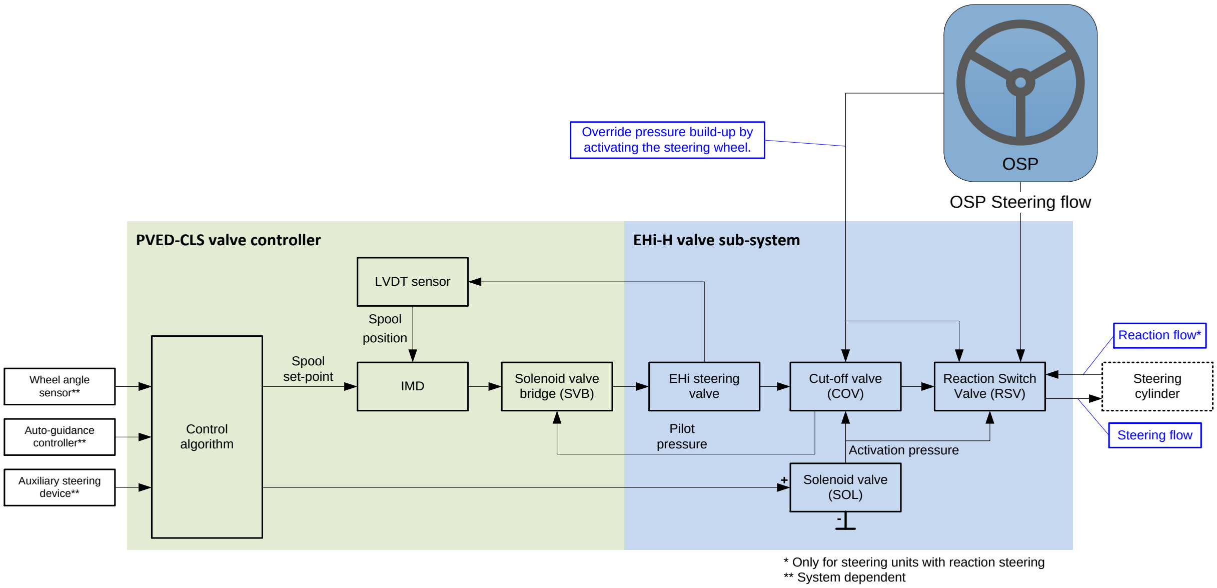
Internal Monitored DisengageInternal Monitored Disengage SSM_068 is performed by the PVED-CLS valve controller and will disengage the EH-steering, resulting in the last part of risk reduction.

Important
The above described technology is patented by Danfoss.

Attention ⚠	**Hydraulic override is only available in systems comprised by a PVED-CLS valve controller and EHi-H valve sub-system.**

10.1 HYDRAULIC OVERRIDE SSM_067

Hydraulic override is used to override the EH-steering mode and force the vehicle to be steered solely by the orbital steering unit, by braking the connection from the EHi steering valve to the steering cylinder. Overriding the EH-steering will also force the EHi steering valve to neutral, as the pilot pressure to the PVED-CLS valve controller is removed when the EH-steering is overridden.



* Only for steering units with reaction steering
** System dependent

Figure 33: High-level block diagram of hydraulic override.

In EH steering mode, the cut-off valve and reaction switch valve is pushed open and closed respectively by the pilot pressure from the solenoid valve. Therefore PVED-CLS valve controller is able to control the steering flow, via the EHi steering valve, based on input from the connected sensors and steering devices. As the RSV is in the closed position the flow from the EHi steering valve will not make the steering wheel turn, even if the orbital steering unit is a reaction type.

When the operator activates the steering wheel, the orbital steering unit builds up an override pressure, which works on the same side as the neutral springs on the RSV and COV. When the combined spring force and override pressure exceeds the pilot pressure, the RSV valve is pushed into its open position and the COV is into its closed position.

As the COV now is in its closed position, the EH-steering flow is blocked and with the RSV in its open position the steering flow from the orbital steering unit has access to the steering cylinder. Therefore, the vehicle is steered solely by the orbital steering unit. Furthermore, the EHi steering valve will fall to neutral, as its pilot pressure connection has been broken by the forced closed COV.

Important

This above described state is true as long as the steering wheel is activated. When steering wheel activation is stopped, operation will revert to EH-steering mode. Disengage of EH-steering mode will be done by the safety function called

Internal Monitored DisengageInternal Monitored Disengage SSM_068, see section 0.

10.2 INTERNAL MONITORED DISENGAGEINTERNAL MONITORED DISENGAGE SSM_068

As described in Hydraulic override SSM_067, the hydraulic override will force the EHi steering valve to neutral by removing the pilot pressure to the SVB of the PVED-CLS valve controller. This means that the EHi steering valve cannot be moved away from neutral position.

When the EH-valve main spool has been found within mechanical neutral for longer that specified by P3587, the internal monitored disengage will set the EH-valve main spool set-point away from neutral, but still inside the deadband of the EHi-H valve sub-system. If the EH-valve main spool still is found in neutral after P3586, from first time observed in within mechanical neutral, the IMD will evaluate that the steering wheel as active and the EH-steering mode will be disengaged.

If the EH-valve main spool is found outside mechanical neutral, within P3586 from first time observed in within mechanical neutral, the IMD will evaluate that the steering wheel as inactive and the EH-steering mode will be not disengaged.

The IMD steering wheel status, from main and safety controller, is cross-checked. If the IMD steering wheel status is different, for longer than specified by the sum of P3395 and P3586, the PVED-CLS will enter safe state.

Parameter	Description	Default value
P3587	Limit for how long time the EH-valve main spool may be within mechanical neutral before IMD set the EH-valve main spool set-point away from neutral [x10ms].	15
P3586	Limit for how long time the EH-valve main spool may be within mechanical neutral before IMD disengages the EH-steering mode [x10ms].	30
P3395	Limit for how long time the IMD steering wheel status of main and safety controller, may be different, before the PVED-CLS enters safe state [x10ms].	10

Attention ⚠	**Do not modify the above parameters.** **Contact Danfoss PAE for questions to the above parameters.**

Important

The auto-guidance controller shall warn the driver by an audible indicator per ISO 10975 Tractors and machinery for agriculture and auto-guidance systems for operator-controlled tractors and self-propelled machines - Safety requirements for auto-guidance systems.

10.2.1 Configuration of Hydraulic Override and Internal Monitored Disengage

Hydraulic override and internal monitored disengage can only be used in systems comprised by a PVED-CLS valve controller and EHi-H valve sub-system. Furthermore, a SASA sensor cannot be present in the system when using hydraulic override and internal monitored disengage, meaning that the disengage method shall be configured to be Internal Monitored Disengage. See the table below.

Parameter	Description	Main controller	Safety controller
P3254	EH-steering disengage method. (0 = SASA (default), 255 = Internal monitored disengage)	255	255

10.2.2 Performance parameters for Internal Monitored Disengage algorithm

During the development of the Internal Monitored Disengage algorithm the parameters P3588 and P3589, listed in the table below, was introduced to optimize the performance of the Internal Monitored Disengage algorithm. The value of these parameters has been validated by test, to secure optimal performance of the Internal Monitored Disengage algorithm, and shall not be altered.

Parameter	Description	Default value
P3588	Dynamic SVC integral limit to use while EH-valve spool is close to neutral.	10
P3589	Dynamic SVC integral gain to use while EH-valve spool is close to neutral.	225

Attention ⚠	**Do not modify the above parameters.** **Contact Danfoss PAE for questions to the above parameters.**

10.3 SAFETY RELATED SPECIFICATIONS

This section handles the safety related specifications for the two safety functions of the hydraulic override.

10.3.1 Hydraulic overide

The safety function

Hydraulic override SSM_067 is comprised by the OSP, COV and RSV. The safety-related block diagram for this safety function can be seen in the figure below.

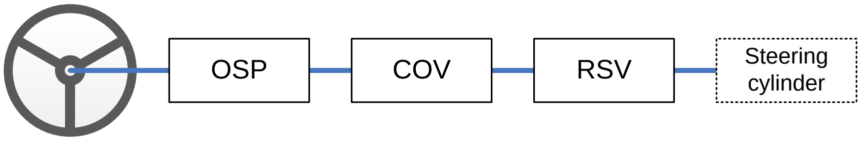


Figure 34: Safety-related block diagram for hydraulic override for the EHi-H valve sub-system.

Fault exclusion applies to all components in the safety-related block diagram, OSP, COV and RSV, as the operator builds up an internal hydraulic override pressure, up to system pressure level, forcing the COV to closed position and RSV to opened position.

10.3.2 Internal Monitored Disengage

The safety-related block diagram for the safety function

Internal Monitored DisengageInternal Monitored Disengage SSM_068 can be found in the figure below.

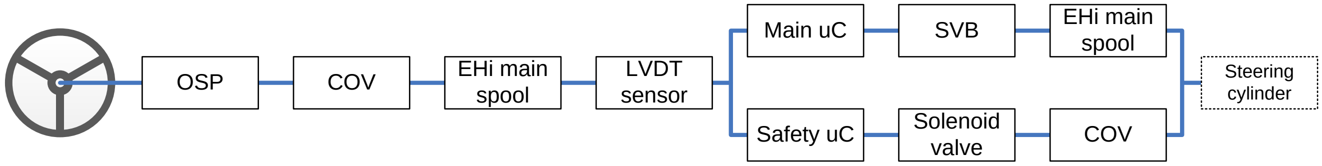


Figure 35: Safety-related block diagram for Internal Monitored Disengage for the EHi-H valve sub-system.

- Fault exclusion applies to following components in the safety-related block diagram; OSP, COV and EHi main spool.
- Following components are comprised by the PVED-CLS; LVDT sensor, Main uC, Safety uC and SVB and Solenoid valve.
- The MTTFd,ch for the entire channel must be better than 10 years (medium) for a category 3 architecture.
- The DCavg must be ≥ 90% (for ISO25119 DCavg must be ≥ 60%).
- The CAN bus takes less than 1% of SIL2 due to the applied safety protocol and is thus omitted for all sensors.

Sub-system monitoring	**DC**	**Description**
PVED-CLS	95 %	Resulting DC per PVED-CLS FMEDA. Lowest number is applied for both channels.
OSP	NA	Designed to fault exclusion.
COV	NA	Designed to fault exclusion.
EHi main spool	NA	Designed to fault exclusion.

The PVED-CLS safety related specifications are described in section 4.1.

Channel 1,2 elements	**MTTFd [years]**	**DC [%]**
PVED-CLS	36	95
OSP	-	-
COV	-	-
EHi main spool	-	-
MTTFd,ch	**36**	
DCavg		**95**

Refer to ISO 13849 for calculation of MTTFd,ch and DCavg.

The MTTFd,ch and the DCavg fulfills the requirement for meeting AgPL d with a category 3 architecture.

11 Safe EH steering shut-off SSM_055

The Safe EH steering shut-off safety function will bring the PVED-CLS and valve sub-system into the safe state on demand or at fail-to-function by de-energizing the valve outputs.
See section 4.4 for further information on the safe state.

The following can trigger the safety function:

- The embedded safety functions.
- Internal monitoring functions for the hardware and software.
- Monitoring functions for the sensor sub-systems.
- Monitoring functions for the valve sub-systems.

The following EH-steering safety architectures for are possible:

- Category 3 architecture: PVED-CLS together with OSPE, EHi-E and EHi-H valve sub-system with external Cut-Off Valve (COV).
- Category 2 architecture: PVED-CLS together with EHPS valve sub-system.

Operation
The PVED-CLS is designed to monitor the operation of the PVED-CLS hardware, software, valve sub-systems as well as interfacing sensor sub-systems. If the monitoring functions detect a fault which reduces the safety integrity level or leads to loss of the safety function, the safe state is demanded.
The PVED-CLS includes two channels. Both will enter the safe state.
The safety related specifications for this safety function including the valve sub-systems are described in section 4.1.

12 Vehicle speed EH steering shut-off SSM_056

The vehicle speed EH steering shut-off safety function will put the PVED-CLS into safe state if a defined vehicle speed threshold is exceeded. This safety function is active in any off-road steering mode. When properly configured the vehicle speed EH steering shut-off will only allow off-road steering functionality below a vehicle speed threshold

Operation

The system enters safe state at the speed defined in parameter P3253 km/h. Below this speed, EH-steering functionality can be used such as variable steering and auto-guidance. If variable steering is in use and the vehicle speed exceeds the speed threshold, the steering ratio will drop to steering ratio lock to lock determined by the OSP displacement.
If the safe vehicle speed threshold is exceeded in auto-guidance mode, the steering flow will be 0 (safe state) and the operator must take over control by using the steering wheel.

Parameter	Description	Recommended value
P3253	The vehicle speed at which the PVED-CLS shall enter the safe state	OEM decision

The factory default value is 25 km/h.

Important

- P3253 shall be set to the maximum vehicle speed which is assessed safe for off-road steering functionality.
- If the PVED-CLS enters safe state. The operator must operate vehicle with the steering wheel.
- The steering wheel ratio lock-to-lock will increase immediately when safe state is achieved. The step depends on the configured EH-steering ratio. The system integrator shall evaluate if this change can lead to a hazard.
- Give audible and visible alarm to operator when any steering mode is suspended due to vehicle speed EH steering shut-off/enter safe state.

Recommendation

- Consider using other means to limiting vehicle speed when using off-road steering functionalities.
- Reduce the immediate change in steering ratio when safe state is achieved as much as possible by gradually approaching the steering ratio ensured by the OSP displacement as a function of vehicle speed.
- Give audible alarm to operator when auto-guidance mode is suspended due to vehicle speed EH steering shut-off.

External reference: ISO 10975 Tractors and machinery for agriculture and auto-guidance systems for operator-controlled tractors and self-propelled machines - Safety requirements for auto-guidance systems.

12.1 SAFETY RELATED SPECIFICATIONS

For reliability calculation, the following safety related block diagram can be used. Only relevant sensors are included.

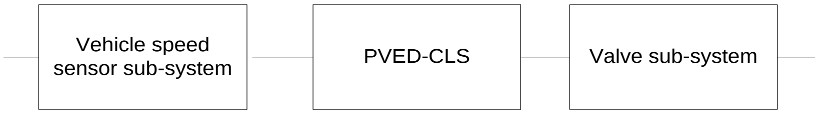


Figure 36: Safety related block diagram.

Note that if an EHPS valve sub-system is applied, then the PVED-CLS has only a single channel for shutting of EH-steering flows. The overall architecture category is thus limited to category 2.

Sub-system	MTTFd	DC	Category	CCF
Vehicle speed sub-system	Sensor sub-system specific See section 8.8			
PVED-CLS	36 years	95 %	3	>65 %
OSPE valve sub-system			3	
EHPS valve sub-system			2	

The PVED-CLS safety related specifications are described in section 4.1.

Example

Meeting safety target PL d/AgPL d per ISO 13849/ISO 25119. An OSPE valve sub-system is used.

- The MTTFd for the safety loop shall be in the range 10-30 years.
- The DC for the safety loop shall be in the range 60-90 %.
- All sub-systems shall conform to category 3 requirements.
- A CCF analysis shall be performed.

Calculation

Important

Any other safety function which must meet PL d/AgPL d and which uses more sensor sub-systems must be analyzed first as these safety functions put more strict requirements on each sub-system.

MTTFd

If no other sensor sub-system is in any other safety function, the below calculation is valid.

$$\frac{1}{MTTFd, ch} = \frac{1}{MTTFd, vehicle\ speed\ sensor} + \frac{1}{MTTFd,\ pvedcls\ and\ valves}$$

For the MTTFd for the entire channel to be better than 10 years, the MTTFd for each sub-system shall be better than 14 years.

Diagnostic Coverage

The diagnostic coverage for the vehicle speed sensor sub-system shall be ≥ 60 % (ISO 25119) and ≥ 90 % (ISO 13849). The vehicle speed sensor sub-system uses the dedicated monitoring in the PVED-CLS. The inputs are cross monitored. A diagnostic coverage in the high range (90-99 %) can be claimed by the provided monitoring functions.

$$DCavg = \frac{\dfrac{DCspeedsensor}{MTTFd, speedsensor} + \dfrac{DCpvedcls}{MTTFd,\ pvedcls\ and\ valves}}{\dfrac{1}{MTTFd, speedsensor} + \dfrac{1}{MTTFd,\ pvedcls\ and\ valves}}$$

- DCavg = 96% when DCspeedsensor is set to 99%.
- The PFH calculations are based on FMEDA calculations according to IEC 61508.
- The calculations are valid for off-road application. All safety functions and related hardware are included.
- No other sensor sub-systems are included in the calculation.
- The CAN bus takes less than 1 % of SIL2 due to the applied safety protocol and is thus omitted for all sensors.

13 Safe EH steering SSM_027

The PVED-CLS safety function, Safe EH steering, is comprised by a set of safety related control functions
The available safety related control functions can be found in section 5.
The safety related specifications for Safe EH steering flow is described in section 4.1.

13.1 SAFE EH-STEERING FLOW COMMAND SSM_057

The safety related control function, Safe EH-steering flow command, calculates a safe EH-valve main spool/EHPS main spool set-point every 10ms as a function of:

- The selected steering mode
- The selected steering device
- The selected steering program
- The vehicle speed
- The wheel angle

The main and safety controller exchange and cross-checks sensor inputs, operation states and the calculated flow command. The main controller is responsible for positioning the EH-valve main spool/EHPS main spool. Both controllers measure the valve main spool position and monitor if the EH-valve main spool/EHPS main spool is positioned according to the EH-valve main spool/EHPS main spool set-point.
If a divergence in any of the input, intermediate or outputs are detected, the safe state is demanded.
The safe EH-steering flow safety function is only available when the PVED-CLS is in normal operation mode.

13.2 MMI STEERING PROGRAM CHANGE LOCK-OUT SSM_058

The safety related control function, MMI program change lock-out, evaluates if a steering program change request from the MMI for both the steering wheel and auxiliary steering device is allowed to take effect. The PVED-CLS will lock the current steering program if the vehicle speed exceeds the parameterized vehicle speed threshold in P3251.
Steering program change requests are ignored while the vehicle speed has above P3251 km/h.

Parameter	Description	Recommended value
P3251	Maximum vehicle speed at which steering program changes are allowed [km/h].	15

The MMI program change lock-out safety related control function may be useful for configurations where the steering programs are significantly different and not safe at all vehicle speeds.

Important

- The system integrator must determine the maximum vehicle speed at which steering program changes are safe.
- The system integrator must analyze if any program change at any speed may lead to a hazard.
- The safety related control function can be used for reducing or avoiding hazards caused by the MMI.
- The lock-out status flags for steering wheel program changes in the Operation Status Message signals if program changes are executed or ignored.
  Observe the current state in the Operation Status Message for evaluating if a MMI steering program change request was executed or ignored.
  See PVED-CLS communication protocol for information on Operation Status Message.

Recommendation

- Configuring all steering programs to be safe in the entire off-road vehicle speed range may make the MMI program change lock-out safety related control function unnecessary. In this case, P3251 can be set equal to P3253 for bypassing the safety related control function.
- For every vehicle speed dependent steering program the steering ratio characteristic giving increasing steering ratio for increasing vehicle speed.
- If a steering program is configured not to be vehicle speed dependent, it must be ensured that the configuration allows safe driving at all possible vehicle speeds.
- Unused steering programs shall be programmed with default values.

13.3 STEERING DEVICE CHANGE LOCK-OUT SSM_059

The safety related control function evaluates if a request to engage auto-guidance mode or the auxiliary steering device can be executed or ignored. The safety related control function is designed to avoid hazards caused by unintended commands from the auto-guidance controller and the auxiliary steering device.

Operation

The PVED-CLS evaluates the incoming steering requests from Guidance Machine Commands and auxiliary steering device. If a request for steering is received and the steering wheel is not in use, the request is granted if the vehicle speed is equal to or below the speed threshold defined in parameter P3250.

A steering request is not memorized. The steering mode will not change to auto-guidance or auxiliary steering before the vehicle speed is below or equal to P3250 and a new auto-guidance engage request is received.

Parameter	Description	Default value
P3250	Safe vehicle speed to allow change of steering device [km/h].	15

Important

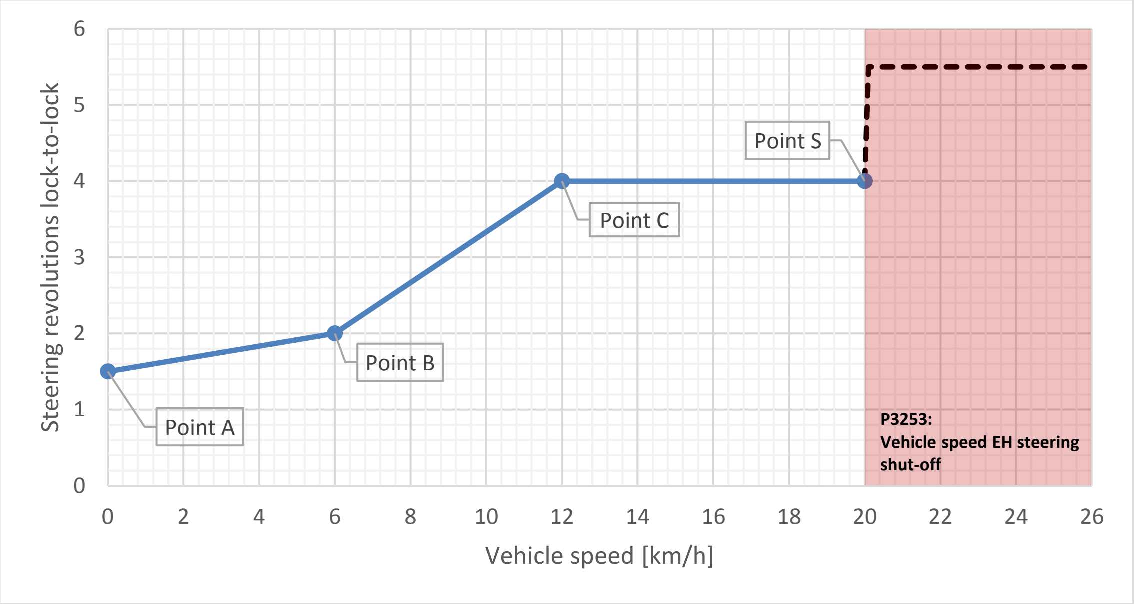
- The system integrator must determine the maximum vehicle speed at which changing to auto-guidance and auxiliary steering device is safe.
- The safety related control function can be used for reducing or avoiding hazards caused by the auto-guidance controller or auxiliary steering device.
- The Operation Status Message lock-out status flags for steering device changes, signals if the auto-guidance controller commands or auxiliary steering requests will be executed or ignored.
  See PVED-CLS communication protocol for information on Operation Status Message.

Recommendation

- Auto-guidance controllers may have similar functionality which should be regarded when setting P3250.

13.4 VEHICLE SPEED DEPENDENT FLOW LIMITATION - STEERING WHEEL MODE SSM_060

The safety related control function, Vehicle speed dependent flow limitation, can amplify the EH steering flow as a function of the vehicle speed. The safety related control function is available for each of the 5 STW programs in normal operation mode.



Operation

The PVED-CLS has 5 different steering wheel programs, where the system integrator can configure the wanted number of steering wheel revolutions lock-to-lock at a given vehicle speed to achieve "Fast steering" or "Variable steering ratio". The steering ratio for each steering wheel program (STW1 to 5) is configured by operation point A, B and C. The steering wheel control algorithm will make linear interpolation in between each of the three points.

Note that point S is defined by vehicle speed EH steering shut-off safety function. At vehicle speed P3253 the PVED-CLS enter safe state and the steering revolution lock-to-lock will be given by the OSP displacement. The OSP displacement will always define the highest possible steering ratio.

Parameter	Description	Default value
P3522, P3530, P3538,P3546, P3554	Number of steering wheel revolutions lock-to-lock for: Point A for STW1, 2, 3, 4 and 5 respectively. [x0.01]	800
P3524, P3532, P3540, P3548, P3556	Number of steering wheel revolutions lock-to-lock for: Point B for STW1, 2, 3, 4 and 5 respectively. [x0.01]	800
P3526, P3534, P3542, P3550, P3558	Number of steering wheel revolutions lock-to-lock for: Point C for STW1, 2, 3, 4 and 5 respectively. [x100]	800
P3528, P3536, P3544, P3552, P3560	Vehicle speed for point B for STW1, 2, 3, 4 and 5 respectively. [km/h]	5
P3529, P3537, P3545, P3553, P3561	Vehicle speed for point C for STW1, 2, 3, 4 and 5 respectively. [km/h]	10

Configuring all steering wheel programs to be safe may reduce the criticality of the MMI sub-system.

Important

- The system integrator shall address and analyze all parameters.
- There is no restriction on the values of Point A, B and C.
- Point A is always specified at Vehicle speed = 0 km/h
- Point C "No of turns" is valid for Point C "Vehicle speed" and vehicle speeds above Point C "Vehicle speed"
- Point A "No of turns" ≤ Point B "No of turns" ≤ Point C "No of turns"
- Point C "Vehicle speed" > Point B "Vehicle speed" > Point A "Vehicle speed" (0 km/h).
- Unused STW programs shall be set to the default values for bypassing flow amplification.
- The system integrator must validate that all steering programs are safe.
- The system integrator must validate that program changes are safe.

Attention ⚠	**A too low steering revolution at too high speeds may lead to instability or loss of vehicle control. Configure the steering wheel programs according to the recommendations.**

13.5 AUTO-GUIDANCE AND AUXILIARY STEERING DISENGAGE BY STEERING WHEEL ACTIVATION SSM_032

The safety related control function disengages auto-steering mode or auxiliary steering mode when the steering wheel is operated and switches to the selected steering program.

Operation

Two criteria shall be fulfilled before the decision is taken to disengage auto-guidance:

1. The steering wheel speed must be above a defined rpm threshold (P3583)
2. The steering wheel angle change must exceed a defined angle range (P3584).

As long as the steering wheel speed is below P3583 rpm, the measured steering wheel angle change is set to 0. Once the steering wheel speed exceeds P3583, the steering angle change is measured and compared to the range defined by P3584. Auto-guidance control is disengaged when both criteria are fulfilled.

Parameter	Description	Recommended value
P3583	Steering wheel "in use" speed threshold [dRPM]	5
P3584	Steering wheel "in use" angle change threshold [degrees]	10

Important

- The system integrator must determine the steering wheel speed and position disengage criteria.
- Setting P3583 and P3584 too low may cause unintended auto-guidance or AUX steering device disengage by e.g. machine vibrations.
- Setting P3583 and P3584 too high may trigger the FDA and result in a trip to the safe state.
- The disengage criteria can be made dependent on steering wheel speed only by setting P3584 to 0.

External reference: ISO 10975 Tractors and machinery for agriculture and auto-guidance systems for operator-controlled tractors and self-propelled machines - Safety requirements for auto-guidance systems.

Attention ⚠	**Unintended and rapidly repeated engaging of auto-guidance control may lead to loss of steering controllability. The scenario is as follows; for each unintended start of auto-guidance the driver must consequently counter-steer to disengage auto-guidance mode.**

13.6 AUTO-GUIDANCE DISENGAGE AT LOW SPEED/PARKING SSM_033

The safety related control function, Auto-guidance disengage at low speed/parking, de-energizes the solenoid valve bridge if the vehicle speed is very low or indicates that the vehicle is parked.

Operation

When the PVED-CLS is in auto-guidance mode, the software can be configured to de-energize the solenoid valve bridge controlling the EH-valve main spool when the vehicle speed is below a configurable threshold set in parameter P3252.

In auto-guidance mode, the software positions the steering cylinder according to the curvature command set-point from the auto-guidance controller.

An unintended curvature command set-point at low vehicle speeds may result in a large and fast change of the steered wheel angle or articulation angle. The PVED-CLS cannot detect if the curvature command change was intended or not. To reduce the risks which may be associated by unintended curvature commands at vehicle standstill, the vehicle speed is used for determining to switch off power to the solenoid valve bridge. By this method, the auto-guidance steering mode is safe at vehicle speeds where it is likely that bystanders may approach the vehicle.

Parameter	Description	Recommended value
P3252	Minimum vehicle speed for auto-guidance with and solenoid valve bridge energized. The unit is x10 meters per hour.	50

Important

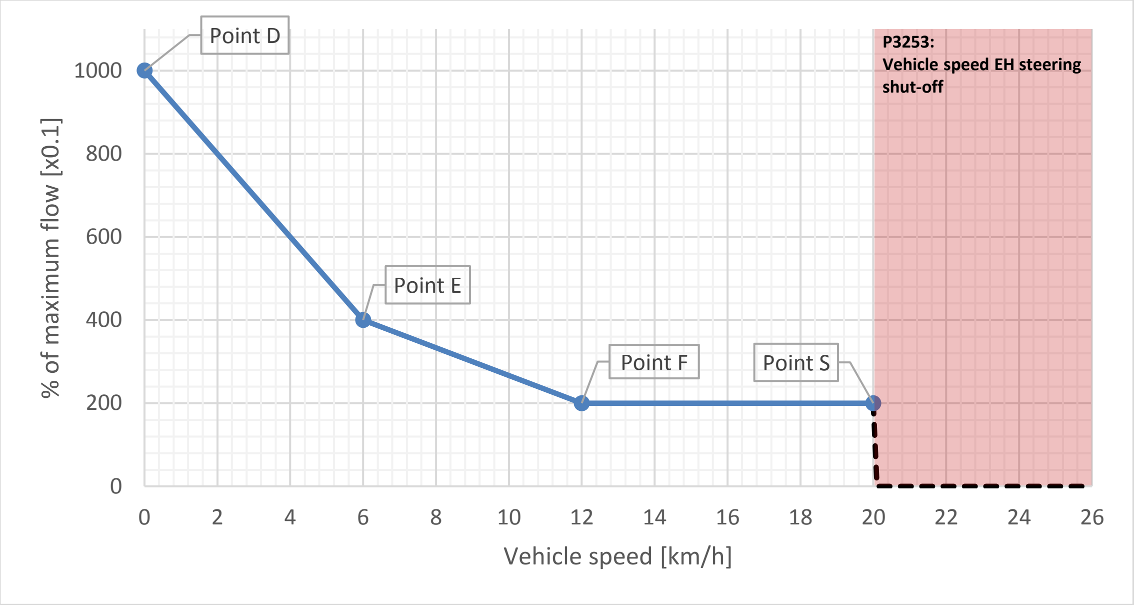
- The system integrator must determine and validate the value of P3252.
- Auto-guidance controllers may emulate similar functionality by freezing the curvature command and in this way "lock" the system. In such cases, P3252 may be set to the same vehicle speed threshold where the curvature command is frozen.
- If the auto-guidance controller is configured to disengage at a certain lower speed threshold, then P3252 shall be set equal to or a little lower to avoid conflicting with the auto-guidance control strategy.
- Note that when the vehicle speed is lower than P3352, then the auto-guidance controller is not able to correct the vehicles path.

Recommendation

P3252 should be set to a non-zero value to ensure that the solenoid valve bridge is always disabled in auto-guidance mode when the vehicle is parked.

13.7 VEHICLE SPEED DEPENDENT FLOW LIMITATION - AUTO-GUIDANCE MODE SSM_034

The safety related control function, Vehicle speed dependent flow limitation, limits the EH steering flow proportional to the vehicle speed when the PVED-CLS is operating in auto-guidance steering mode.



Operation

By configuring the safe maximum EH steering flow characteristic proportional to the vehicle speed, a safe rate of steering changes can be achieved for all vehicle speeds. At low speeds, high steering flows are allowed for quickly acquiring the path. At higher speed, lower steering flows are used for path corrections.
The characteristic is configured by operation point D, E and F which can be freely defined.
The auto-guidance control algorithm will make a linear interpolation in between each of the three points.

Note that point S is defined by vehicle speed EH steering shut-off safety function. At vehicle speed P3253 the PVED-CLS enter safe state. The operator must use the steering wheel. The steering revolution lock-to-lock will be given by the OSP displacement. The OSP displacement will always define the highest possible steering ratio.

The vehicle speed dependent maximum flow shall be configured as follows.

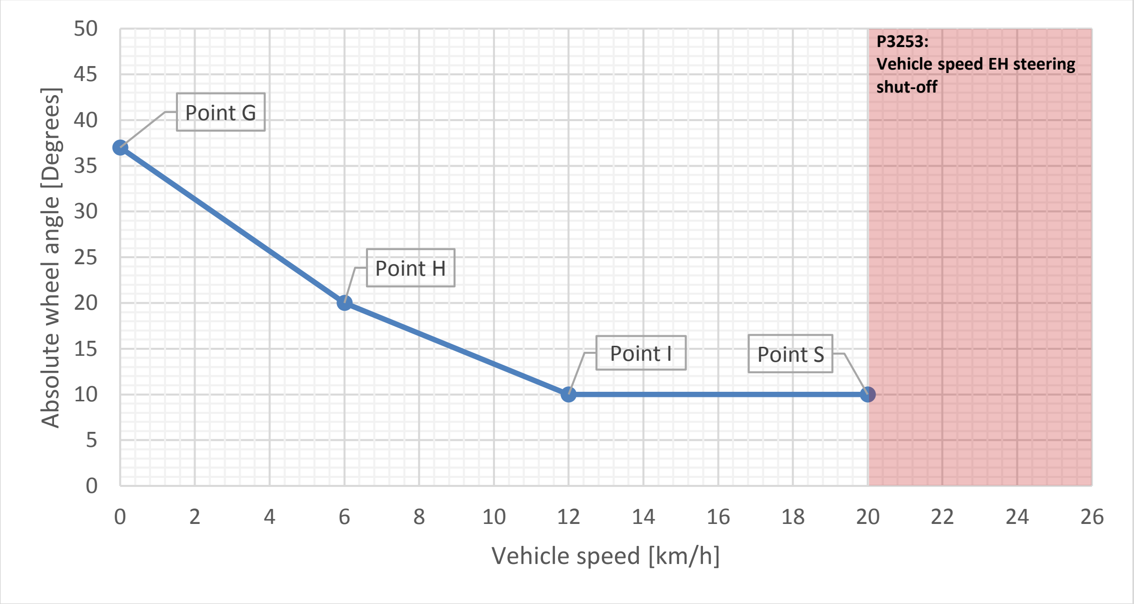
Parameter	Description	Recommended value
P3451	The maximum flow at point D (0 km/h)	OEM decision
P3453	The vehicle speed at point E	OEM decision
P3455	The maximum flow at point E	OEM decision
P3457	The vehicle speed at point F	OEM decision
P3459	The maximum flow at point F	OEM decision

Important

- Point D: Set P3451 to a high value to enable fast steering response at low speeds. For experimentation, start with 1000 (100 %).
- Point F: Set P3459 to a low value which gives the fastest rate of steering change that is deemed safe at fastest vehicle speed which is allowed in auto-guidance mode. For experimentation, start with 100 (10 %) at 20 km/h.
- Point E: Set P3453 and P3455 in between point D and E. Set P3455 to a value which is equal to the fastest steering change that is deemed safe at P3453 km/h.
- Parameter values must conform to: (0 < P3453 < P3457) and (P3451 > P3455 > P3459).
- The system integrator must validate the configured characteristic.

13.8 VEHICLE SPEED DEPENDENT WHEEL ANGLE LIMITATION - AUTO-GUIDANCE MODE SSM_035

The safety related control function, Vehicle speed dependent wheel angle limitation, limits the maximum steered wheel angle or articulation angle proportional to the vehicle speed when the PVED-CLS is operating in auto-guidance steering mode.



Operation

By configuring a safe maximum steered wheel angle or articulation angle characteristic proportional to the vehicle speed, a safe minimum turning radius can be achieved for all vehicle speeds. At low speeds, a small turning radius is allowed for fast acquiring the path. At higher speed, the turning radius is limited to a higher value.
The characteristic is configured by operation point G, H and I which can be freely defined. The auto-guidance control algorithm will make a linear interpolation in between each of the three points.

Note that point S is defined by vehicle speed EH steering shut-off safety function. At vehicle speed P3253 the PVED-CLS enter safe state. The operator must use the steering wheel. The steering revolution lock-to-lock will be given by the OSP displacement. The OSP displacement will always define the highest possible steering ratio.

The vehicle speed dependent wheel or articulation angle shall be configured as follows.

Parameter	Description	Recommended value
P3461	The maximum angle at point G. Fixed at 0 km/h.	OEM decision
P3463	The vehicle speed at point H	OEM decision
P3465	The maximum flow at angle point H	OEM decision
P3467	The vehicle speed at point I	OEM decision
P3469	The maximum flow at angle point I	OEM decision

Important

- Point G: Set P3461 to a high value to allow narrow turning radiuses. For experimentation, start with the largest possible wheel- or articulation angle. Use values given for maximum turn angle P3426 and P3428 in the vehicle geometry sector.
- Point I: Set P3467 to the vehicle speed where the highest possible turning radius limitation is desired.
- Point I: Set P3469 to the turn angle which is deemed safe at P3467 km/h.
- Point H: Set P3463 and P3465 between point G and I.
- Parameter values must conform to: (0 < P3463 < P3467) and (P3461 > P3465 > P3469).
- The system integrator must validate the configured characteristic.

13.9 AUTO-GUIDANCE DISENGAGE BY AUX STEERING DEVICE - MINI-STEERING WHEEL SSM_036

The safety related control function disengages auto-steering mode when the auxiliary mini-steering wheel is operated and switches to the selected steering program.

Operation

Two criteria shall be fulfilled before the decision is taken to disengage auto-guidance:

1. The mini-steering wheel speed must be above a defined rpm threshold (P3646)
2. The mini-steering wheel angle change must exceed a defined angle range (P3719).

As long as the mini-steering wheel speed is below P3646 rpm, the measured steering wheel angle change is set to 0. Once the steering wheel speed exceeds P3646 rpm, the steering angle change is measured and compared to the range defined by P3719. Auto-guidance control is disengaged when both criteria are fulfilled.

Parameter	Description	Recommended value
P3239	Auxiliary steering device present	TRUE
P3240	Auxiliary steering device type is set to mini-steering wheel	2
P3646	Steering-wheel "in use" speed threshold [dRPM]	15
P3719	Steering-wheel "in use" angle change threshold [degrees]	10

Important

The system integrator must determine the steering wheel speed and position disengage criteria.

- Setting P3646 and P3719 too low may cause unintended auto-guidance by e.g. machine vibrations.
- The disengage criteria can be made dependent on steering wheel angular speed only by setting P3719 to 0.
- The system integrator must determine the auxiliary steering wheel disengage threshold.

External reference: ISO 10975 Tractors and machinery for agriculture and auto-guidance systems for operator-controlled tractors and self-propelled machines - Safety requirements for auto-guidance systems.

13.10 AUTO-GUIDANCE DISENGAGE BY AUX STEERING DEVICE - OPEN LOOP JOYSTICK SSM_037

The safety related control function disengages auto-steering mode when the open loop auxiliary joystick is operated. The software switches to open loop joystick steering mode.

Operation

Activation of the open loop auxiliary joystick resulting in flow command equal to or greater than the value defined in parameter P3647 disengages auto-steering mode. The threshold unit is 1/1000 of the joystick full-flow command.

Parameter	Description	Recommended value
P3239	Auxiliary steering device present	TRUE
P3240	Auxiliary steering device type is set to open loop joystick	0
P3647	Open loop auxiliary joystick in-use detection flow threshold [IR].	10

Important

- The system integrator must determine the auxiliary joystick disengage threshold.
- Setting P3647 too low may cause unintended auto-guidance disengage by e.g. machine vibrations.

External reference: ISO 10975 Tractors and machinery for agriculture and auto-guidance systems for operator-controlled tractors and self-propelled machines - Safety requirements for auto-guidance systems.

13.11 AUTO-GUIDANCE DISENGAGE BY AUX STEERING DEVICE - CLOSED LOOP JOYSTICK SSM_065

The safety related control function disengages auto-steering mode when the closed loop auxiliary joystick is operated. The software switches to closed loop joystick steering mode.

Operation

Activation of the closed loop engage button works as the sole means to disengage auto-steering mode and the software enters closed loop joystick steering mode.

Parameter	Description	Recommended value
P3239	Auxiliary steering device present	TRUE
P3240	Auxiliary steering device type is set to closed loop joystick	1

Important

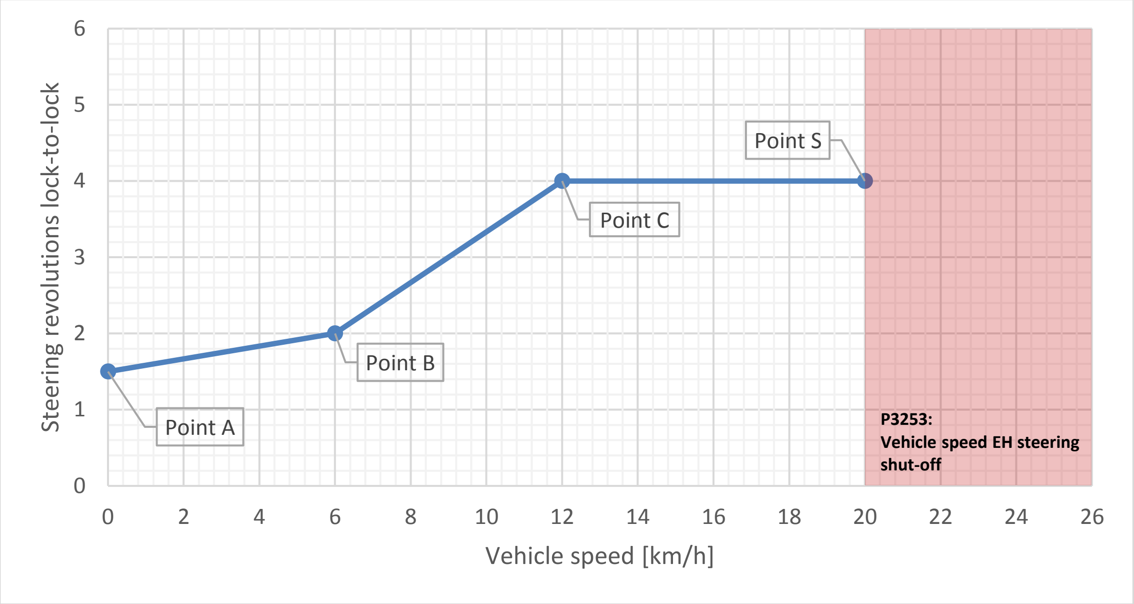
- Auto-steering mode will not be disengaged if the closed loop joystick is activated. Upon activation of closed loop joystick engage button, the steering controller will immediately move the steered wheels to the current joystick set-point.
- The system integrator is responsible for ensuring that using the closed-loop joystick for disengaging meets the required performance level.

External reference: ISO 10975 Tractors and machinery for agriculture and auto-guidance systems for operator-controlled tractors and self-propelled machines - Safety requirements for auto-guidance systems.

Attention ⚠	**Disengaging auto-guidance while there is a large closed-loop error between the joystick set-point position and the steered wheel position, will lead to prompt wheel movement.**

13.12 VEHICLE SPEED DEPENDENT FLOW LIMITATION - MINI-STEERING WHEEL MODE SSM_038

The safety related control function, Vehicle speed dependent flow limitation for auxiliary mini-wheel steering, can amplify the EH steering flow as a function of the vehicle speed. The safety related control function is available for each of the five auxiliary mini-steering wheel programs in normal operation mode.



Operation

The PVED-CLS has five different auxiliary mini-steering wheel programs, where the system integrator can configure the wanted number of steering wheel revolutions lock-to-lock at a given vehicle speed to achieve "Fast steering" or "Variable steering ratio". The steering ratio for each mini-steering wheel (AUX1 to 5) is configured by operation point A, B and C. The steering wheel control algorithm will make linear interpolation in between each of the three points.

Note that point S is defined by vehicle speed EH steering shut-off safety function. At vehicle speed P3253 the PVED-CLS enters safe state and steering control must be regained via the steering wheel.

Parameter	Description	Default value
P3650, P3658, P3666, P3674, P3682	Number of steering wheel revolutions lock-to-lock for: Point A for AUX1, 2, 3, 4 and 5 respectively. [x0.01]	800
P3652, P3660, P3668, P3676, P3684	Number of steering wheel revolutions lock-to-lock for: Point B for AUX1, 2, 3, 4 and 5 respectively. [x0.01]	800
P3654, P3662, P3670, P3678, P3686	Number of steering wheel revolutions lock-to-lock for: Point C for AUX1, 2, 3, 4 and 5 respectively. [x0.01]	800
P3656, P3664, P3672, P3680, P3688	Vehicle speed for point B for AUX1, 2, 3, 4 and 5 respectively. [km/h]	5
P3657, P3665, P3673, P3681, P3689	Vehicle speed for point C for AUX1, 2, 3, 4 and 5 respectively. [km/h]	10

Configuring all steering wheel programs to be safe may reduce the criticality of the MMI sub-system.

Important

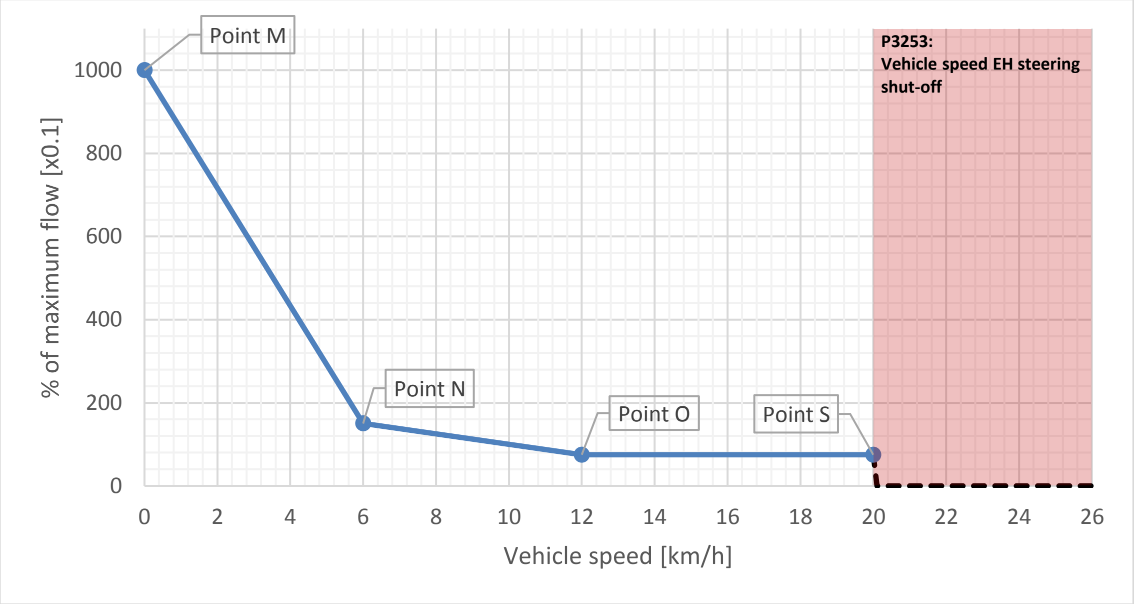
- The system integrator shall address and analyze all parameters.
- There is no restriction on the values of Point A, B and C.
- Point A is always specified at Vehicle speed = 0 km/h
- Point C "No of turns" is valid for Point C "Vehicle speed" and vehicle speeds above Point C "Vehicle speed"
- Point A "No of turns" ≤ Point B "No of turns" ≤ Point C "No of turns"
- Point C "Vehicle speed" > Point B "Vehicle speed" > Point A "Vehicle speed" (0 km/h).
- Unused AUX programs shall be set to the default values for bypassing flow amplification.

- The system integrator must validate that all steering programs are safe.
- The system integrator must validate that program changes are safe.

Attention ⚠	• **A too low steering revolution at too high speeds may lead to instability or loss of vehicle control.** • **Configure the steering wheel programs according to the recommendations.**
Warning ⚠	**Using the auxiliary mini-steering wheel and exceeding the vehicle speed threshold defined by P3253 will lead to loss of steering with the auxiliary mini-steering wheel. Steering control must be regained by the steering wheel.**

13.13 VEHICLE SPEED DEPENDENT FLOW SCALING - OPEN LOOP AUXILIARY JOYSTICK SSM_061

The safety related control function, Vehicle speed dependent flow limitation for auxiliary joystick steering, is scaling the EH steering flow as a function of the vehicle speed. The characteristic which can be configured for the joystick program is shown below.



Operation

The vehicle speed dependent flow scaling function, for the auxiliary joystick steering program, maps the full scale of the joystick signal to a vehicle speed dependent maximum steering flow scale.

Example

At a given vehicle speed, if the maximum output flow range at a given vehicle speed results in 400 IR and the joystick position is 700 IR, the resulting flow command calculated by PVED-CLS will be 700 IR • (400IR/1000IR) = 280IR.

Parameter	Description	Default value
P3690	Point M: Max possible flow at vehicle speed 0 km/h. [x0.1 of maximum flow capacity]	1000
P3692	Point N: Flow command at 'Vehicle speed for point N' [x0.1 of maximum flow capacity]	50
P3694	Point O: Flow command at 'Vehicle speed for point O' [x0.1 of maximum flow capacity]	25
P3696	Vehicle speed for point N. [km/h]	15
P3697	Vehicle speed for point O. [km/h]	25

Important

- The system integrator shall address and analyze all parameters.
- Point M "Max flow" ≥ Point N "Max flow" ≥ Point O "Max flow"
- Point C "Vehicle speed" > Point B "Vehicle speed" > Point A "Vehicle speed" (0 km/h).
- Point O "Vehicle speed limited flow" > Point N "Vehicle speed limited flow" > Point M "Vehicle speed limited flow"

Attention ⚠	**A too high maximum flow range at a given vehicle speed may lead to instability or loss of vehicle control.**
Warning ⚠	**Using the auxiliary joystick and exceeding the vehicle speed threshold defined by P3253 will lead to loss of steering in joystick steering mode. Steering control must be regained by the steering wheel.**

13.14 SAFE AUTO-CALIBRATION STOP - SERVICE MODE SSM_039

The safety related control function, Safe auto-calibration stop, aborts a valve auto-calibration procedure and positions the EH-valve main spool in neutral when the steering wheel is activated. The function is only available when the PVED-CLS is in service mode.

Operation

The embedded valve auto-calibration procedure can be invoked in service mode. The operator must activate the steering wheel from the cabin prior to starting the procedure to signal operator presence. Once the PVED-CLS registers steering wheel activation (P3583 and P3584), a spool calibration activation window (P3801) is opened for receiving the valve auto-calibration start command. After the spool calibration activation window has timed out, auto-calibration start commands will be ignored.

Once the auto-calibration procedure is started, the steered wheels will be moving autonomously while searching the valve deadbands. The steering wheel will work as stop sensor during. If auto-calibration is stopped by the steering wheel, the calibration procedure will reset to the initial state where it will wait to be restarted.

Parameter	Description	Default value
P3583	Steering wheel "in use" speed threshold [dRPM]	5
P3584	Steering wheel "in use" angle change threshold [degrees]	10
P3801	Spool calibration activation time-out [seconds]	20

Important

Refer to section 13.5 for setting the steering wheel activation threshold (P3583 and P3584).

Warning ⚠	**The system integrator shall ensure that the operator is informed to stay in the cabin while the valve auto-calibration procedure is on-going.**

13.15 SAFETY RELATED SPECIFICATIONS FOR OSPE, EHI-E AND EHI-H VALVE SUB-SYSTEMS SSM_040

For reliability calculation, the following safety related block diagram can be used. Only relevant sensors are included.

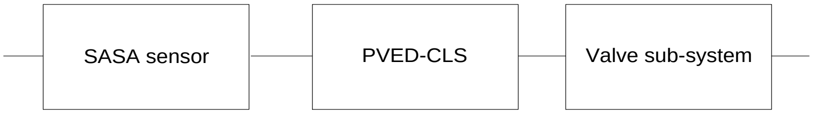


Figure 37. Safety related block diagram.

Important

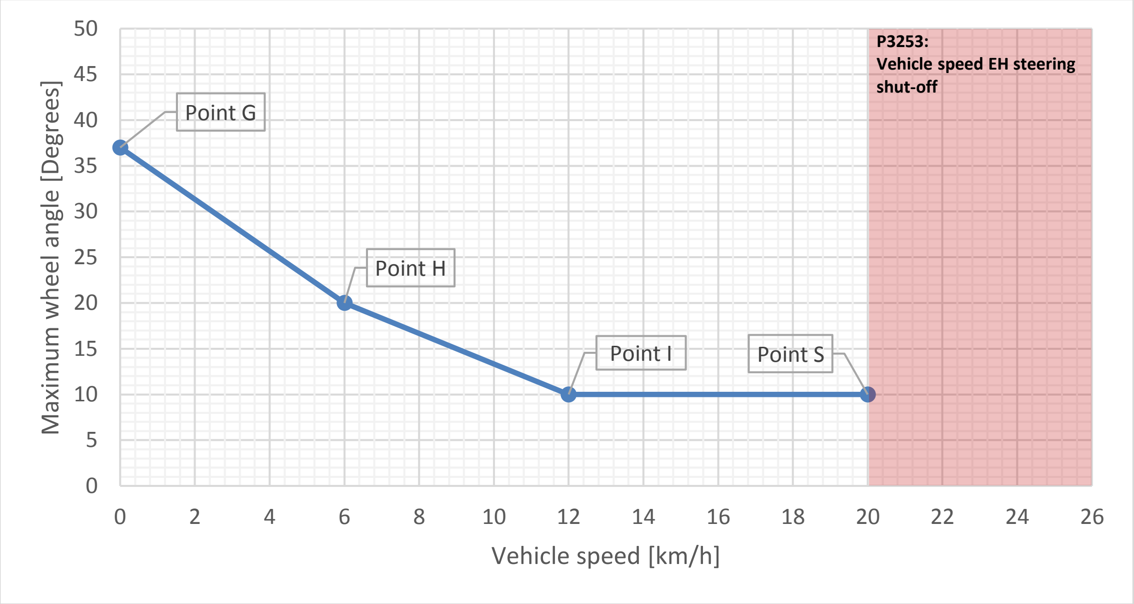
- The target AgPLr is d.
- The MTTFd,ch for the entire channel must be better than 10 years (medium).
- The DCavg must be ≥ 90 % (for ISO25119 DCavg must be ≥ 60 %).
- The sensor sub-systems are designed to be suitable for a category 3 safety loop.
- The sensor sub-system requirements must be met.

Sub-system	MTTFd	DC	Category	CCF
SASA sensor sub-system	73 years	99 %	3	√
PVED-CLS OSPE valve sub-system	36 years	95 %	3	√

The PVED-CLS safety related specifications are described in section 4.1.

13.16 VEHICLE SPEED DEPENDENT WHEEL ANGLE LIMITATION - CLOSED LOOP JOYSTICK SSM_062

The safety related control function, Vehicle speed dependent wheel angle limitation, limits the maximum steered wheel angle or articulation angle proportional to the vehicle speed when the PVED-CLS is operating in closed loop joystick mode.



Operation

By configuring a safe maximum steered wheel angle or articulation angle characteristic proportional to the vehicle speed, a safe minimum turning radius can be achieved for all vehicle speeds, this is done by limiting the wheel angle set-point from the closed loop joystick. At low speeds, a small turning radius is allowed for fast acquiring the path. At higher speed, the turning radius is limited to a higher value.

The characteristic is configured by operation point G, H and I which can be freely defined. The closed loop joystick control algorithm will make a linear interpolation in between each of the three points.

Note that point S is defined by vehicle speed EH steering shut-off safety function. At vehicle speed P3253 the PVED-CLS enter safe state. The operator must use the steering wheel. The steering revolution lock-to-lock will be given by the OSP displacement. The OSP displacement will always define the highest possible steering ratio.

The vehicle speed dependent wheel or articulation angle shall be configured as follows.

Parameter	Description	Recommended value
P3720	The maximum wheel angle at point G. Fixed at 0 km/h.	OEM decision
P3723	The vehicle speed at point H	OEM decision
P3721	The maximum wheel angle at angle point H	OEM decision
P3724	The vehicle speed at point I	OEM decision
P3722	The maximum wheel angle at angle point I	OEM decision

Important

- Point G: Set P3720 to a high value to allow narrow turning radiuses. For experimentation, start with the largest possible wheel- or articulation angle. Use values given for maximum turn angle P3426 and P3428 in the vehicle geometry sector.
- Point I: Set P3724 to the vehicle speed where the highest possible turning radius limitation is desired.
- Point I: Set P3722 to the turn angle which is deemed safe at P3467 km/h.
- Point H: Set P3723 and P3721 between point G and I.
- Parameter values must conform to: (0 < P3723 < P3724) and (P3720 > P3721 > P33722).
- The system integrator must validate the configured characteristic.

Warning ⚠	**The above described safety related control function limits the maximum allowed wheel angle proportional to the vehicle speed. This means that if the vehicle is driving through a curve, with a given joystick in the position, the wheel angle will change if the speed is increased or decreased.**

13.17 HYDRAULIC OVERRIDE OF AUTO-CALIBRATION - SERVICE MODE SSM_069

The safety related control function, hydraulic override of auto-calibration, aborts a valve auto-calibration procedure and positions the EH-valve main spool in neutral when the steering wheel is activated. The function is only available when the PVED-CLS valve controller is used together with an EHi-H valve sub-system and the PVED-CLS is in service mode.

Operation

The embedded valve auto-calibration procedure can be invoked in service mode. Once the auto-calibration procedure has been invoked, a spool calibration activation window is opened for receiving the valve auto-calibration start command, as long as no steering wheel movement is observed.

Once the auto-calibration procedure is started, the steered wheels will be moving autonomously while searching the valve deadbands. During the auto-calibration the steering wheel will work as stop sensor. The steering wheel movement will be detected by measures described in section 10 Hydraulic override for EHi-H valve sub-systems. If steering wheel movement is detected, the auto-calibration will be aborted and only restart if the valve auto-calibration start command is received.

Important

Refer to section 10 Hydraulic override for EHi-H valve sub-systems for setting the parameters related hydraulic override.

Warning ⚠	**The system integrator shall ensure that the operator is informed to stay in the cabin while the valve auto-calibration procedure is on-going.**

13.17.1Configuration of Hydraulic Override and Internal Monitored Disengage

Hydraulic override and internal monitored disengage can only be used in systems comprised by a PVED-CLS valve controller and EHi-H valve sub-system. Furthermore, a SASA sensor cannot be present in the system when using hydraulic override and internal monitored disengage, meaning that the disengage method shall be configured to be Internal Monitored Disengage. See the table below.

Parameter	Description	Main controller	Safety controller
P3254	EH-steering disengage method. (0 = SASA (default, 255 = Internal monitored disengage)	255	255

13.18 HYDRAULIC OVERRIDE OF AUTO-GUIDANCE AND AUXILIARY STEERING SSM_070

The safety related control function, hydraulic override of auto-guidance and auxiliary steering, disengages auto-steering mode or auxiliary steering mode when the steering wheel is activated and switches to the selected steering program.

Operation

Steering wheel activation will be detected by measures described in section 10 Hydraulic override for EHi-H valve sub-systems.

Important

Refer to section 10 Hydraulic override for EHi-H valve sub-systems for setting the parameters related hydraulic override.

Attention ⚠	**Unintended and rapidly repeated engaging of auto-guidance control may lead to loss of steering controllability. The scenario is as follows; for each unintended start of auto-guidance the driver must consequently counter-steer to disengage auto-guidance mode.**

13.18.1 Configuration of Hydraulic Override and Internal Monitored Disengage

Hydraulic override and internal monitored disengage can only be used in systems comprised by a PVED-CLS valve controller and EHi-H valve sub-system. Furthermore, a SASA sensor cannot be present in the system when using hydraulic override and internal monitored disengage, meaning that the disengage method shall be configured to be Internal Monitored Disengage. See the table below.

Parameter	Description	Main controller	Safety controller
P3254	EH-steering disengage method. (0 = SASA (default, 255 = Internal monitored disengage)	255	255

14 Safe on-road mode

The 'Safe on-road mode' safety function can be used in cases where it is desired that the PVED-CLS is powered while the vehicle is being used on public roads. No electro-hydraulic steering functionality is available in safe on-road mode. The rationale for this may be to continuously receive status information or sensor data.

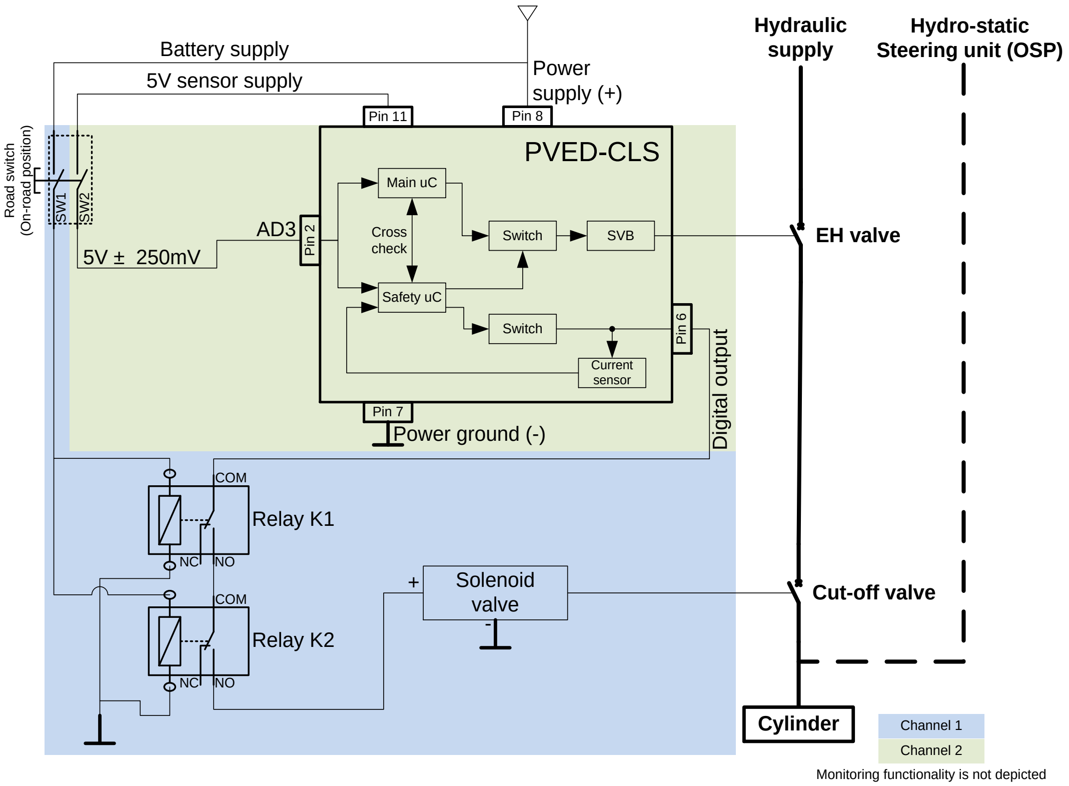
Warning ⚠	**The system integrator shall ensure that the PVED-CLS and valve sub-system are brought into a safe state while the vehicle is being used on public roads.**

The safety function works differently and offers differing safety integrity levels depending on which valve sub-system is being used.

14.1 OSPE, EHI-E AND EHI-H VALVE SUB-SYSTEM SSM_041

Operation

The road switch for OSPE, EHi-E and EHi-H valve sub-systems described in section 8.10 shall be used and configured. The architecture for the safety function, safe on-road mode, shall be established by adding an independent and diverse electro-mechanical shut-down channel (channel 1) which works in parallel to the PVED-CLS (channel 2). The two realized channels are depicted in the below figure.



The road switch shall connect and disconnect a) battery supply to relay K1 and K2 and b) 5V sensor supply. There shall be no electrical connection between NO and COM when the relay is de-energized.

Road switch open (safe on-road mode): Both relays shall be de-energized. The enabling signal (AD3) to the PVED-CLS is pulled to ground by the PVED-CLS. The cut-off solenoid valve is de-energized.
Switch closed (EH steering enabled): The enabling signal (AD3) shall be in the 'enable' voltage range. Both relays shall be powered. K1 and K2 shall connect PVED-CLS digital output to the cut-off solenoid valve.

Monitoring:
The PVED-CLS monitors the switch and relay operation by cross-checking the enabling signal (AD3) with the supplied current to the cut-off solenoid valve. When no current must be delivered, the presence of the open connection is

periodically tested by voltage test-pulsing. At detection of a fault, the PVED-CLS enters safe state and issues a diagnostic trouble code on the CAN bus.
The 5V sensor supply is monitored for short-circuits to ground or battery supply. The enable/disable voltage on the AD3 input is range checked.

Channel 1 consists of SW1, two NO relays and the solenoid valve and the cut-off valve.
Channel 2 consists on SW2 and the PVED-CLS, the SVB and the EH-valve.
Channel 1 and 2 can both independently perform the safety function. Channel 2 is used for monitoring channel 1. Fault accumulation is addressed as follows; the safety function can be demanded in the presence of two undetected failures. The failure(s) may not be detected until the safety function is demanded but at least one of the channels will perform the safety function.

The safety related block diagram can be drawn as follows.

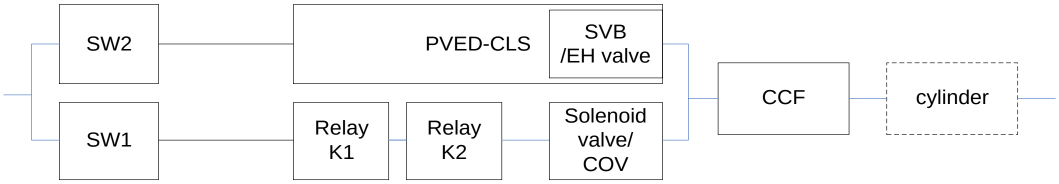


Figure 38: Safety related block diagram

To design the safety function to meet category 4, AgPL/PL e, in accordance with ISO 2525119 and ISO 13849, the principle of combining channels by safety capability is applied as specified in IEC 61508.

The following requirements shall be met to reach SIL3 according to IEC 61508 and AgPL/PL e in accordance with ISO 25119 and ISO 13849:

- Both channels shall meet SIL2
- The systematic capability (SC) of both channels shall be ≥ 2.
- Both channels work shall work in high demand mode.
- Channel 2 is of type B (complex).
- Channel 1 is of type A (non-complex).
- The channels shall be independent and diverse.
- A common cause analysis shall be performed
- Equivalence mapping to ISO 25119 and ISO 13849 yields:
  - Each channel shall meet an MTTFd ≥ 30 years.
  - Each channel shall at least achieve AgPLd / PLd according to ISO 25119 and ISO 13849.
  - The diagnostic coverage shall be ≥ 90 % for each channel
  - The safety function shall be performed in the presence of two undetected faults
- The PVED-CLS works as a monitoring device for channel 1.
- To apply fault exclusion, the switch, relay, wiring and installation enclosure satisfies the standards ISO 13849-2 annex A and D IEC 60947-5-1 and IEC 60204.

Calculation
Safety related specifications are relevant for the calculation.

Sub-system	MTTFd	DC	Category	CCF
Road switch sub-system	Road switch sub-system section 8.11			
PVED-CLS	57 years	95 %	3	√
Solenoid valve, cut-off valve	150 years	90 %		

The MTTFd for PVED-CLS has been adjusted to include only elements which are relevant for the specific safety function. The MTTFd for the PVED-CLS includes the solenoid valve bridge and the EH-valve.

The PVED-CLS operates as a monitoring device for the electro-mechanical channel. The following diagnostic coverage can be used for the calculation:

Sub-system monitoring	DC	Description
PVED-CLS	96 %	Resulting DC per PVED-CLS FMEDA. Lowest number is applied for both channels.
Solenoid valve, Cut-off valve	90 %	Full-stroke testing of the solenoid valve and cut-off valve on each program transition to an EH-steering program.
Road switch	99 %	Cross-checking of SW1 and SW2 signals by the PVED-CLS.
Relay monitoring (K1, K2)	99 %	The connection from the PVED-CLS, through the relays to the solenoid valve is on-line tested by the PVED-CLS as follows; In on-road mode a periodical test voltage is applied to check if a current is flowing to the solenoid valve. If the measured current exceeds the test threshold defined by P3242 (100 mA @12 V) a fault is detected. (100 mA@12 V is not sufficient to open the COV). In off-road mode it is tested if the current is supplied to the solenoid valve is correctly controlled and reached the current set-point.

Example calculation

The switch and relay elements shall be supplied by a 3rd party. This examples show how the MTTFd requirements of the elements can be determined. In the below table the MTTFd for these elements are shared evenly. Channel 1 constrains the MTTFd values of the switch and relays most. The lower MTTFd for each of these elements can be show to be 115 years in order for channel 1 to meet a minimum MTTFd of 30 years.

Channel 1 elements	MTTFd [years]	DC [%]
SW1 (switch channel 1)	115	99
Relay K1	115	99
Relay K2	115	99
Solenoid valve (SV), COV	150	90
MTTFd,ch	**30**	
DCavg		**97**

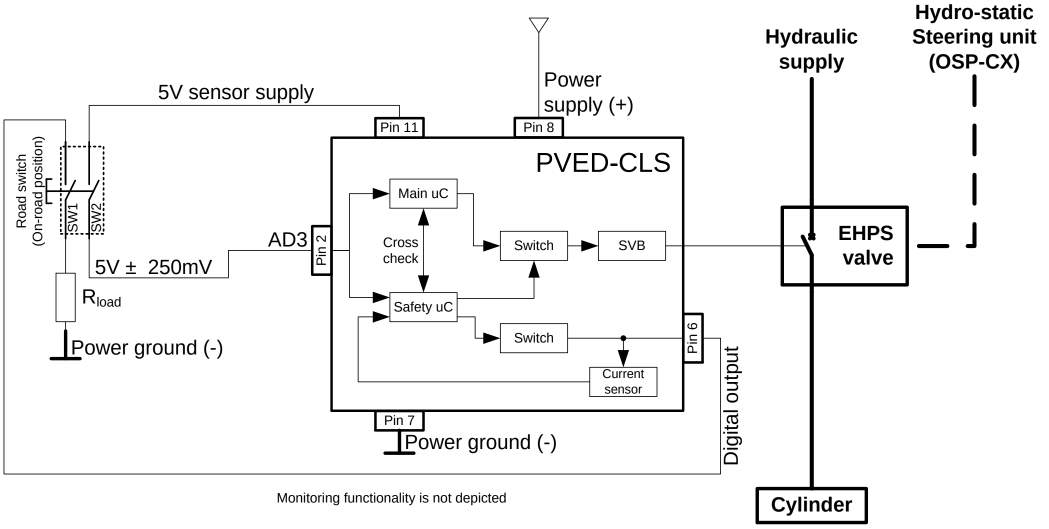
Channel 2 elements	MTTFd [years]	DC [%]
SW2 (switch channel 2)	115	99
PVED-CLS (SVB, EH valve)	57	95
MTTFd,ch	**38**	
DCavg		**96**

Refer to ISO 13849 for calculation of MTTFd,ch and DCavg.

14.2 EHPS-SYSTEM SSM_042

Operation

The road switch for EHPS valve systems, described in section 8.11 shall be used and configured. The architecture for the safety function, safe on-road mode, can be achieved by connecting the road switch sub-system to the PVED-CLS as depicted in the below figure. The architecture enables implementing the safety function to SIL2, PL d and AgPL d.



The following elements are relevant for the safety function.

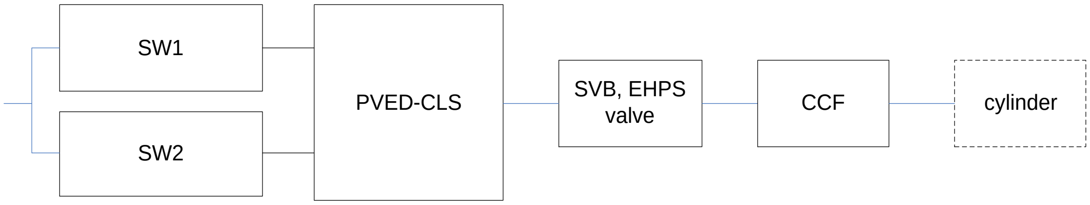


Figure 39: Safety related block diagram

Calculation

To achieve PL d or AgPL d, the MTTFd must be higher than 30 years (high).
The channel is limited to category 2 element due to the single final element (EHPS valve).

Sub-system	MTTFd	DC	Category	CCF
Road switch sub-system	Road switch sub-system section 8.11			
PVED-CLS	57 years	95 %	2	√
EHPS valve sub-system				√

Monitoring: To achieve AgPL d/PL d, the DC must be equal or higher than 60 % per ISO25119 and 90 % per ISO 13849 respectively. The PVED-CLS road switch monitoring features are used for diagnostics. The inputs are cross-checked. A diagnostic coverage in the high range (90-99 %) can be claimed.

Example calculation

The switch shall be supplied by a 3rd party. This examples show how the MTTFd requirements of the switch can be determined. The lower MTTFd for the switch can be show to be 70 years in order for the channel to meet a minimum MTTFd of 30 years.

Channel 1 elements	MTTFd [years]	DC [%]
Road switch (SW1, SW2)	70	99
PVED-CLS (SVB, EH valve)	57	95
MTTFd,ch	**31**	
DCavg		**96**

15 Hazards not covered by PVED-CLS safety functions or monitoring SSM_054

Warning ⚠	**The following list of hazardous events and associated risks are not - and cannot - be covered by functional safety realized in the PVED-CLS. The system integrator shall carefully study the below list and ensure an adequate risk reduction.**

15.1 UNINTENTIONAL PERIODICAL AUTO-GUIDANCE ENGAGE COMMANDS

A faulty auto-guidance receiver or auto-guidance man-machine interface implementation may lead to a dangerous situation. A single unintended auto-guidance engage command shall be resolved by the driver by activating the steering wheel. Additional safety functions can be utilized to ensure that a resulting unintended change of steering direction happens sufficiently slowly for the operator to intervene in a controlled fashion.

Several unintentional and repeating auto-guidance engage commands may result in an accumulation of steering flow to one direction if the driver expects that he/she shall only disengage the steering motion with a small counter steering activation on the steering wheel. The hazard increases with the valve capacity. And may be most severe at low vehicle speeds where flow limitation has the smallest effect.

15.2 USE CAN DATA FOR EXTERNAL SAFETY RELATED CONTROL FUNCTIONS

The system integrator is advised not to use CAN messages with no safety protocol for safety related control functions. This is true for e.g. Guidance Machine Status, Diagnostic Message DM1 and Status message 1 to 6. Refer to the PVED-CLS communication manual for messages with and without a safe protocol layer.

15.3 UNINTENDED LOSS OF VARIABLE STEERING

A too sudden increase in the steering ratio lock-to-lock (more steering wheel revolutions is suddenly needed) may lead to unintended operator steering reactions. The system integrator is advised to analyze and become familiar with the impact of losing variable steering in steering wheel mode. In the situation where EH-steering is lost i.e. by entering the safe state, on-road mode or losing battery power, the EH steering flow contribution will stop and steering control is obtained by the steering orbital. The change in steering ratio depends on the orbital displacement and the variable steering ratio at the time when the EH steering flow was lost.
The system integrator is recommended to use visual and audio alarms to notify the operator.

15.4 LOSS OF EH-FLOW TO ONE DIRECTION

In variable steering configurations for steering wheel modes, a hardware malfunction may in rare occasions result in loss of EH-flow to one direction. This will result in an asymmetric left-right steering ratio, meaning that variable steering works correct to the right but not to the left or wise versa. When the variable steering configuration guideline is followed, the impact, asymmetric behavior, is most noticeable at low vehicle speeds, where the EH flow contribution is highest, and becomes less noticeable as vehicle speed increases and the EH contribution decreases. If aggressive variable steering configurations is used, meaning that the OSP displacement ratio to EH-steering is very small, the system integrator is recommended to test the fault impact on the vehicle to assess the controllability.
In auto-guidance and joystick modes, the valve will not be able to steer to one direction. In these cases the driver shall intervene and take control with the steering wheel.
In general, no diagnostic function will detect the failure as the failure mode, no EH flow, is considered safe, thus functional safety is not impacted and works as designed.

Important

The following faults do not bring the PVED-CLS into the safe state. An interfacing system ECU must capture these DTCs and take appropriate action:

- Battery voltage too low throws an INFO level DTC. The fault is cleared again when the voltage supply is within valid range. The fault is not critical but the EH-steering performance may be reduced.
- The average life-time temperature exceeds 85 °C. The fault is not critical to a degree where the PVED-CLS shall be switched off immediately. However, the installation shall be inspected and a corrective action shall be taken.

16 Environmental control measures

The installation of the PVED-CLS is critical for the machine uptime. In order to respect the absolute stress ratings of the electronic components, the PVED-CLS must be carefully installed in an area with a known maximum ambient temperature.

The PCB ambient temperature is measured internally and is a sum of the ambient temperature of the PVED-CLS installation and the self-heating of the PVED-CLS.

Attention ⚠	**The PVED-CLS must not be installed in areas where the ambient temperature exceeds 85°C.** **Contact a Danfoss Product Application Engineer for further information.**

Operation

For controlling common cause failure, the PVED-CLS features the following functions

- PCB overheating shut-down
- PCB average over-temperature warning

16.1 PCB OVERHEATING SHUT-DOWN SSM_043

Under normal operation the PVED-CLS must continuously measure the PCB temperature. If the PCB temperature exceeds 120 °C, the PVED-CLS enters safe state immediately.

For manufacture testing purposes only, it is possible to disable this function by setting the temperature severity level to INFO. Thereby the PVED-CLS will not to enter safe state if the PCB temperature exceeds 120 °C.

Parameter	Description	Recommended value
P3386	Temperature severity level (0 = Severity level: Critical, 255 = Severity level: INFO)	0

Important

- It is strictly prohibited to set the temperature severity level to other than critical.
- Setting the temperature severity level to other than critical leads to immediate loss of warranty.

Attention

⚠

The system integrator shall:

- Secure that the temperature severity level is set to critical.

16.2 PCB AVERAGE OVER-TEMPERATURE WARNING SSM_044

The PVED-CLS maintains a PCB temperature histogram to monitor the average PCB temperature over the PVED-CLS life-time. A J1939 DM1 Information message will be issue if the average temperature exceeds 85 °C. The PVED-CLS will continue operation while issuing the info CAN message.

Important

It is recommended that an external ECU is configured to listen the average over-temperature information. If observed the system integrator should consider revising the PVED-CLS installation environment.

The temperature histogram can be read out of memory by e.g. the PLUS+1 PVED-CLS service tool. See PVED-CLS Parameter Description for details on where the data can be read.

17 Safety Parameterization SSM_045

Parameterization or configuration is the process of modifying software parameters in EEPROM which can modify the behavior of the safety device.

Warning ⚠	- **Modifying behavior includes changing or disabling a safety function or a monitoring function behavior or performance.** - **Any parameterization of the PVED-CLS shall follow the be devised safety parameterization procedure.**

The PVED-CLS support protocol services which enable the design of safe parameterization covering the channel; the service tool user, the service tool hardware and software, the communication channel and the PVED-CLS eeprom memory.

17.1 SAFETY PARAMETERIZATION PROCEDURE

Step	Description	Response/Result
1	**Enter boot-loader mode** Set the PVED-CLS in boot-loader mode	PVED-CLS de-energizes all outputs (safe condition) and enables access to configuration memory
2	**User identification** Enter the access level (Manufacturer, OEM or dealer) and the Parameter Sector Access Code (PSAC)	The user identifies him/her-self and request access rights to the sectors subject for modification. Failing to set the PSAC or unauthorized modification attempts will be detected and bring the PVED-CLS into the safe state on the subsequent power-up.
3	**Upload data** Upload the data for the sector which is subject for modification. Request uploading data in the diverse data format. Decode and display the data for both the main and safety controller in a diverse data format	The PVED-CLS returns all parameter values to the service tool as bit-wise inverted data. The diverse data enforces realization of a read-back and display method in the service tool which is diverse from the write procedure in step 4 and 5
4	**Data modification** Modify one or more parameters in the sector and calculate the sector CRC value. Input values are entered as strings values (numbers and characters)	The data is encoded from string-to-hexadecimal values. The modified sector and sector CRC is stored in service tool memory
5	**Download data** Download the modified sector and the associated sector CRC from service tool memory to both the main and safety controller memory	When downloading a new sector to the main and safety controller, the previous signature CRC becomes invalid. The PVED-CLS will be locked in the safe state until a correct signature CRC is created and downloaded to the PVED-CLS
6	**Upload data** Upload the data for the sector which is subject for modification. Request uploading in diverse data format. Decode and display the data for both the main and safety controller as ascii characters	The PVED-CLS transmits all parameter values as bit-wise inverted data. The diverse data format enables the realization of a read-back and display method which is diverse from the write procedure in step 5
7	**Data validation** The user shall inspect all parameter values in the sector	The user inspects that the data is correctly modified and that the other parameters in the sector are valid
8	**User approval signature** The user approves the data in the sector by calculating the signature CRC. The signature CRC depends on the sector CRC and the entered PSAC	The PSAC for the modified sector is downloaded to the PVED-CLS configuration memory
9	**Reset** Reset or power-cycle the device for the changes to take effect	Safe parameterization is complete. The user shall validate the changes

Important

- The service tool user closes the safety loop during parameterization i.e. a skilled user approves the parameter settings.
- Details on safe parameterization can be found in the PVED-CLS KWP2000 protocol and PVED-CLS Parameter Description.
- The PLUS+1 service tool for the PVED-CLS uses the safe parameterization procedure.

- Unauthorized changes will lead to a permanent safe state condition until the correct parameters are approved.
- Contact Danfoss Power Solutions PAE for information on the OEM and Dealer PSAC

18 System Integration and Testing

As specified in the safety-life cycle; after installation, integration or modification of the PVED-CLS, valve, SASA sensor and other sensors, the system integrator or another representative for the OEM for the shall validate the installation, configuration and correct behavior before releasing the vehicle for series production.
System integration testing shall cover the fully integrated system including

- Hydraulic installation
- Mechanical installation including sensor installation
- Electrical installation and cable harness
- Software configuration
- Functional safety
- Interface to other sub-systems
- Systematic safety integrity of the safety channels

Warning ⚠	**The system integration testing shall always be performed before start of production and after modification of the system.**

For further information on validation consult IEC 61508, ISO 13849 or ISO 25119.

18.1 VEHICLE FAULT INSERTION TESTING SSM_046

The functional safety provided by the PVED-CLS and valve may work differently from vehicle to vehicle as it may depend on factors such as configuration, vehicle geometry, valve size and cylinder volume. The system integrator is advised to perform fault insertion testing on the integrated system for failure modes where the system reaction to a fault cannot be predicted or simulated.

Contact Danfoss Power Solutions PAE for more information.

18.2 SAFETY VALIDATION TESTING SSM_047

Validation is the final test of the functional safety before commissioning the system to the end.
This safety validation test activity shall:

- Answer the question if the system integrated correctly?
- Answer the question if the system configured as specified?
- Answer the question if the system is working correctly?
- Achieve confidence in that the installation is performed correctly and that the specified functional safety is working as expected.

Contact Danfoss Power Solutions PAE for more information.

19 Diagnostics and troubleshooting

The PVED-CLS performs monitoring/diagnostic of the internal electronics, valve operation as well as external interfacing signals. Each monitoring function triggers a transition to the safe state in case a fault is detected.

- The controller which detects a given fault first, makes a transition to the safe state and informs the peer controller to also enter safe state.
- The detecting controller transmits a diagnostic trouble code related to the root-cause on to the CAN bus.
- The controller which were requested to enter safe state, issues ‘SPN 520208 Demanded safe state’.

19.1 ERROR CODES

See PVED-CL User Manual for details on error codes.

20 Component identification

The following information identifies the PVED-CLS and valve assembly. The below sections explains the various methods to perform identification.

20.1 VALVE ASSEMBLY BARCODE LABEL SSM_048

The valve assembly barcode for the fully assembled valve unit number consists of the order number (8 digit number) and a serial number. The order number specified on the customer drawing, identifying the final valve assembly (valve, valve controller, software, parameters), is glued onto the valve assembly (OSP gear set) as well as stored electronically in the PVED-CLS on the following parameter addresses.

Parameter	Address	Format	Description
Sales order number byte 1	P4064	U8	Sales order number (8 digit number)
Sales order number byte 2-7	P4065-P4070		
Sales order number byte 8	P4071		
Sales order number byte 9-14	P4072-4077		Reserved

The data can be accessed by uploading the data in boot-loader mode. See PVED-CLS KWP2000 protocol.

20.2 BOOTLOADER AND APPLICATION SOFTWARE IDENTIFICATION SSM_049

The following electronic identification for the embedded software can be retrieved from the PVED-CLS via the CAN bus.

Identification data item	Format	Size (bytes)
Boot-loader software version	ASCII	39
Boot-loader program date	BCD	3
Application software version	ASCII	39
Application program date	BCD	3

The boot-load and application software and program date information is stored in flash memory and generated by Danfoss at compile time for the main and safety controller respectively. The data is accessible via the KWP2000 Read ECU Identification service. See PVED-CLS KWP2000 protocol.

Example for main controller:

Boot-loader software version	BOOT_CLS-_M_R385_KWP2000-_11153472_-rrr
Boot-loader program date	13.03.15
Application software version	APP-_CLS-_M_R198_SEHS----_11153340_-B02
Application program date	22.03.17

Sub-string 'M' means main controller. Sub-string 'R198' means release software version 1.98. Sub-string '11153340' is a Danfoss part number for the main application software. 'B02' indicates the build number.
For the boot-loader software version '-rrr' are reserved characters.

Example for safety controller:

Boot-loader software version	BOOT_CLS-_M_R385_KWP2000-_11153472_-rrr
Boot-loader program date	13.03.15
Application software version	APP-_CLS-_S_R198_SEHS----_11153341_-B02
Application program date	22.03.17

Sub-string 'S' means safety controller. Sub-string 'R198' means release software version 1.98. Sub-string '11153341' is a Danfoss part number for the safety application software. 'B02' indicates the build number.
For the boot-loader software version '-rrr' are reserved characters.

20.3 PVED-CLS COMPONENT IDENTIFICATION AND SERIAL NUMBER SSM_050

The PVED-CLS valve controller can be identified by a serial number which is stored in the PVED-CLS eeprom memory.

Parameter	Address	Format	Description
Danfoss serial number byte 1	P962	U8	PVED-CLS Serial number
Danfoss serial number byte 2-24	P963-985		
Danfoss serial number byte 25	P986		

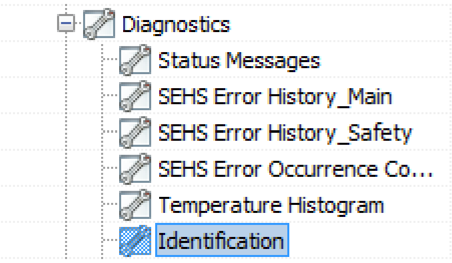
The below example shows how the PVED-CLS serial number is encoded:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
1	1	1	0	8	6	8	1	-	A	1	2	0	1	1	7	1	3	5	1	3	0	0	0	4
Part no.									Rev	Plant code				Line		Date (yywwd)					Serial no.			

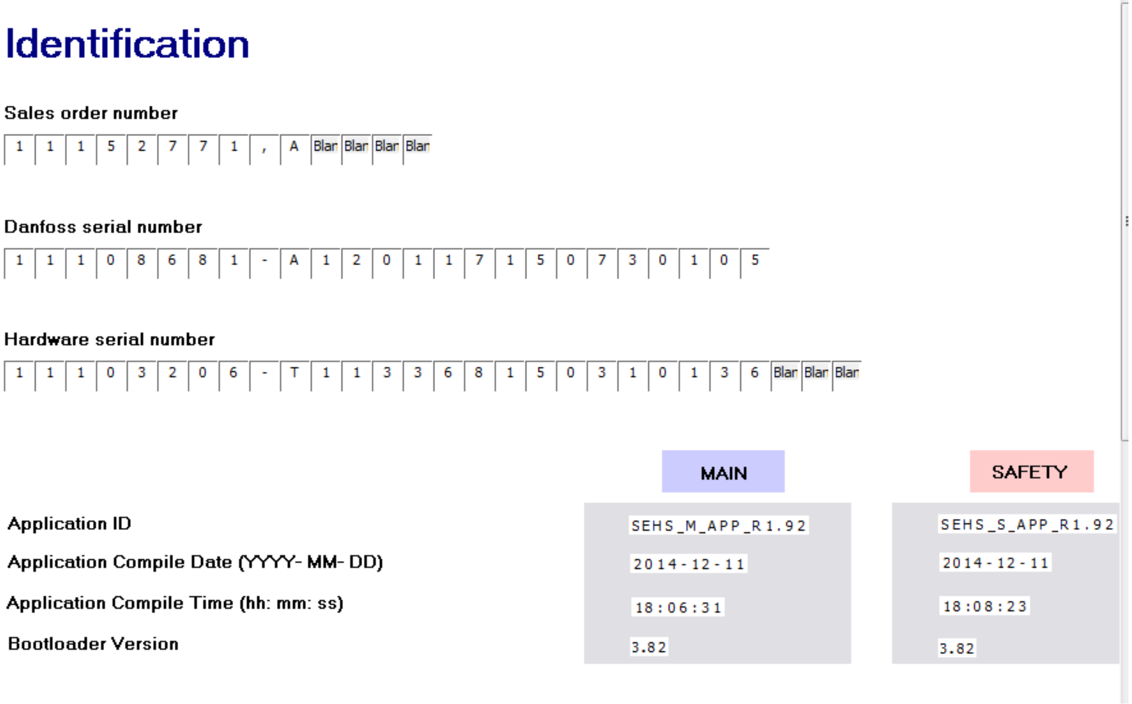
The data can be accessed by uploading the data in boot-loader mode by the KWP2000 protocol. See PVED-CLS KWP2000 protocol.

20.4 PLUS+1 SERVICE TOOL IDENTIFICATION PAGE SSM_051

The software and hardware can also be uniquely identified via the PLUS+1 service tool page "Identification" in the Diagnostics group.



Example of the information on the Identification page:



Identification

Sales order number

1	1	1	5	2	7	7	1	,	A	Blar	Blar	Blar	Blar

Danfoss serial number

1	1	1	0	8	6	8	1	-	A	1	2	0	1	1	7	1	5	0	7	3	0	1	0	5

Hardware serial number

1	1	1	0	3	2	0	6	-	T	1	1	3	3	6	8	1	5	0	3	1	0	1	3	6	Blar	Blar	Blar

	MAIN	SAFETY
Application ID	SEHS_M_APP_R1.92	SEHS_S_APP_R1.92
Application Compile Date (YYYY- MM- DD)	2014-12-11	2014-12-11
Application Compile Time (hh: mm: ss)	18:06:31	18:08:23
Bootloader Version	3.82	3.82

20.5 J1939 REQUEST PGN FOR SOFTWARE ID AND COMPONENT ID SSM_052

The software identification and component identification can be retrieved by a request program group query for software identification (PGN 65242) and component identification (PGN 65259). The data can be queried while the PVED-CLS is in operation mode.

Requesting Software ID will return the same data as given in section 20.2. Both the boot-loader software version and application software version is output in one Broadcast Announcement Message.

Requesting Component ID will return the same data as given in section 0

Example of data broadcasted by Component Identification BAM:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
*	1	1	1	0	8	6	8	1	*	A	1	2	0	1	1	7	1	3	5	1	3	0	0	0	4	*	*

Refer to PVED-CLS communication protocol documentation for details.

21 Contact Information if an abnormal safety related failure occurs

Attention ⚠	**Contact Danfoss Product Application Engineering:** • **If the product exhibits an unexpected behavior** • **If an unintended steering movement is observed and the product does not enter the safe state** • **At the suspicion of any loss of safety integrity** • **Have sales order number, PVED-CLS serial number and recorded evidence (CAN logs (.asc, .blf) or similar) of the behavior ready** • **Do not remove the PVED-CLS and valve from the vehicle until agreed with Danfoss Product Engineering as faults may not be replicable on isolated components.**

22 PVED-CLS service part handling and repair instructions

Attention ⚠	• **Do not attempt to perform modifications or repair of the PVED-CLS or valve.** • **Do not perform any unauthorized software download or modification of the PVED-CLS** • **If the product is covered by the warranty then it shall be returned to Danfoss for inspection and root cause analysis** • **Repairing a PVED-CLS shall be done by replacing it with a new unit.** • **Perform safety validation of the PVED-CLS before commissioning into the target system/vehicle.** • **The replaced PVED-CLS shall be decommissioned by e.g. adequately marking the part to avoid unintended installation to another vehicle or modifying the part so re-installation is never possible.**

Refer to the OSPE steering valve service manual, L1506577 for valve repair instructions.
Refer to the PVED-CLS 2.00 firmware release note for PVED-CLS service part software operations.

22.1 SAFETY VALIDATION STEPS AFTER REPLACING A PVED-CLS WITH A SERVICE PART

Steps 1-2 may be performed before or after mounting the PVED-CLS to the steering valve.

1. Use the PLUS+1 service tool or read out the Identification data of the PVED-CLS.
2. Compare the following software elements to the customer drawing/specification
   a. Bootloader software version
   b. Main controller software version
   c. Safety controller software version
   d. Parameter sector CRCs for the following sectors
      i. SVC (VPS)
      ii. Hydraulic Configuration
      iii. Fault Detection Algorithm (FDA)
      iv. CAN Wheel Angle Sensor
      v. Analogue Wheel Angle Sensor
      vi. Peripherals Configuration
      vii. Communication Protocol
      viii. Internal Monitoring
      ix. Vehicle Geometry
      x. GPS configuration
      xi. Steering wheel configuration
      xii. Auxiliary Steering Configuration
      xiii. Auto-calibration

   The sector CRCs for each sector shall match the CRCs on the customer drawing/specification.
3. Perform Wheel Angle Sensor and Spool calibration to complete the service part software configuration
4. Refer to section 18 on system validation after modification and repair.

23 Revision history

Date	Change	Revision
20 Dec 2013	Draft version – not reviewed. Compatible with application firmware version 1.72 Document is under internal review.	DRAFT NOT RELEASED
15 Jan 2014	Component identification is added. Compatible with application firmware version 1.72 Document is under internal review.	DRAFT NOT RELEASED
11 Mar 2014	Draft version. Compatible with application firmware version 1.81 Requirement identification tags are added for traceability purposes. Functional safety related to the auxiliary steering device is not detailed. Document is under internal review. Document is not reviewed by independent organization.	0.9 DRAFT NOT RELEASE
01 May 2014	Draft version. Compatible with application firmware version 1.82 Section Architecture for de-energize for on-road operation is revised. Section 4.3, 8.10, 8.11, 7.2, 0, 7.2.3, 14.1	0.91 DRAFT NOT RELEASE
13 May 2014	Traceability tags are added. Review #472	0.93 DRAFT NOT RELEASE
05 Sep 2014	Reliability calculations on road-switch architecture is under revision. This document is under preparation for submission for assessment by TÜV.	0.94 DRAFT NOT RELEASE
22 Oct 2014	Prepared for PVED-CLS application software version 1.91 Section 17 Safe parameterization is added.	0.95 DRAFT NOT RELEASE
04 Feb 2015	Prepared for PVED-CLS application software version 1.92 Section 13.5 and 13.9 Auto-steering disengage by steering wheel functionality is changed. Section 9.1 COV self-test execution times are updated. Section 7.2, 0 and 7.2.3System diagrams are corrected. Section 13.14 on safe auto-calibration stop is corrected (steering wheel movement).	0.96 DRAFT NOT RELEASE
17 Apr 2015	Prepared for PVED-CLS application software version 1.93. Section 4.3 is corrected. Note on minimum time-out values is added. Section 18 on System integration is added. Section 20.4 on Identification via PLUS+1 Service tool is added. Section 20.5 on J1939 software identification and component identification is added. Section 9.4 on main spool monitoring is added. Review #µ70.	0.97 Submitted to TÜV Awaits assessment
28-04-2015	Section 15 is extended with advice on CAN message safety protocol.	0.98
28-04-2015	Section 0: Explicit reaction time is added for the valves as notes.	0.99
09-09-2015	Section 4.1: Safety requirement level is corrected to 3. Section 9.5: Fault Detection Algorithm operation description is added. Section 4.4: The role of the OSP-CX is documented as part of the safe state for EHPS systems.	1.00
05-10-2015	Section **Error! Reference source not found.** TÜV certificate is added.	1.01
20-10-2015	Section 7.1 Updated drawing of PVED-CLS Section 13.14 A warning to the system integrator is added	1.02
15-01-2016	Prepared for PVED-CLS application software version 1.95 SSM tag inconsistency is corrected. Section 0 SSM tag changed to 055. Section 12 SSM tag changed to 056. Section 13.1 SSM tag changed to 057. Section 13.2 SSM tag changed to 058. Section 13.3 SSM tag changed to 059. Section 13.4 SSM tag changed to 060. Section 1.2 Software identification is updated to software version 1.95. Section 8.9 Wording; GPS is replaced with auto-guidance controller. Section 5 Safety function overview is reworked. Section 13.13 on Vehicle speed flow scaling on joystick is added.	1.03
21-01-2016	Added SSM_062 & SSM_063 for closed loop joystick to the safety function overview in section 5	1.04
27-01-2016	Section 5 Safety function overview. Mapping of hazardous situations to safety functions is added. Section 15.3 Information on hazard Unintended loss of variable steering is added. Section 9.1.1 5V description on 5V sensor output is added. Section 24.2 Advanced single channel WAS monitoring with FDA is added. Review #1454	1.05
17-02-2016	Section 22 Repair instructions is detailed. Service manuals for OSPE and EHPS valve is added to the document references. SSM_012 is reserved for hardware features. Section 6 is empty and deleted. Section 8.8.2 Vehicle speed sensor sub-system monitoring is detailed further. Review #1454	1.06
30-05-2016	Revision history moved to back of document. Section 7.2 Auxiliary steering device sensor sub-system SSM_017 has been changed to Open loop auxiliary steering device sensor sub-system SSM_017, and is now concerning the mini-steering wheel and open loop joystick sub-systems. Section 7.3 Closed loop auxiliary steering device sensor sub-system SSM_064 has been added. Section 7.4 Safe closed loop joystick engage SSM_063 has been added.	1.96.1

	In section 12.9 tag SSM_036 the description of parameter P3240 has been changed. In section 12.10 tag SSM_037 the description of parameter P3240 has been changed. Section 12.11 Auto-guidance disengage by AUX steering device (closed loop joystick) SSM_065 has been added. In section 12.5 tag SSM_032 the numbering of the operation points has been corrected. Section 16.1 PCB Overheating shut-down SSM_043 has been changed to include a description of the parameter temperature severity level. Section 7.13 Bootloader version check SSM_066 has been added. Diagram in section 7.8 Vehicle Speed Sensor SSM_021 updated. Diagram in section 7.9 Auto-guidance sub-system SSM_022 updated. Diagram in section 7.10 Road-switch (for OSPE valve) SSM_023 updated. Diagram in section 7.11 Road-switch (for EHPS valve) SSM_024 updated. Diagram in section 7.12 Man Machine INTERFACE (MMI) SSM_025 updated. Diagram in section 8.4 Steering status CAN message SSM_029 updated. Diagram in section 8.1 Cut-off valve (OSPE valve systems) SSM_026 updated. Diagram in section 24.2 Appendix B - Advanced single channel WAS diagnostic with FDA updated. Section 12.16 Vehicle speed dependent wheel angle limitation (Auxiliary closed loop joystick) SSM_062 added. SSM_061 Vehicle speed dependent flow scaling (auxiliary joystick) changed to SSM_061 Vehicle speed dependent flow scaling (open loop auxiliary joystick). Out of calibrated range has been added in section 7.5 Wheel angle sensor (WAS) – Dual channel Analogue SSM_018. Out of calibrated range has been added in section 7.6 Wheel angle sensor (WAS) – CAN basedSSM_019. Out of calibrated range has been added in section 7.7 Wheel angle sensor (WAS) – Single channel Analogue SSM_020. FDA description added in section 7.6 Wheel angle sensor (WAS) – CAN basedSSM_019. Section 14.4 Loss of EH-flow to one direction has been added. Revision numbering changed to be: [Software version].[document revision number]	
20-06-206	Section 3 on errata information added. Table in 1.2 PVED-CLS Software configuration updated. Changed the wording of the second important note on page 13.	1.96.2
08-08-2016	In the section 8.1.2 Monitoring under 8.1 Steering wheel sensor sub-system SSM_016, the parameter address for the maximum message timeout has been corrected. Wording of section 13.11 Auto-guidance disengage by AUX steering device (closed loop joystick) SSM_065 has been changed, so the description of the safety function is elaborated. In Section 1.2, Time Stamp of software binaries added.	1.96.3
18-08-2016	Software version on front page changed to 1.97. The description of the parameter P3375 in section 8.5.2 Monitoring has been changed to 'Analogue sensor cross-check monitoring. Maximum analogue sensor divergence. Unit is internal resolution [IR] i.e. after scaling.' In section 8.1.2 Monitoring the bullet point about data validation has been updated to include information on the ranges for angle and angular velocity. In section 8.2.1.3 Monitoring - Auxiliary mini-steering wheel the bullet point about data validation has been updated to include information on the ranges for angle and angular velocity. Under the important note in section 9.5.3 FDA parameter tuning, a new bullet point with the note 'In order to prevent the Fault Detection Algorithm from giving false errors form high frequent wheel angle oscillations, the Fault Detection Algorithm will ignore wheel angle oscillations above 6.7Hz' has been added. In the section 8.10.2 Monitoring information on the 100ms delay from AD3 has changed from off-road mode to on-road mode until low-power test pulse pattern starts has been added and marked with an asterisk. The asterisk refers to the following explanation 'the delay of 100ms from the mode has changed to on-road mode until low-power test pulse pattern starts, has been introduced in order to prevent false errors caused by relay-contact bounce' placed at the end of the section. The table in section 5.1 Safety Functions SSM_010 has been updated with the SSM_030 FDA – Fault Detection Algorithm. In the table in section 5.1 Safety Functions SSM_010 under SSM_057 Safe EH steering flow command the Wheel Angle Sensor sub-system has been made optional. Under the important note in section 9.5.3 FDA parameter tuning, a new bullet point with the note 'If the system is configured without a wheel angle sensor, the Fault Detection Algorithm will not be executed' has been added. The section 8.2 Open loop Auxiliary steering device sensor sub-system SSM_017 has been updated with Elobau® and analogue joystick. The following subsections are new: 8.2.2.4 Interface - Elobau® open loop joystick, 8.2.3.1 Interface – Analogue open loop joystick, 8.2.2.6 Monitoring - Elobau® open loop joystick and 8.2.3.3 Monitoring - Analogue open loop joystick. Review #1838.	1.97.1

12-01-2017	The paragraph number of the references to the section FDA – Fault Detection Algorithm has been corrected throughout the document.	1.97.2
19-01-2017	Cosmetic change important note and recommendation in section 12 Vehicle speed EH steering shut-off SSM_056. Important note and recommendation added in section 4.4 Safe state SSM_006. Changed wording in important note in section 0 Analogue interface. Changed wording in important note in section 8.5.2 Monitoring. Updated Service pages revision for 1.97 firmware to Service pages 1.97 revision D	1.97.3
25-01-2017	Corrections according to review #2104.	1.97.4
29-03-2017	Updated for software version 1.98 - only binary file names and P1d file updated. - no review required.	1.98.1
07-08-2017	Updated for software 2.00. EHi-H functionality added. Corrections according to review #2445.	2.00.1
26-09-2017	SEHS-2819 Section 4: PFHd values are corrected per IEC61508 ed. 1 1oo2 formula.	2.00.2
13-11-2017	Corrections according to review #2445. PVED-CLS Software configuration SSM_000 updated.	2.00.3
23-11-2017	Information on P3395 added in **Error! Reference source not found.** Information on MMI lockout added in; Auto-guidance sub-system SSM_022 Open loop Auxiliary steering device sensor sub-system SSM_017 Closed loop Auxiliary steering device sensor sub-system SSM_064	2.00.4

24 Appendixes

24.1 APPENDIX A - GENERAL SPECIFICATIONS

Further information on valve sub-systems and general specifications can be found on the Danfoss homepage via following link:
HTTP://POWERSOLUTIONS.DANFOSS.COM/PRODUCTS/STEERING/PVED-CLS-INTELLIGENT-STEERING-SUB-SYSTEM/

24.2 APPENDIX B - ADVANCED SINGLE CHANNEL WAS DIAGNOSTIC WITH FDA

It may be possible to obtain a diagnostic coverage of 90 % for a single channel WAS sub-system by applying FDA monitoring as shown in sector 8.7. FDA monitoring may be applied as a reference sensor for the WAS. The principle in FDA is to verify that all sensor inputs are working in a correlated way i.e. that the WAS is moving to the right when the valve is steering out flow to the right direction. Similar, the WAS must not move when the valve is not steering out flow. See section 9.5 for details on FDA.

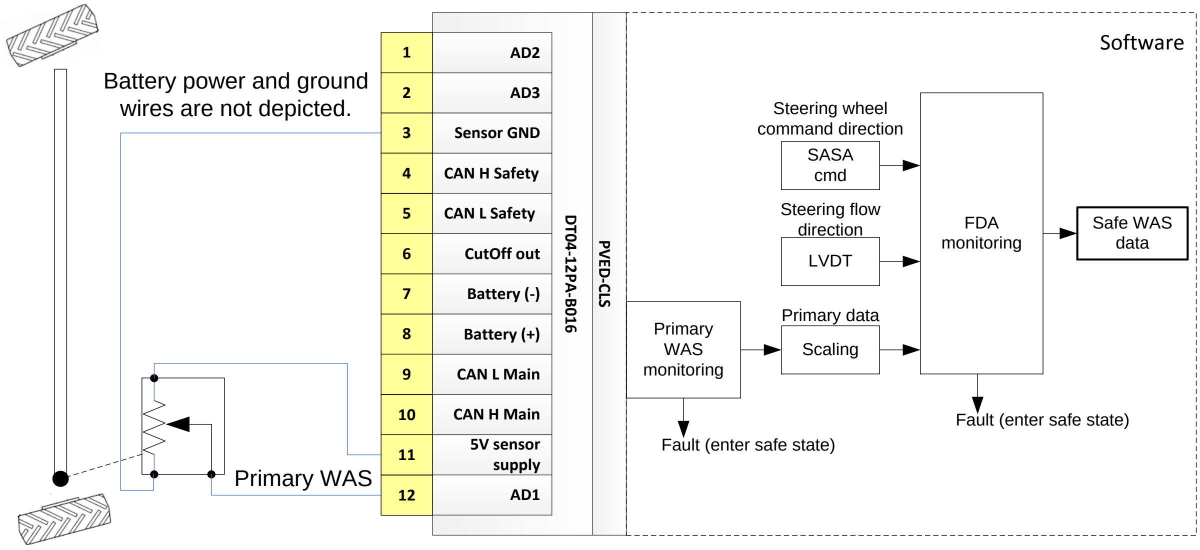


Figure 40: Single channel WAS sub-system (with FDA).

Operation

In comparison to applying a redundant WAS for diagnostic purposes, where the absolute wheel angle position is monitored by a comparison principle, single channel WAS monitoring by FDA relies on a sensor movement and direction comparison with a reference sensor. FDA is performed by both channels in the PVED-CLS. The WAS and EH-valve main spool position sensor outputs Left, right and neutral. FDA monitoring works in all off-road steering wheel modes, on-road mode, safe on-road mode and auto-guidance mode.

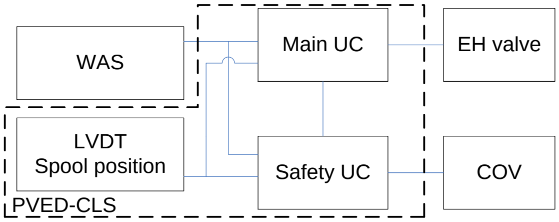


Figure 41: Single channel WAS interface with FDA monitoring.

Example calculation

The WAS shall be supplied by a 3rd party. The architecture conforms to category 3. Identical channels are assumed. The WAS is included in both channels even though it is physically only present on one channel.
For reliability calculation, the following safety related block diagram shows an EH-steering system for auto-guidance and variable steering.

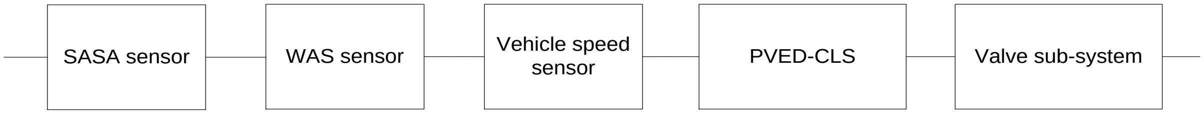


Figure 42: Safety related block diagram.

- The target AgPLr is d
- The MTTFd,ch for the entire channel must be better than 10 years (medium) for a category 3 architecture.
- The DCavg must be ≥ 90 % (for ISO25119 DCavg must be ≥ 60 %).
- The MTTFd for the vehicle speed sub-system and the WAS are example value. Refer to the 3rd party supplier for precise values.
- The CAN bus takes less than 1 % of SIL2 due to the applied safety protocol and is thus omitted for all sensors.

The PVED-CLS operates as a monitoring device for the electro-mechanical channel. The following diagnostic coverage can be used for the calculation:

Sub-system monitoring	DC	Description
PVED-CLS, OSPE valve	95 %	Resulting DC per PVED-CLS FMEDA. Lowest number is applied for both channels.
SASA	99 %	The SASA sensor is monitored by a comparison cross-check of SASA channel 1 and 2
Vehicle speed sensor	99 %	The vehicle speed sensor sub-system is monitored by a comparison cross-check of vehicle speed channel 1 and 2.
WAS	90 %	The WAS movement and direction is compared to the EH-valve main spool position which is used as a reference sensor. The movement and direction checking is done on the states Left movement, Right movement and neutral.

The PVED-CLS safety related specifications are described in section 4.1.

Channel 1,2 elements	MTTFd [years]	DC [%]
SASA	73	99
WAS (example)	50	90
Vehicle speed sensor (example)	50	99
PVED-CLS, OSPE valve	36	95
MTTFd,ch	**12**	
DCavg		**95**

Refer to ISO 13849 for calculation of MTTFd,ch and DCavg.

The MTTFd,ch and the DCavg fulfills the requirement for meeting AgPL d with a category 3 architecture.

Attention

⚠

The system integrator shall:

- Design the WAS sub-system.
- Ensure that the sub-system components are fit for the purpose.
- Conduct an FMEA to uncover dangerous failures.

- Implement measures against dangerous failures.
- Perform a CCF analysis.
- Document the sub-system as part of the safety case if it analyzed to be part of the safety function.
- Tune the FDA parameters.
- Ensure that the use of FDA for WAS monitoring works as expected.
- Perform safety validation on the architecture.
- Ensure that the fault reaction time and residual fault effect for FDA WAS monitoring is acceptable.

Important

The fault reaction time is the time where a fault is present (potentially resulting in a dangerous condition) till it is detected and contained i.e. system is brought to a safe state.