Leeswijzer

Bevindingen Onderzoek Functie “Noodstop”

Sluiscomplex “Zandkreek” & “Grevelingen”

**Inleiding**

Bijgaand treft u de rapportage “Bevindingen onderzoek noodstop Grevelingen en Zandkreeksluizen” aan. Dit betreft een interne bedrijfsrapportage van Rijkswaterstaat en is bedoeld om aan te geven welke technische problematiek hier speelt (speelde) en welk handelingsperspectief bestaat.

**Context Onderzoek**

Rijkswaterstaat is, in het kader van Informatie Beveiliging (cyber security), een uitvoeringsprogramma gestart om informatie(-systemen) te beveiligen tegen misbruik, spionage en uitval. Het onderdeel IMpuls-Programma Aanpak Kritieke Technische infrastructuur (IMPAKT) heeft tot doel om per infrastructuur object de automatisering en (informaite-)beveiliging te verbeteren. IMPAKT bezoekt hiertoe RWS objecten, brengt risico’s (kwetsbaarheden) en maatregelen in kaart en geeft hier uitvoering aan.

**Scope Onderzoek**

Het bijgaande onderzoeksrapport van IMPAKT beschrijft de bevindingen van kwetsbaarheden in de technische installaties van de Grevelingen en Zandkreeksluizen, zowel van de bediening op afstand als de installaties op locatie. Daarbij is getoetst aan technische kaders en vigerende wet- en regelgeving. Het onderzoek beschrijft niet de aspecten mens en organisatie[[1]](#footnote-1) en proces[[2]](#footnote-2).

**Context bevindingen**

De bevindingen moeten worden gezien als een interne rapportage over de aangetroffen technische kwetsbaarheden in de noodstopvoorziening en zijn erop gericht om de Rijkswaterstaat dienstverlening te verbeteren. Een aantal nuances is daarbij niet aangebracht. Zo is bijvoorbeeld niet in ogenschouw genomen hoe de processen tussen techniek, bedienaar en (vaar-)weggebruiker zijn geregeld. De daarvoor bestaande instructies en procedures mitigeren grotendeels het risico van het technisch falen van (onderdelen van) de noodstopvoorziening.

Bevindingen

Onderzoek Functie “Noodstop”

 Sluiscomplex

“Zandkreek” & “Grevelingen”

Projectleider: Pascal de Groot (CIV)

Auteurs: Pascal de Groot (CIV) ism Pilz Nederland

Getoetst door oa: Leon Uijttewaal (CIV) – Ketenmanager Bediening Beweegbare Objecten

Vastgesteld door: Olaf van Duin (CIV) – Programmadirecteur Beveiligd Werken RWS

Uitgiftedatum: 16.05.2014

Versienummer: 1.0

Status: Definitief

Inhoud

[1 Inleiding 4](#_Toc387383878)

[2 Bevindingen Noodstoptest Sluiscomplex “Zandkreek” 5](#_Toc387383879)

[2.1 Kenmerken 5](#_Toc387383880)

[2.2 Samenvatting 5](#_Toc387383881)

[2.2.1 Kritische bevindingen m.b.t. veiligheid 5](#_Toc387383884)

[2.2.2 Kritische bevindingen m.b.t. beschikbaarheid: 6](#_Toc387383885)

[2.3 Risico 7](#_Toc387383886)

[2.3.1 Actueel risico (IST-waarde) 7](#_Toc387383887)

[2.3.2 Restrisico (SOLL-waarde) 7](#_Toc387383888)

[2.4 Voorgestelde maatregelen 8](#_Toc387383889)

[3 Bevindingen Noodstoptest Sluiscomplex “Grevelingen” 9](#_Toc387383890)

[3.1 Kenmerken 9](#_Toc387383891)

[3.2 Samenvatting 9](#_Toc387383892)

[3.2.1 Kritische bevindingen m.b.t. veiligheid 9](#_Toc387383893)

[3.2.2 Kritische bevindingen m.b.t. beschikbaarheid: 9](#_Toc387383894)

[3.3 Risico 11](#_Toc387383895)

[3.3.1 Actueel risico (IST-waarde) 11](#_Toc387383896)

[3.3.2 Restrisico (SOLL-waarde) 11](#_Toc387383897)

[3.4 Voorgestelde maatregelen 12](#_Toc387383898)

[4 Bijlage: Korte beschrijving 14-punten risicograaf 13](#_Toc387383899)

# Inleiding

Tijdens de inspecties van het programma “IMPAKT” is de goede en veilige werking noodstopfunctie van de Sluiscomplexen “Grevelingen” en Zandkreek” onderzocht. De bevindingen hiervan zijn vastgelegd in dit document.

Aan de hand van een studie van de technische tekeningen en door middel van het fysiek testen is de noodstopfunctie geverifieerd en gevalideerd. De uitkomst hiervan is dat de noodstopfunctie, wettelijk gezien, niet betrouwbaar genoeg is. Als gevolg hiervan is er geen garantie, dat wanneer ingrijpen op het proces met de noodstop noodzakelijk is deze ook werkelijk functioneert.

De basisprincipes bij het ontwerpen van een systeem, is dat bij falen van een component, dit niet mag leiden tot een onveilige situatie. Zowel het ontwerp als de gebruikte componenten voldoen niet aan deze basisprincipes.

# Bevindingen Noodstoptest Sluiscomplex “Zandkreek”

## Kenmerken

* Sluis tussen het Veersemeer en de Oosterschelde, bestaande uit 1 kolk met dubbele puntdeuren. Over beide sluishoofden ligt een beweegbare brug in de 1e deltaweg (80 km/u).
* Het complex wordt regulier vanuit het Topshuis bediend en is lokaal voorzien van een Scada-bediening die identiek is aan die in het Topshuis.
* In de besturingsruimte van het bediengebouw is een noodbediening aanwezig voor de sluiskolk, hierbij is er geen zicht op de bewegende delen van de installatie.
* In de besturingsruimten van de bruggen is een noodbediening aanwezig, waarbij geen zicht op het verkeer en de bewegende delen aanwezig is.

De noodbediening wordt alleen in die situaties gebruikt, wanneer de reguliere en onderhoudsbediening niet meer functioneert en het niet meer mogelijk is om het sluiscomplex in de gewenste toestand te brengen.

## Samenvatting

Uit de bevindingen die gedaan zijn tijdens de analyse van de documentatie, de schouw en de noodstoptest kan geconcludeerd worden dat:

* de veiligheid voor (vaar)weggebruikers en onderhoudspersoneel in het kader van de wettelijke zorgplicht voor de beheerder is niet in alle situaties gewaarborgd,
* bij falen van de noodstopfunctie is de kans dat het object langdurig niet beschikbaar is, groot.

Bovenstaande aspecten maken direct ingrijpen noodzakelijk.

### Kritische bevindingen m.b.t. veiligheid

* Het noodstopsysteem is niet betrouwbaar en niet conform beproefde veiligheidsprincipes[[3]](#footnote-3) uitgevoerd. Dat blijkt uit de volgende bevindingen:
	+ De noodstop vanuit de “Bediening op Afstand” en de lokale bediening lopen via de niet fail-safe PLC/componenten. Dit betekent dat de maximale betrouwbaarheid van deze noodstop niet voldoet aan de normen: Categorie B van EN954-1, SIL classificatie cf NEN-EN-IEC 62061 of de PL cf NEN-EN-ISO 13849.
	Als gevolg hiervan is er geen garantie, dat wanneer ingrijpen op het proces met de noodstop noodzakelijk is deze ook werkelijk functioneert.
	+ Wanneer de “Bediening op Afstand” is geactiveerd functioneert de lokale noodstop niet.
	Dit betekent dat een bedienaar of onderhoudspersoneel op locatie aanwezig is niet in staat is in te grijpen als hij een ongewenste situatie ziet ontstaan.
	+ In het noodstopcircuit is een interface relais aanwezig die de werking van de noodstop vanuit de “Bediening op Afstand” en lokaal overbrugd. Dit relais is niet voorzien van enige vorm van diagnose en is voorzien van een handmatige overbruggingsfunctie.
	Door deze oplossing is het mogelijk dat de noodstop in het geheel niet functioneert.
	+ De afsluitbomen zijn niet opgenomen in het noodstop circuit, zowel dalend als openend. Hierdoor is het voor de bedienaar onmogelijk in te grijpen mocht er een gevaarlijke situatie ontstaan tijdens het bewegen van de afsluitbomen.
	Bij deze installatie is de kans op het ontstaan van gevaarlijke situaties extra groot aangezien het proces al lang loopt voordat de bomen werkelijk gaan dalen.
	+ De noodstopcircuits van de verschillende deelinstallaties zijn niet gekoppeld. Als op de noodstop van de besturingsruimte van de brug wordt gedrukt stopt het sluisproces niet. Vanuit deze positie is wel zicht op de sluis en niet op de brug.
	Door onbekendheid bij potentiële gebruikers van deze noodstopfunctie, kan dit een risico zijn voor (vaar)weggebruiker en onderhoudsaannemer.
	+ Wanneer de noodstop in een van de machinekelders wordt geactiveerd tijdens het nivelleren, starten de nivelleerschuiven automatisch na het uittrekken van de noodstopdrukker.
	Voor mensen op locatie is het niet duidelijk dat er een beweging wordt gestart.
	+ Bij een noodstop tijdens het openen van de binnendeuren stopt de beweging, maar lukt het niet meer om na een bediencommando de binnendeuren te laten bewegen. Op het moment dat de buitendeuren bediend gaan worden dan bewegen de buitendeuren wel, maar gaan ook zonder waarschuwing de binnendeuren mee bewegen.
	Onverwacht bewegen van sluisdeuren kan een risico zijn voor vaarweggebruiker en onderhoudsaannemer.

### Kritische bevindingen m.b.t. beschikbaarheid

* Als een noodstop via de “Bediening op Afstand” wordt ingeslagen tijdens het bewegen van de brug aan het Veersemeer, moet de storing in de besturingsruimte van de sluis worden gereset. Dit betekent een lange stilstand.
* Elektrische schema’s zijn niet up to date en bevatten met name op het gebied van het noodstopcircuit tegenstrijdigheden. Dit betekent kans op langere stilstand.

## Risico

Beweegbare infrastructuur objecten zijn grote machines waarbij het, net als bij b.v. liften, niet onmogelijk is dat er als gevolg van een ongeval dodelijke slachtoffers te betreuren zijn.” Het enige wat wij als beheerder kunnen doen is de kans op een ongeval zo klein mogelijk te maken door zowel procesmatig als technisch voorzorgsmaatregelen te treffen.

Het risiconiveau op falen van de functie “noodstop” is voor zowel de “actuele situatie” als “na uitvoering van de beheersmaatregelen” bepaald aan de hand van de Risico Inventarisatie Evaluatie instrument “14-punten risicograaf”. Dit Instrument is gericht op de machine en de interactie van bediener met de machine en is een praktisch en kwalitatief hoogstaande methode voor de bepaling van het risiconiveau.

### Actueel risico (IST-waarde)

Het risico op “Falen noodstopfunctie” krijgt een score van 14 op basis van de 14-punten risicograaf (zie bijlage). Wat als zeer hoog gecategoriseerd wordt.

Hierbij zijn de volgende scores gegeven:

* Effect 3 (Dood).

Het optreden van het risico kan ongevallen met ernstig letsel of de dood tot gevolg hebben.

* Blootstelling 2 (vaak tot continu)

Vaar- en weggebruikers worden continu blootgesteld aan het mogelijke gevaar.

* Waarschijnlijkheid 3 (falen kan vaak voorkomen, maar hoeft niet tegelijk op te treden met de aanleiding op basis waarvan de noodstop wordt ingedrukt).
* Gevaarafwending 2 (Nauwelijks mogelijk)

Technisch: de noodstopfunctie is zowel bij “Bediening op Afstand” als lokale bediening, technisch gezien onbetrouwbaar.

Gedrag: de bedienaren denken langer na over het gebruik van een noodstop.

### Restrisico (SOLL-waarde)

Het risico op “Falen noodstopfunctie” krijgt na uitvoeren van de beheersmaatregelen (tot en met korte termijn) een score van 9 op basis van de 14-punten risicograaf (zie bijlage). Wat als hoog gecategori-seerd wordt.

Hierbij zijn de volgende scores gegeven:

* Effect 3 (Dood).

Het effect blijft gelijk aan IST, omdat dit bij een beweegbare brug en/of een schutsluis niet is te veranderen, wel wordt de kans van optreden verlaagd door de beheersmaatregelen uit te voeren*.*

* Blootstelling 2 (vaak tot continu)

Blijft gelijk aan IST: Vaar- en weggebruikers worden continu blootgesteld aan het mogelijke gevaar.

* Waarschijnlijkheid 1

Verlaagd door uitvoeren beheersmaatregelen, omdat dan sprake is van een betrouwbaarder systeem, maar score blijft qua gedrag afhankelijk van o.a. alertheid bedienaar en gebruiker.

* Gevaarafwending 1 (mogelijk onder bepaalde omstandigheden)

Veranderd: is lager geworden door betrouwbaarder systeem, maar blijft qua gedrag afhankelijk van oa alertheid bedienaar en gebruiker.

## Voorgestelde maatregelen

Hieronder wordt in termijnen aangeven, hoe het risico tot een acceptabel niveau wordt beperkt.

**Direct**

* Organisatorisch
	+ Management communiceert dat het geaccepteerd is dat er na het drukken van een noodstop een storing ontstaat met langdurige hinder voor de gebruikers. Dit leidt tot minder twijfel bij het bediend personeel om een noodstop te gebruiken en dat dit niet als negatief wordt beoordeeld.
	+ Niet bedienen tijdens onderhoudswerkzaamheden aan de bewegingswerken en elektrotechnische installaties aangezien de lokale noodstop op de bedienplek niet functioneert (tijdens “Bediening op Afstand”).

**Korte termijn (binnen 2 weken)**

* Organisatorisch
	+ Alleen nog bedienen via het lokale bediensysteem. De verbinding tussen het complex en het Topshuis loopt via een niet fail-Safe verbinding hierdoor is de werking van de noodstop vanuit de “Bediening op Afstand” niet gegarandeerd.
	+ Bedienend personeel dient geïnstrueerd te worden over de aanpassingen aan de noodstop functionaliteit.
* Technisch
	+ Aanpassen noodstopcircuit van de noodstop op de lokale werkplek. De noodstop op de lokale werkplek dient hard bedraad opgenomen te worden. Op deze manier wordt de betrouwbaarheid van het noodstopcircuit verhoogd.
	+ Noodstopdrukkers in de kelders van de sluisaandrijving toevoegen zodat aan beide zijden van de motor een noodstop ter beschikking is. Hierdoor is het niet meer noodzakelijk in het gevaarlijke gebied te kruipen voor dat de noodstop bereikbaar is.

**Middellange termijn (binnen 4 maanden)**

* Organisatorisch
	+ Actualiseren van de handleidingen en bedienend personeel instrueren over de aanpassingen aan de noodstop functionaliteit. De noodstopfunctionaliteit opnemen in de bedieningshandleidingen.
	+ Actualiseren/opstellen van werkinstructies en onderhoudspersoneel instrueren zodat er veilig aan de installatie gewerkt kan worden. Hierbij dient o.a. duidelijk gemeld te worden dat na het herstellen van een noodstop ingezette bewegingen, zonder opnieuw een commando te geven, spontaan door kunnen gaan.
	+ De noodstoppen periodiek (jaarlijks) tijdens bewegingen testen. Dit dient opgenomen te worden in het onderhoudscontract. Voor het uitvoeren van noodstoptest kan de testmodule gebruikt worden die opgeleverd is door het Impakt-team.
* Technisch
	+ T.b.v. noodstop functionaliteit dient de “Bediening op Afstand” verbinding vervangen door een die via een minimaal gecertificeerd SIL2 protocol communiceert, zodat de noodstop op afstand kan voldoen aan de benodigde betrouwbaarheid.

**Lange termijn**

* Programmeren; het voldoen aan de machinerichtlijn, zodat de machine volledig voldoet aan de wet en regelgeving.

#  Bevindingen Noodstoptest Sluiscomplex “Grevelingen”

## Kenmerken

* Sluis tussen het Grevelingenmeer en de Krammer, bestaande uit 1 kolk met dubbele puntdeuren. Over beide sluishoofden ligt een beweegbare brug in de N59 (80 km/u).
* Het complex wordt regulier vanuit het Topshuis bediend en is lokaal voorzien van een Scada-bediening die identiek is aan die in het Topshuis.
* In de besturingsruimte van het bediengebouw is een noodbediening aanwezig voor de sluiskolk, hierbij is er geen zicht op de bewegende delen van de installatie.
* In de besturingsruimten van de bruggen is een noodbediening aanwezig, waarbij ook geen zicht op het verkeer en de bewegende delen aanwezig is.

De noodbediening wordt alleen in die situaties gebruikt, wanneer de reguliere en onderhoudsbediening niet meer functioneert en het niet meer mogelijk is om het sluiscomplex in de gewenste toestand te brengen.

## Samenvatting

Uit de bevindingen die gedaan zijn tijdens de analyse van de documentatie, de schouw en de noodstoptest kan geconcludeerd worden dat:

* de veiligheid voor (vaar)weggebruikers en onderhoudspersoneel in het kader van de wettelijke zorgplicht voor de beheerder is niet in alle situaties gewaarborgd,
* bij falen van de noodstopfunctie is de kans dat het object langdurig niet beschikbaar is groot.

Bovenstaande aspecten maken direct ingrijpen noodzakelijk.

### Kritische bevindingen m.b.t. veiligheid

* Het noodstopsysteem is niet betrouwbaar en niet conform beproefde veiligheidsprincipes uitgevoerd. Dat blijkt uit de volgende bevindingen:
	+ De noodstop vanuit de “Bediening op Afstand” en de lokale bediening lopen via niet fail-safe PLC/componenten. Dit betekent dat de maximale betrouwbaarheid van deze noodstop niet voldoet aan de normen: Categorie B van EN954-1, SIL classificatie cf NEN-EN-IEC 62061 of de PL cf NEN-EN-ISO 13849.
	Als gevolg hiervan is er geen garantie dat wanneer ingrijpen op het proces met de noodstop noodzakelijk is deze ook werkelijk functioneert. Wanneer de bediening op afstand is geactiveerd functioneert de lokale noodstop niet.
	Dit betekent dat een bedienaar of onderhoudspersoneel, die op locatie aanwezig is niet in staat is in te grijpen als hij een ongewenste situatie ziet ontstaan.
	+ De noodstopcircuits van de verschillende deelinstallaties zijn niet gekoppeld, alleen de noodstop op de lokale bediening en van “Bediening op Afstand” heeft invloed op het volledige complex.
	Door onbekendheid bij potentiële gebruikers van deze noodstopfunctie, kan dit een risico zijn voor (vaar)weggebruiker en onderhoudsaannemer.
	+ Tijdens de noodstoptest van de afsluitbomen viel afsluitboom 2 circa 1 meter naar beneden.

### Kritische bevindingen m.b.t. beschikbaarheid:

* Een noodstop tijdens het openen van de afsluitbomen resulteert in het vastlopen van het stappenprogramma van de brug PLC. De enige mogelijkheid om hier uit te komen is de afsluitbomen via het handmatig bedienen van de relais op te sturen. Als de bomen eenmaal op zijn pakt de besturing automatisch (zonder verdere reset) het afbouwen weer op.
* De brug aan de Grevelingenzijde maakt zeer bedenkelijke mechanische geluiden tijdens het openen van de brug.
* Een groot aantal storingen in de aandrijving van de Grevelingenbrug worden niet weergegeven op het scada systeem. Hierdoor is het lastig snel een diagnose te stellen, een voorbeeld hiervan is geen status vermelding van een geactiveerde noodstopdrukker.
* Wanneer na het sluiten van de afsluitbomen te snel het commando brug openen wordt gegeven gaat de frequentieregelaar in storing. Het Scada systeem krijgt hier geen melding van en laat de aansturing staan.
* PLC programma is niet afgestemd op de hardware hierdoor ontstaan deadlock situaties.

## Risico

Beweegbare infrastructuur objecten zijn grote machines waarbij het, net als bij b.v. liften, niet onmogelijk is dat er als gevolg van een ongeval dodelijke slachtoffers te betreuren zijn.” Het enige wat wij als beheerder kunnen doen is de kans op een ongeval zo klein mogelijk te maken door zowel procesmatig als technisch voorzorgsmaatregelen te treffen.

Het risiconiveau op falen van de functie “noodstop” is voor zowel de “actuele situatie” als “na uitvoering van de beheersmaatregelen” bepaald aan de hand van de Risico Inventarisatie Evaluatie instrument “14-punten risicograaf”. Dit Instrument is gericht op de machine en de interactie van bediener met de machine en is een praktisch en kwalitatief hoogstaande methode voor de bepaling van het risiconiveau.

### Actueel risico (IST-waarde)

Het risico op “Falen noodstopfunctie” krijgt een score van 14 op basis van de 14-punten risicograaf (zie bijlage). Wat als zeer hoog gecategoriseerd wordt.

Hierbij zijn de volgende scores gegeven:

* Effect 3 (Dood).

Het optreden van het risico kan ongevallen met ernstig letsel of de dood tot gevolg hebben.

* Blootstelling 2 (vaak tot continu)

Vaar- en weggebruikers worden continu blootgesteld aan het mogelijke gevaar.

* Waarschijnlijkheid 3 (falen kan vaak voorkomen, maar hoeft niet tegelijk op te treden met de aanleiding op basis waarvan de noodstop wordt ingedrukt).
* Gevaarafwending 2 (Nauwelijks mogelijk)

Technisch: de noodstopfunctie is zowel bij “Bediening op Afstand” als lokale bediening, technisch gezien onbetrouwbaar.

Gedrag: de bedienaren denken langer na over het gebruik van een noodstop.

### Restrisico (SOLL-waarde)

Het risico op “Falen noodstopfunctie” krijgt na uitvoeren van de beheersmaatregelen (tot en met korte termijn) een score van 9 op basis van de 14-punten risicograaf (zie bijlage). Wat als hoog gecategori-seerd wordt.

Hierbij zijn de volgende scores gegeven:

* Effect 3 (Dood).

Het effect blijft gelijk aan IST, omdat dit bij een beweegbare brug en/of een schutsluis niet is te veranderen, wel wordt de kans van optreden verlaagd door de beheersmaatregelen uit te voeren.

* Blootstelling 2 (vaak tot continu)

Blijft gelijk aan IST: Vaar- en weggebruikers worden continu blootgesteld aan het mogelijke gevaar.

* Waarschijnlijkheid 1

Verlaagd door uitvoeren beheersmaatregelen, omdat dan sprake is van een betrouwbaarder systeem, maar score blijft qua gedrag afhankelijk van o.a. alertheid bedienaar en gebruiker.

* Gevaarafwending 1 (mogelijk onder bepaalde omstandigheden)

Veranderd: is lager geworden door betrouwbaarder systeem, maar blijft qua gedrag afhankelijk van oa alertheid bedienaar en gebruiker.

## Voorgestelde maatregelen

Hieronder wordt in termijnen aangeven, hoe het risico tot een acceptabel niveau wordt beperkt.

**Direct**

* Organisatorisch
	+ Management communiceert dat het geaccepteerd is dat er na het drukken van een noodstop een storing ontstaat met langdurige hinder voor de gebruikers. Dit leidt tot minder twijfel bij het bediend personeel om een noodstop te gebruiken.
	+ Niet bedienen tijdens onderhoudswerkzaamheden aan de bewegingswerken en elektrotechnische installaties, aangezien de lokale noodstop op de bedienplek niet functioneert (tijdens “Bediening op Afstand”).

**Korte termijn (binnen 2 weken)**

* Organisatorisch
	+ Alleen nog bedienen via het lokale bedien systeem. De verbinding tussen het complex en het Topshuis loopt via een niet fail-Safe verbinding hierdoor is de werking van de noodstop vanuit de “Bediening op Afstand” niet gegarandeerd.
	+ Bedienend personeel dient geïnstrueerd te worden over de aanpassingen aan de noodstop functionaliteit.
* Technisch
	+ Aanpassen noodstopcircuit van de noodstop op de lokale werkplek. De noodstop op de lokale werkplek dient hard bedraad opgenomen te worden. Op deze manier wordt de betrouwbaarheid van het noodstopcircuit verhoogd.
	+ De aandrijving van afsluitboom 2 controleren.

**Middellange termijn (binnen 4 maanden)**

* Organisatorisch
	+ Actualiseren van de handleidingen en bedienend personeel instrueren over de aanpassingen aan de noodstop functionaliteit. De noodstopfunctionaliteit opnemen in de bedieningshandleidingen.
	+ Actualiseren/opstellen van werkinstructies en onderhoudspersoneel instrueren zodat veilig aan de installatie gewerkt kan worden. Hierbij dient o.a. duidelijk gemeld te worden dat na het herstellen van een noodstop ingezette bewegingen, zonder opnieuw een commando te geven, spontaan door kunnen gaan.
	+ De noodstoppen periodiek (jaarlijks) tijdens bewegingen testen. Dit dient opgenomen te worden in het onderhoudscontract. Voor het uitvoeren van noodstoptest kan de testmodule gebruikt worden die opgeleverd is door het Impakt-team.
* Technisch
	+ T.b.v. noodstop functionaliteit dient de “Bediening op Afstand” verbinding vervangen door een die via een gecertificeerd SIL2 protocol communiceert, zodat de noodstop op afstand kan voldoen aan de benodigde betrouwbaarheid.
	+ De onderhoudsaannemer laten onderzoeken waarom de afsluitbomen na het indrukken van de noodstop in storing vallen. In overleg met de beheerder en het IPM team stelt de onderhoudsaannemer een verbetervoorstel op.

**Lange termijn**

* Programmeren; het voldoen aan de machinerichtlijn, zodat de machine volledig voldoet aan de wet en regelgeving.

# Bijlage: Korte beschrijving 14-punten risicograaf

1. Mens: bedienaar, (vaar-)weggebruiker en onderhoudsmedewerker. Organisatie onderdelen, -taken en

-verantwoordelijkheden. [↑](#footnote-ref-1)
2. Bedienprotocollen en (vaar-)wegvoorschriften. [↑](#footnote-ref-2)
3. Voor de gebruikte componenten is geen faalwijze in geval van een interne fout gespecificeerd. Dit betekent dat het component geen component volgens beproefde veiligheidsprincipes is (zoals gedefinieerd in NEN-EN ISO 13849-2). [↑](#footnote-ref-3)