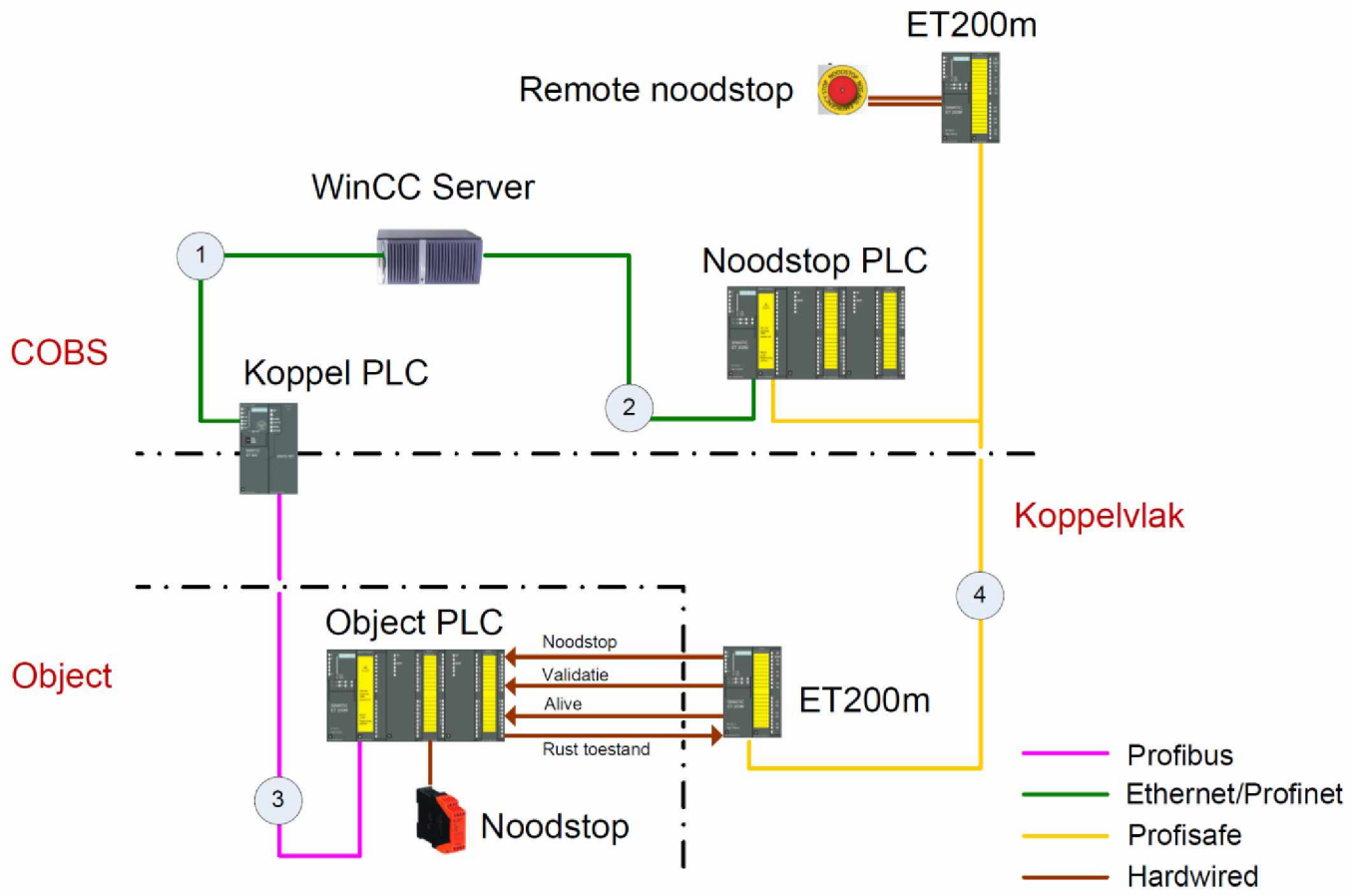


Project name	**640700 IAP Waternet**
Safety standard	EN/IEC 62061:2005 + COR:2010
Author	5.1,2,e
Company name	
Company address	
Version	1.2
Creation date	October 22, 2013 2:54:22 PM CEST
Last saved date	December 17, 2013 12:52:59 PM CET
Comment	
Pilz PAScal	Version v1.6.3 Build6

Using Version 3.1 of the calculation algorithm in accordance with EN ISO 13849-1
Using Version 3.0 of the calculation algorithm in accordance with EN/IEC 62061

Validatie Noodstopkoppeling volgens IEC 62061

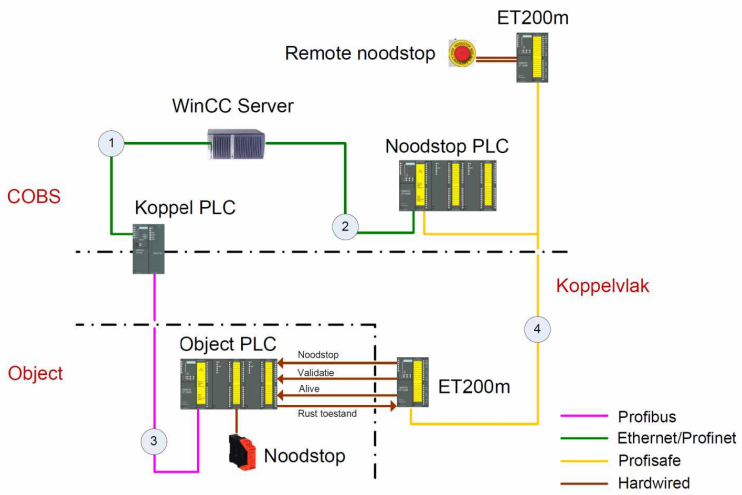
De IEC 61508 (Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES). is met name gericht aan de fabrikant van veiligheidscomponenten. Deze norm vormt daarnaast de basis voor de verder uitgewerkte normen die specifiek gericht zijn aan een bepaalde branche. De IEC 62061 (Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems) is gericht aan de samensteller van een veiligheidssysteem voor machines. Deze norm is specifiek gericht op de machinebranche.

Aangezien de brug aangemerkt wordt als zijnde machine (volgens de Machinerichtlijn 2006/42/EG) en het systeem (afstandsbediening) een 'applicatie' is van veiligheidscomponenten dient gevalideerd te word of het systeem voldoet aan de eisen gesteld in deze 'applicatie' norm, de IEC 62061.

Gebruikte componenten

Op basis van onderstaande data (behaald uit de aangeleverde databladen door IAP) zijn de gegevens in deze berekening gebaseerd. Deze databladen zijn afkomstig van de betreffende leverancier van de componenten.

Data:	Component:					
Fabrikant	Moeller	Siemens	Siemens	Siemens	Siemens	Phoenix
Type	M22	SM326 DI	CPU 417	Profisafe	SM 326 DO	PSR-SCF
SIL Claim Limit	3*	3	3	3	3	3
PFHd	-	$1{,}0 \cdot 10^{-9}$	$5{,}3 \cdot 10^{-9}$	$1{,}0 \cdot 10^{-9}$	$1{,}0 \cdot 10^{-9}$	$2{,}02 \cdot 10^{-9}$
MTTFd	-	-	-	-	-	-
B10d	100000	-	-	-	-	-
Mission Time	20 jaar	20 jaar	20 jaar	20 jaar	20 jaar	20 jaar
	* SIL CL is drie door de gebruikte redundante architectuur PFH en MTTF volgen uit de berekening	*MTTFd en B10d niet aanwezig, SIL Claim limit en PFHd zijn leidend*				

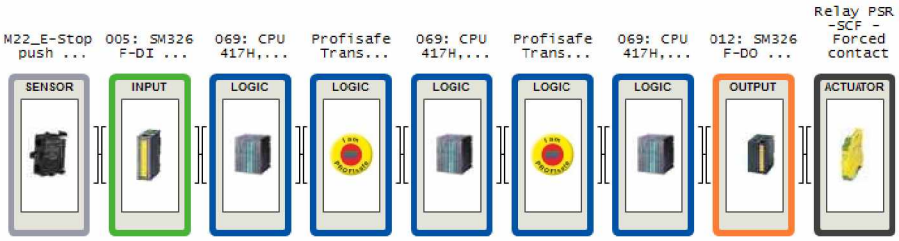


Deze validatie richt zich op de koppeling tussen de remote noodstop, beheer door de noodstop PLC en doorgave naar de remote module bij de object PLC. Bij de object PLC is een hardwired koppeling die niet in deze validatie wordt meegenomen.

SRCF overview

System/Module	Target SIL	Result	CCF Factor	PFHd	SIL/PFHd	SILCL	Reached SIL
Noodstopkoppeling	3	Target Achieved	0.10	2.05E-08	3	3	3

Details: Noodstopkoppeling



Name	Noodstopkoppeling
Comment	SIL 3 niveau is door OG aangegeven Architectuur uitgevoerd, dubbelkanalig inclusief terugkoppeling en kortsluitdetectie. Uitgangspunten 1 x per week bediening van de noodstopfunctie Dagen per jaar operationeel 365 Uren per dag operationeel 24 De noodstopafhandeling verloopt via een remote IO systeem naar een lokale noodstopPLC die de juiste noodstop doorgeeft aan het remote IO systeem bij de brug. De verbinding tussen de PLC's is middels een veilige netwerkverbinding
Target SIL	3
Result	Target Achieved
CCF Factor	0.10
PFHd	2.05E-08
SIL/PFHd	3
SILCL	3
Reached SIL	3

CCF result

	Point(s):0/105
	No (0)
1a	No (0)
1b	No (0)
2	No (0)
3	No (0)
	No (0)
4	No (0)
5	No (0)
6	No (0)
7	No (0)
	No (0)
8	No (0)
	No (0)
9	No (0)
10	No (0)
	No (0)
11	No (0)
	No (0)
12	No (0)
13	No (0)

Subsystem details: Noodstopkoppeling

Subsystem	Type	Number of physical elements/channels	Application	Version	Operating hours per day	Operating days per year	Time between two operations	T1: Proof test interval [year(s)]	T2: Diagnostic test interval [hour(s)]	Mission time [year(s)]	W co
Subsystem 1	Sensor	One						20	168		
M22_E-Stop push button, all Types[1] [***]			E-Stop push button, all Types (0) - Dual channel	1.0	24	365	1 week(s)	-	-	20.00	D ac
Subsystem 2	Input	One						-	-		
005: SM326 F-DI 24, (6ES7326-1BK02-0AB0), 2kanalig # SM326 F-DI 24, (6ES7326-1BK02-0AB0), two channel 1.0 - Dual-channel[2] [***]			Dual-channel	1.0				-	-	20.00	N
Subsystem 3	Logic	One						-	-		
Comment	Lokale noodstop PLC Ingang op desk bij bedienaar										
069: CPU 417H, (6ES7417-4HT14-0AB0) # CPU 417H, (6ES7417-4HT14-0AB0) 1.0 - Dual-			Dual-channel	1.0				-	-	20.00	N

channel[3] [***]											
Subsystem 4	Logic	One						-	-		
Profisafe Transmission[4] [***]			Profisafe Bus Error	All versions				-	-	20.00	N
Subsystem 5	Logic	One						-	-		
Comment	Noodstop PLC										
069: CPU 417H, (6ES7417-4HT14-0AB0) # CPU 417H, (6ES7417-4HT14-0AB0) 1.0 - Dual-channel[3] [***]			Dual-channel	1.0				-	-	20.00	N
Subsystem 6	Logic	One						-	-		
Profisafe Transmission[4] [***]			Profisafe Bus Error	All versions				-	-	20.00	N
Subsystem 7	Logic	One						-	-		
Comment	Lokale noodstop PLC uitgang										
069: CPU 417H, (6ES7417-4HT14-0AB0) # CPU 417H, (6ES7417-4HT14-0AB0) 1.0 - Dual-channel[3] [***]			Dual-channel	1.0				-	-	20.00	N
Subsystem 8	Output	One						-	-		
012: SM326 F-DO 8, (6ES7326-			Dual-channel	1.0				-	-	20.00	N

2BF41-0AB0) # SM326 F-DO 8, (6ES7326-2BF41-0AB0) 1.0 - Dual-channel[5] [***]											
Subsystem 9	Actuator	One						20	0		
Relay PSR-SCF - Forced contact[6] [***]			Relay PSR-SCF SIL 3 Application	1.0				-	-	20.00	N

[***]Replace the components after the specified number of years. Please include this in your user manual.

[Number] : See component data for details

Component data

Number	Component Type	Name	Application	Version	B10d	MTTFd [year(s)]	PFHd [per hour]	SILCL	λd / λ (% of dangerous failures)	Wiring configuration required	Bus connection required
1	Moeller	M22_E-Stop push button, all Types	E-Stop push button, all Types (0) - Dual channel	1.0	100,000	-	-	-	20.00%	Yes	No
2	SM326	005: SM326 F-DI 24, (6ES7326-1BK02-0AB0), 2kanalig # SM326 F-DI 24, (6ES7326-1BK02-0AB0), two channel 1.0 - Dual-channel	Dual-channel	1.0	-	-	1.0E-9	3	-	No	No
3	CPU	069: CPU 417H, (6ES7417-4HT14-0AB0) # CPU 417H, (6ES7417-4HT14-0AB0) 1.0 - Dual-	Dual-channel	1.0	-	-	5.3E-9	3	-	No	No

		channel									
4	Siemens	Profisafe Transmission	Profisafe Bus Error	All versions	-	-	1.0E-9	3	-	No	No
5	SM326 F-DO8	012: SM326 F-DO 8, (6ES7326-2BF41-0AB0) # SM326 F-DO 8, (6ES7326-2BF41-0AB0) 1.0 - Dual-channel	Dual-channel	1.0	-	-	1.0E-9	3	-	No	No
6	Phoenix	Relay PSR-SCF - Forced contact	Relay PSR-SCF SIL 3 Application	1.0	-	-	2.02E-11	3	-	No	No

Attachments

Attachment:	Eaton-263467-M22-PVT-nl_NL.pdf
Attachment Description:	Datablad Eaton Noodstop drukknop
Attached to:	PAScal Project: 640700 IAP Waternet
Attachment:	PSR-...-24DC-FSP-2X1-1X2.pdf
Attachment Description:	Datablad Phoenix Interfacerelais
Attached to:	PAScal Project: 640700 IAP Waternet
Attachment:	S7300FS_e.pdf
Attachment Description:	Datablad Siemens PLC
Attached to:	PAScal Project: 640700 IAP Waternet

CCF questions (EN/IEC 62061)

ID	Group	Question
1a	Separation / segregation	Are SRECS signal cables for the individual channels routed separately from other channels at all positions or sufficiently shielded?
1b		Where information encoding/decoding is used, is it sufficient for the detection of signal transmission errors?
2		Are SRECS signal and electrical energy power cables separated at all positions or sufficiently shielded?
3		If subsystem elements can contribute to a CCF, are they provided as physically separate devices in their local enclosures?
4	Diversity / redundancy	Does the subsystem employ different electrical technologies for example, one electronic or programmable electronic and the other an electromechanical relay?
5		Does the subsystem employ elements that use different physical principles (e.g. sensing elements at a guard door that use mechanical and magnetic sensing techniques)?
6		Does the subsystem employ elements with temporal differences in functional operation and/or failure modes?
7		Do the subsystem elements have a diagnostic test interval of <= 1 min?
8	Complexity / design / application	Is cross-connection between channels of the subsystem prevented with the exception of that used for diagnostic testing purposes?
9	Assessment / analysis	Have the results of the failure modes and effects analysis been examined to establish sources of common cause failure and have predetermined sources of common cause failure been eliminated by design?
10		Are field failures analysed with feedback into the design?
11	Training / competence	Do subsystem designers understand the causes and consequences of common cause failures?
12	Environmental Control	Are the subsystem elements likely to operate always within the range of temperature, humidity, corrosion, dust, vibration, etc. over which it has been tested, without the use of external environmental control?
13		Is the subsystem immune to adverse influences from electromagnetic interference up to and including the limits specified in Annex E?

Questions about risk analysis (EN/IEC 62061)

Risk parameter	Examination	Evaluation
Severity	Severity of injury	Irreversible: death, losing an eye or arm Irreversible: broken limb(s), losing a finger(s) Reversible: requiring attention from a medical practitioner Reversible: requiring first aid
Frequency/Duration	Duration of exposure < 10 minutes? Frequency and duration of exposure to the hazard	 An hour or less Between an hour and a day Between a day and two weeks Between two weeks and a year More than a year
Occurrence	Probability of occurence of dangerous event	Very high Likely Possible Rarely Scarcely possible
Avoidance	Probability of avoiding or limiting harm	Impossible Rarely Likely

END USER DISCLAIMER FOR PASCAL

The PAScal calculation tool can help you to define the Performance Level in accordance with EN ISO 13849-1 and the SIL in accordance with EN/IEC 62061. Additional requirements of the standards (e.g. requirements for safety-related software and systematic safety integrity) must be considered separately. Knowledge and correct application of the relevant standards and directives, in particular EN ISO 13849-1, EN/IEC 62061 and IEC 61508 are therefore a requirement for using this tool. Warranty and liability claims will be rendered invalid if damages can be attributed to a failure to follow the guidelines in the operating manual, if the libraries used are not current, or if the user of this software is not suitably qualified.
All calculations are made in accordance with the current status of the standards and to the best of our knowledge and belief.

The following libraries are used to calculate the safety functions:

Library	Vers
SIEMENS1_Undefined subsystem type_EN	1.0

Use only libraries of trusted sources. Make sure to verify the origin of the used libraries. Confirm the device data against documentation and certificates provided by device manufacturers.
Please note: Latest versions of the libraries in PAScal format are available on:www.pilz.com/PAScal_Lib
Libraries in other formats are typically available directly on the device manufacturers' web sites.

PAScal is a tool produced by Pilz

Pilz GmbH & Co. KG Sichere Automation
Felix-Wankel-Straße 2
73760 Ostfildern
Germany
Tel.: 5.1,2,e
Fax: 5.1,2,e
Web: www.pilz.de