

1 Over dit document

titel FMEA functies van ETCS aan boord
Maatregelen voor het verbeteren van RAMS van ETCS aan boord
Functional failure list ETCS aan boord



author OPTM team materieel :
xxx

Programma ERTMS

reference
version 0.5a

The information in this document has been compiled with the greatest possible care.
Nevertheless, no rights can be derived from this.
The ERTMS Programme reserves the right to alter this document at any time

2 Doel van dit document

Dit document geeft een overzicht van:

- 1) Het effect van falen van de functies van ETCS aan boord van het materieel op de operationele treindienst
- 2) Maatregelen voor het voorkomen van functie uitval
- 3) Maatregelen welke de impact op de operationele dienstst reduceren (bij functie uitval)
- 4) Mogelijke 'functional failures'

Belangrijk is dat de maatregelen opgepakt worden. Veel maatregelen zijn geborgd door een requirement in het PVE Materieel. Per maatregel wordt verwezen naar de bijbehorende requirements, vanuit de requirement (Polarion) wordt verwezen naar de bijbehorende maatregel.

3 Versiebeheer

datum	versie	locatie van wijzigingen	omschrijving van wijzigingen
2-11-2017	0.1	alles	Initiële versie
24-11-2017	0.2	Tabblad FMEA en maatregelen	De FMEA vanuit Word naar Excel verplaatst en volledig herzien. Tabblad 'functional failure' toegevoegd
	0,3		Referenties bij maatregelen vermeld.
3-1-2018	0,4	Functional failure list FMEA	FFL herzien.
20-03-2018	0,5	Functional failure list FMEA	Deel TIM aangepast + opmerkingen redigeer sessie 19/03/2018 verwerkt
22-1-2020	0.5a	alle tabs	Geanonimiseerd t.b.v. publicatie

ID	Functie	Functie omschrijving	Oorzaak	Merkbaar door?	Effect op de trein	Functional failure Foutcategorie (voor toepassen maatregel)	Maatregelen	Functional failure Foutcategorie (na toepassen maatregel)	Effect van toepassen maatregelen
1	EVC (niet in sleeping mode)	Centrale besturing van ETCS.	Softwarefout Voeding defect Hardware defect	System failure op DMI Diagnosemelding op TDD	Zowel bij ATB als L2 wordt de trein stilgezet d.m.v. een snelremming. Gebruikersproces 'Rijden in isolation mode' wordt actief.	ATB: No protection FC01 ETCS L2: No protection FC01	M2, Reduceert impact, ETCS reset knop M3, Reduceert impact, Snelheid op DMI in 'isolation mode' M4, Voorkomt falen, Software quality assurance M6, Reduceert impact, Cold movement detector	ATB: Reduced speed FC01 ETCS L2: No protection FC01	ATB: FC02 (snelheidsmeter blijft beschikbaar, rijden met 80 km/u). Regelgeving is rijden tot het eerste knooppunt. Dus trein valt uit. Dus FC01. ETCS L2: - Reset is effectief: FC02 / FC03 (afhankelijk van snelheid en positie trein op het moment van optreden) - Reset is niet effectief of niet zinvol: FC01 Met effectieve controle op de kwaliteit van de software wordt de kans op softwarefouten kleiner.
2	EVC (in sleeping mode)	Centrale besturing van ETCS.	Softwarefout Voeding defect Hardware defect	System failure op DMI Diagnosemelding op TDD	Zowel bij ATB als L2 wordt de trein stilgezet d.m.v. een snelremming. Machinist dient ETCS installatie te isoleren in achteroplopende cabines/treinstellen.	ATB No traction / EB FC01 ETCS L2 No traction / EB FC01	M4, Voorkomt falen, Software quality assurance M5, Reduceert impact, Monitoring & diagnose M15, Reduceert impact, Geen EB in sleeping mode	ATB: No function loss FC03 ETCS L2: No function loss FC03	ATB / ETCS L2: FC03 (geen EB meer bij een defect in 'sleeping mode') Met effectieve controle op de kwaliteit van de software wordt de kans op softwarefouten kleiner. De diagnose/monitoring functie zorgt er voor dat het defect vroegtijdig bekend is en geacteerd kan worden op een defect in een toekomstig 'bediend treinstel'.
3	ATB-STM	ATB baan signalen lezen en verwerken. EB bij afwezigheid remdetectie. EB bij te snel naderen rood sein (ATB v) Informatie doorgeven aan de machinist (bijv. ATB foutcode en blauwgedrukt)	Hardware defect Software fout Voeding	ATB snelremming System failure op DMI Diagnosemelding op TDD	ATB: Trein wordt stilgezet d.m.v. snelremming. L2: geen effect Voorwaarde: ATB uitgevoerd als STM.	ATB: No protection FC01 ETCS L2: No function loss FC03	M3, Reduceert impact, Snelheid op DMI in 'isolation mode' M7, Voorkomt falen, Inlezen en verwerken ATB buiten bedrijf door ETCS M13, Reduceert impact, Defect STM ATB heeft geen invloed functioneren L2	ATB: Reduced speed FC01 ETCS L2: No function loss FC03	ATB: FC01 (snelheidsmeter blijft beschikbaar, rijden met 80 km/u) ETCS L2: - Defect in opgetreden op ATB baanvak: FC03 (geen functieseries) - Defect opgetreden op L2 baanvak: FC03
4	ATB-STM Spoel	Oppikken en doorgeven van de ATB baancode	ATB baancode wordt niet meer doorgegeven	Spoel defect Bekabeling defect	ATB: melding en max. 40 km/h. Mogelijk ook uitval ATBv. L2: niet merkbaar, pas wanneer de trein in ATB gebied komt, wordt de storing merkbaar. Machinist zal de STB-ATB isoleren en met maximaal 80 km/u de rit vervolgen.	ATB Reduced speed FC01 ETCS L2: No function loss FC03		ATB Reduced speed FC01 ETCS L2: No function loss FC03	
5	GSM-R modem (inclusief antennes) Euroradio	Fysiek tot stand brengen en houden van een GSM-R verbinding naar de wal. Verzenden van EVC berichten over GSM-R en het ontvangen van RBC berichten over GSM-R.	Voeding defect Hardware defect: Slecht signaal Interferentie met UMTS banden Verkeerde parametrisering	Uitval één modem en overname binnen T_NVContact: - diagnose melding op TDD Uitval één modem en geen overname binnen T_NVContact: - diagnose melding op TDD - verlies radio contact symbool op DMI Verlies radio contact RBC (walprobleem, software probleem, uitval alle modems of Euroradio) - diagnose melding op TDD - verlies radio contact symbool op DMI Uitval GSMR modems in ATB bedrijf	Mogelijk functie verlies bij RBC transitie. Een bedrijfsremming wordt ingezet. De verwachting is dat verbinding terug is (de remming opgeheven wordt) voordat de trein stilstaat. Wanneer geen verbinding met de RBC meer mogelijk is, kan de trein rijden in SR of IS. Welke mode procedureel toegestaan is, moet vastgesteld worden in het gebruikersoverleg tussen ProRail en NS (xxx). Mogelijk kan een reset helpen om het contact terug te krijgen. Onduidelijk. Leverancier afhankelijk. Mogelijk een system failure	ATB & ETCS L2 No function loss FC03 ATB & ETCS L2 No function loss FC03 ATB & ETCS L2 No protection FC01 ATB: No protection FC01	M8, Voorkomt falen, Monitoren verborgen defect M10, Voorkomt falen, 1 modem handover bij RBC overgang M9, Voorkomt falen, Goed modem management M10, Voorkomt falen, 1 modem handover bij RBC overgang M20, Reduceert impact, Inrichten ketenmonitoring / beheer M5, Reduceert impact, Monitoring & diagnose M11, Voorkomt falen, Eisen van subset 93 M1, Voorkomt falen, Geen system failure bij ATB only M20, Reduceert impact, Inrichten ketenmonitoring / beheer	ATB & ETCS L2 No function loss FC03 ATB & ETCS L2 No function loss FC03 ATB & ETCS L2 No protection FC01 ATB: No function loss FC03	ETCS L2 - Goede diagnose: defecte modem wordt gemeld aan de onderhouder: voorkomt een FC01 ETCS L2 - blijft FC03. Alleen de vertraging wordt minder ETCS L2 Deze faalmodus heeft een relatie met het falen van het GSMR netwerk. Een defecte GSM-R netwerk is niet direct eenduidig te scheiden van een defect in de GSM-R modems. Keten monitoring + beheer helpt beide partijen het onderhoud effectiever en efficiënter in te richten en sneller eventuele structurele problemen op te lossen: geen uitval/foutcategorie ATB Geen systeemfailure. FC03. De diagnose/monitoring functie zorgt er voor dat het defect vroegtijdig bekend is en geacteerd kan worden op een defect in een toekomstig 'bediend treinstel'.
6	TIU compleet of defecte ingangen	Inlezen van informatie van trein naar EVC, bijv. remsysteem, tractie installatie, cabine selectie, rijrichting, sleeping, etc. Aansturen van functies in de trein.	voeding hardware defect defecte buskoppeling defect ingangen sleeping, etc. Software falen	System failure op DMI Diagnosemelding op TDD	Zowel bij ATB als L2 wordt de trein stilgezet d.m.v. een snelremming. Gebruikersproces 'Rijden in isolation mode' wordt actief.	ATB & ETCS L2 No protection FC01	M12, Voorkomt falen, RAMS eisen -> doel redundantie M8, Voorkomt falen, Monitoren verborgen defect	ATB & ETCS L2 No protection FC01	ETCS L2 + ATB - door strenge RAMS eisen wordt de leverancier (waarschijnlijk) gedwongen tot het toepassen van redundantie: FC03 - door deze redundantie is het belangrijk dat verborgen defecten gemonitord worden: voorkomt een FC01.
7	TIU: tractie-vrijgave + feed back loop	Extra redundant pad voor uitschakelen van de tractie vrijgave.	Defecte uitgang + stuurcircuit	Tractie wordt ongewenst uitgeschakeld: - geen aanzet koppel Tractie wordt ongewenst niet uitgeschakeld: - diagnosemelding op TDD	De machinist kan niet rijden met de trein: gestrande trein. Geen	ATB & ETCS L2 No traction FC01 n.v.t.	M5, Reduceert impact, Monitoring & diagnose M14, Reduceert impact, TIU: outputs - IS mode	ATB & ETCS L2 No traction FC01 n.v.t.	ETCS L2: - diagnose zorgt ervoor dat de machinist weet dat de ETCS installatie de oorzaak is voor het ontbreken van de tractievrijgave en deze dient te isoleren. Bij de isolatie komt de tractievrijgave weer terug: minder vertraging bij FC01.
8	TIU: emergency brake commando + feed back loop	Het geven van een emergency brake (EB).	Een output defect. Veiligheid kritische randapparatuur defect	Onterecht geen EB: - Melding op DMI - Diagnosemelding op TDD Onterecht een EB - Lege treinleiding	Remtest wordt niet gehaald (dit leidt tot een blokkering van de tractievrijgave). Trein is niet inzetbaar. Onterechte remming: De machinist ervaart een lege treinleiding zonder aanleiding.	ATB & ETCS L2 No traction FC01 ATB & ETCS L2: Emergency brake FC01	M5, Reduceert impact, Monitoring & diagnose	ATB & ETCS L2 No traction FC01 ATB & ETCS L2: Emergency brake FC01	ETCS L2 + ATB De diagnose functie van TCMS signaleert dat de ETCS de oorzaak is en adviseert de ETCS in 'isolation mode' te schakelen: minder vertraging bij FC01.

ID	Functie	Functie omschrijving	Oorzaak	Merkbaar door?	Effect op de trein	Functional failure Foutcategorie (voor toepassen maatregel)	Maatregelen	Functional failure Foutcategorie (na toepassen maatregel)	Effect van toepassen maatregelen
9	TIU: service brake + feed back loop	Het geven van een service brake.	Defecte uitgang + stuurcircuit	Onterecht geen service brake: - Een emergency brake.	Geen commando: ETCS detecteert dat de service brake niet functioneert en volgt met een emergency brake/system failure. Wordt ook gecontroleerd bij de remtest. Onterecht commando: Een maximale service brake zonder aanleiding.	ETCS L2: No protection FC01 An unexpected service brake FC01	M21, Reduceert impact, geen system failure bij defect servicebrake. M5, Reduceert impact, Monitoring & diagnose	ETCS L2: Emergency brake instead of service brake FC01 An unexpected service brake FC01	ETCS L2 De machinist is gewend dat de servicebrake ingrijpt. Een emergency brake is ingrijpend en leidt tot een stilstaande trein. Dit is reden voor vertraging. ETCS L2 + ATB De diagnosefunctie signaleert dat de ETCS een onterechte service brake activeert en adviseert de ETCS in 'isolation mode' te schakelen: minder vertraging bij FC01.
10	TIU: stroom-afnemer aansturing + feed back loop	Het omlaag/omhoog sturen van de stroomafnemer	Defecte uitgang + stuurcircuit	Onterecht geen omlaag commando: - Stroom afnemer gaat niet automatisch omlaag Onterechte omlaag commando: - Stroomafnemer gaat niet omhoog	Beperkt, machinist kan ook een commando via DMI geven. Ingrijpend. Trein niet inzetbaar.	ETCS L2: No automatic pantograph control FC03 ATB & ETCS L2 No pantograph up commando possible FC01	M5, Reduceert impact, Monitoring & diagnose M14, Reduceert impact, TIU: outputs - overbrugging	ETCS L2: No automatic pantograph control FC03 ATB & ETCS L2 No automatic pantograph control FC02	De diagnosefunctie informeert de machinist over dit defect. De machinist weet dat hij/zij de stroomafnemer zelf aan dient te sturen: voorkomt verwarring ETCS L2 + ATB Na deactivering van de pantograaf aansturing vanuit ETCS kan het treinstel weer ingezet worden
11	TIU: snelschakelaar aansturing + feed back loop	Het uit en inschakelen van de snelschakelaar	Defecte uitgang + stuurcircuit	Onterecht geen snelschakelaar uit commando: - Snelschakelaar gaat niet uit Onterecht snelschakelaar uit commando: - Snelschakelaar gaat niet in	Beperkt, machinist kan ook een commando via DMI geven. Ingrijpend. Trein niet inzetbaar.	ETCS L2: No automatic circuit breaker out control FC03 ATB & ETCS L2: No circuit breaker in commando possible FC01	M5, Reduceert impact, Monitoring & diagnose M14, Reduceert impact, TIU: outputs - overbrugging	ETVS L2: No automatic circuit breaker out commando FC03 ATB & ETCS L2: No automatic circuit breaker out commando FC02	De diagnosefunctie informeert de machinist over dit defect. De machinist weet dat hij/zij de snelschakelaar zelf uit dient te schakelen: voorkomt verwarring ETCS L2 + ATB Na deactivering van de snelschakelaar aansturing vanuit ETCS kan het treinstel weer ingezet worden
12	Odometer	snelheidsbepaling bevestigen rijrichting afstandsbeplanning van de trein tot aan de LRBG	Voeding Hardware defect Asgever Radar Optische sensor (door vervuiling) Weersomstandigheden Instelfout Confidence level mal function Enkelvoudige fout	Uitval voeding/ odometer compleet of system failure door afwijkende snelheidsmetingen (bijvoorbeeld door weersomstandigheden): - system failure op DMI - diagnosemelding op TDD Onjuiste / onnauwkeurige snelheidsmeting door onjuiste configuratie / weeromstandigheden: - afwijkend gedrag	Zowel bij ATB als L2 wordt de trein stilgezet d.m.v. een snelremming. Gebruikersproces 'Rijden in isolation mode' wordt actief. - afwijkende afstanden met release speed - missen van balises - onverwachte remmingen	ATB & ETCS L2: No protection FC01 ETCS L2: An unexpected TRIP FC01	M2, Reduceert impact, ETCS reset knop M16, Voorkomt falen, Bewaking confidence level M17, Reduceert impact, Bewaking wielband correctie	ATB & ETCS L2: No protection FC01 ETCS L2: An unexpected TRIP FC01	ETCS L2 + ATB Een system failure kan komen als door weeromstandigheden de odometrie volledig in de war is (door slip). Een ETCS reset kan hierbij helpen: FC02 ETCS L2 Diagnose op het correct functioneren van de odometrie maakt inzichtelijk dat deze afwijkt, afwijkend gedrag is hieraan te relateren. De afwijking wordt sneller verholpen.
13	BTM	Ontvangen van telegrammen van balises en deze combineren tot een boodschap van een balisegroep, tijdstempel toevoegen. (Met het tijdstempel wordt de odometer geijkt.) Controle van een balisegroepsbericht op compleetheid en correctheid. Bepalen van de locatie en identiteit van balises.	voeding BTM defecte antenne defecte kabel geen / verminkt bericht	BTM functie uitgevallen en detectbaar door EVC: - system failure op DMI - diagnosemelding op TDD BTM functie uitgevallen en niet detectbaar door EVC (antenne defect): - Trip of servicebrake met melding balise fout op DMI - diagnosemelding op TDD Balise defect: - mogelijk trip of servicebrake met melding balise fout op DMI - diagnosemelding op TDD Berichten gemist (inconsistent door EMC of BTM functies tijdelijk uitgevallen): - Trip of servicebrake met melding balise fout op DMI - diagnosemelding op TDD	Zowel bij ATB als L2 wordt de trein stilgezet d.m.v. een snelremming. Gebruikersproces 'Rijden in isolation mode' wordt actief. Unlinked balise groep: - Geen effect Linked balise groep: - 'linking reaction': geen reactie, TRIP of service brake, twee keer balise groep missen: service brake. Unlinked balise groep: - Geen effect Linked balise groep: - 'linking reaction': geen reactie, TRIP of service brake Unlinked balise groep: - service brake Linked balise groep: - 'linking reaction': geen reactie, TRIP of service brake	ATB & ETCS I2: No protection FC01 ETCS I2: An unexpected service brake FC02 ETCS I2: An unexpected service brake FC02 ETCS I2: An unexpected service brake FC02	M1, Voorkomt falen, Geen system failure bij ATB only (defect GSMR / BTM) M5, Reduceert impact, Monitoring & diagnose M20, Reduceert impact, Inrichten ketenmonitoring / beheer M20, Reduceert impact, Inrichten ketenmonitoring / beheer M20, Reduceert impact, Inrichten ketenmonitoring / beheer	ATB: No function loss FC03 ETCS I2: No protection FC01 ETCS I2: An unexpected service brake FC02 ETCS I2: An unexpected service brake FC02 ETCS I2: An unexpected service brake FC02	ATB Gewenst is dat bij STM-ATB bedrijf bij een defect geen 'system failure' komt op het moment dat de machinist 'STM-ATB only' heeft gekozen. Dit voorkomt een FC01. ETCS L2 Met behulp van keten monitoring worden defecten in het materieel en in de infra beter geduid en effectiever/snelhersteld. ETCS L2 Met behulp van keten monitoring worden defecten in het materieel en in de infra beter geduid en effectiever/snelhersteld. ETCS L2 Met behulp van keten monitoring worden defecten in het materieel en in de infra beter geduid en effectiever/snelhersteld.
14	DMI	Geen mogelijkheid tot interactie tussen ETCS en machinist.	voeding DMI hardware defect software defect	Scherf wordt zwart of staat vast.	Zowel bij ATB als L2 wordt de trein stilgezet d.m.v. een snelremming. Gebruikersproces 'Rijden in isolation mode' wordt actief.	ATB & ETCS L2: No protection FC01	M18, Reduceert impact, Redundante DMI	ATB & ETCS L2: Temporarily no DMI FC02	ETCS L2 + ATB Uitgangspunt is dat het materieel voorzien wordt van een redundant scherm. Bij een defect dient omgeschakeld te worden naar een redundant scherm. Dit kan binnen 10 minuten. Dus fout wordt FC02.
15	Recorder	Verzamelen, opslaan en terugvinden van treininformatie van ETCS en ATB (en overige systemen)	voeding JRU hardware defect software defect	Niet merkbaar	Geen	ATB & ETCS L2: No function loss FC03	M5, Reduceert impact, Monitoring & diagnose	ATB & ETCS L2: No function loss FC03	ETCS L2 + ATB Met behulp van diagnose wordt het falen zichtbaar voor de onderhoudsorganisatie. Herstelling binnen een bepaalde tijd na optreden.

ID	Funcctie	Funcctie omschrijving	Oorzaak	Merkbaar door?	Effect op de trein	Functional failure Foutcategorie (voor toepassen maatregel)	Maatregelen	Functional failure Foutcategorie (na toepassen maatregel)	Effect van toepassen maatregelen
16	Cold movement detector	Nadat de trein in No power mode is geweest, is de positie informatie beschikbaar. De trein hoeft hierdoor niet in een degraded mode naar een balisegroep te rijden voor een positie referentie.	Hardware defect Voeding CMD	Tijdens de SoM zal de mcN merken dat de positie van de trein niet bekend is. Als de trein is verplaatst tijdens No power komt dezelfde reactie. Voor de mcN is geen onderscheid te maken tussen beide situaties. De storing is zodoende lastig merkbaar.	In bepaalde situaties extra opstarttijd benodigd. Herstelling voordat de situatie voordoet waarbij deze functie opstarttijd verkort.	ATB & ETCS L2: Timeloss by start up ETCS FC02	M5, Reduceert impact, Monitoring & diagnose	ATB & ETCS L2: Timeloss by start up ETCS FC02	ETCS L2 Met behulp van diagnose wordt het falen zichtbaar voor de machinist en onderhoudsorganisatie. Hersteling binnen een bepaalde tijd na optreden.
17	TIM	treintegriteitsfunctie	Hardware defect Voeding Automatische koppeling	Uitval voor aanvang rit: - storing is merkbaar indien mcN wegbekendheid heeft (hij weet op welke trajecten L3 is geïmplementeerd) en het valt hem op dat een kleine icoon op de DMI geen L3 aangeeft. ----- Bij uitval tijdens de rit: - een service brake. ----- Kortdurend uitval of treinlengte is onbekend.	Capaciteitsverlies, vooral bij lage snelheid. Dit kan effect hebben op andere treinen, dit is afhankelijk van de dienstregeling. ----- Tijdens de rit: korte vertraging (FC02) en capaciteitsverlies (vooral bij lage snelheid). ----- Achteroplopende trein moet meer ruimte houden. Vertraging.	ETCS hL3: No hybrid level 3 possible FC02 ----- ETCS hL3: No hybrid level 3 possible FC02 ----- ETCS hL3: train length to long FC03	M5, Reduceert impact, Monitoring & diagnose	ETCS hL3: No hybrid level 3 possible FC02 ----- ETCS hL3: No hybrid level 3 possible FC02 ----- ETCS hL3: train length to long FC03	ETCS L2 Met behulp van diagnose wordt het falen zichtbaar voor de machinist en onderhoudsorganisatie. Hersteling binnen een bepaalde tijd na optreden.
18	Rand-apparatuur t.b.v. data-entry en dynamische remcurve	Treinlengte en remkracht bepaling	hardware defect software defect (TCMS interface)	Defect bij SOM, geen data beschikbaar: - machinist voert handmatig in ----- Defect bij SOM, foutieve data ingevoerd - Machinist kan/moet fout opmerken. ----- Defect tijdens de rit: Op het moment dat dit, volgens de TSI, als automatische data invoer gezien wordt, volgt er een service brake bij een defect tijdens de rit.	Geen dynamische remcurve. Grotere veiligheidsmarges. ----- Veilige fout: - langere remcurve, iets tijdsverlies Onveilige fout: - ??? ----- Service remming of een TRIP. De veiligheids marge op de remcurve wordt vergroot. Dit kan leiden tot een 'TRIP'.	ETCS L2: Only manual data entry FC03 ----- ETCS L2: Only manual data entry FC03 ----- ETCS L2: An unexpected service brake FC02		ETCS L2: Only manual data entry FC03 ----- ETCS L2: Only manual data entry FC03 ----- ETCS L2: An unexpected service brake FC02	

ID	Level	Functional failure	Category
1	ATB & ETCS L2	No pantograph up commando possible	FC01
2	ATB & ETCS L2:	No protection	FC01
3	ATB & ETCS L2:	No traction	FC01
4	ATB & ETCS L2:	Emergency brake	FC01
5	ATB & ETCS L2:	No circuit breaker in commando possible	FC01
6	ATB & ETCS L2:	Temporarily no DMI	FC02
7	ATB:	Reduced speed	FC01
8	ETCS HL3:	No hybrid level 3 possible	FC02
9	ETCS L2:	An unexpected TRIP	FC02
10	ETCS L2:	An unexpected service brake	FC02
11	ETCS L2:	Extra stop of the train	FC02
12	ETCS HL3:	ETCS hL3: train length to long	FC03
13	ETCS L2:	Timeloss by start up ETCS	FC02
14	ETCS L2:	Emergency brake instead of service brake	FC01

ID	Type maatregel	Omschrijving (kort)	Borging	Toelichting	Referentie aanduiding	Kolom1
M1	Voorkomt falen	Geen system failure bij ATB only (defect GSMR / BTM)	ETCS-6643	Op het moment dat de machinist de keuze 'ATB only' maakt mogen defecten in de BTM en in de GMSR modems niet leiden tot een 'system failure'. Belangrijk is wel dat deze systemen actief zijn (bij ATB only) en gediagnosticeerd worden. Zodat defecten voortijdig gemeld en vervolgens afgehandeld kunnen worden.	M1, Voorkomt falen, Geen system failure bij ATB only (defect GSMR / BTM)	
M2	Reduceert impact	ETCS reset knop	ETCS-2028 ETCS-5456	De ervaring is dat een reset van het systeem een software storing kan oplossen. In combinatie met de maximale vereiste opstarttijden kan een ETCS installatie binnen 90 seconden weer operationeel zijn.	M2, Reduceert impact, ETCS reset knop	
M3	Reduceert impact	Snelheid op DMI in 'isolation mode'	ETCS-3558	Op het moment dat de OBE of de STM-ATB faalt, dient in veel gevallen de desbetreffende installatie 'buiten bedrijf' gesteld te worden. Op het moment dat in 'isolation mode' de snelheidsmeter nog actief is, is de impact van het falen minder. De trein kan dan nog (bijvoorbeeld) ingezet worden op ATB baanvakken (max. 80 km u).	M3, Reduceert impact, Snelheid op DMI in 'isolation mode'	
M4	Voorkomt falen	Software quality assurance		De ervaring is dat software falen regelmatig voorkomt bij ETCS. Aandacht aan software kwaliteit in elke fase van het project heeft een positieve invloed. De kans op software falen wordt kleiner.	M4, Voorkomt falen, Software quality assurance	
M5	Reduceert impact	Monitoring & diagnose	3. System Chapter 4	Op het moment dat de machinist/helpdesk snel inzicht heeft de oorzaak van het falen en bijpassende afhandeling spaart dit tijd. De diagnosefunctie van TCMS informatie de machinist over het defect en adviseert een bepaalde handeling. Daarnaast kan de helpdesk m.b.v. monitoring informatie sneller en effectiever helpen.	M5, Reduceert impact, Monitoring & diagnose	
M6	Reduceert impact	Cold movement detector	ETCS-3247	De CMD heeft als taak positieinformatie / balise informatie te onthouden. Hiermee is de laatste positie bij een reset of opstart van het treinstel bekend. Dit scheelt tijd bij het opstarten.	M6, Reduceert impact, Cold movement detector	
M7	Voorkomt falen	Inlezen en verwerken ATB buiten bedrijf door ETCS	ETCS-5776	Zoveel mogelijk ontkoppelen van architectuurontwerp zodat fouten over en weer zo min mogelijk impact hebben. De ETCS installatie dient de status 'ATB buiten bedrijf' in te lezen en zorg te dragen dat onder ETCS L2 er in deze toestand geen 'system failure' komt.	M7, Voorkomt falen, Inlezen en verwerken ATB buiten bedrijf door ETCS	
M8	Voorkomt falen	Monitoren verborgen defect	3. System Chapter 4	Defecten in redundante systeemdelen worden via monitoring gemeld aan de onderhouder. Het defect wordt hersteld. Hiermee wordt functie uitval voorkomen bij een tweede defect.	M8, Voorkomt falen, Monitoren verborgen defect	
M9	Voorkomt falen	Goed modem management	ETCS-5469	Maximaal 1 x van de 1000x mag het voorkomen dat bij een communicatie fout (van één modem) de communicatie met het RBC hinderlijk uitvalt (hiermee wordt afgedwongen dat een defecte modem automatisch overgenomen wordt door de redundante modem).	M9, Voorkomt falen, Goed modem management	
M10	Voorkomt falen	1 modem handover bij RBC overgang	Infra	Mogelijk maken van een 1 modem handover binnen Nederland bij RBC overgangen. Dit is technisch mogelijk, maar moet goed geparametriseerd worden vanuit de infra. Dit is van toepassing bij 'circuit switched' communicatie. Aangezien dit nog gebruikt wordt op terugvalniveau en bij een deel van het park is het belangrijk dat deze eis gesteld wordt aan de infraprovider.	M10, Voorkomt falen, 1 modem handover bij RBC overgang	
M11	Voorkomt falen	Eisen van Subset 93	ETCS-5466	In de PVE wordt de vrijwillige subset (bijv. subset 93) verplicht. Deze subset stelt aanvullende performance eisen aan de GSMR keten	M11, Voorkomt falen, Eisen van Subset 93	
M12	Voorkomt falen	RAMS eisen -> doel redundantie	ETCS-5467 ETCS-5468	Betrouwbaarheid eisen worden zo gedefinieerd dat de leverancier er voor zorg draagt dat enkelvoudig falen niet kan leiden tot functieverlies / uitval.	M12, Voorkomt falen, RAMS eisen -> doel redundantie	
M13	Reduceert impact	Defect STM ATB heeft geen invloed functioneren L2	ETCS-6643	Een defect in de STM mag niet gevolg hebben dat het treinstel niet kan functioneren op een level 2 baanvak.	M13, Reduceert impact, Defect STM ATB heeft geen invloed functioneren L2	
M14	Reduceert impact	TIU: outputs - overbrugging	ETCS-6639 ETCS-6032 ETCS-6030	Belangrijk is dat defecten aan de uitgangen gerelateerd aan 'tractievrijgave' en 'track condities' in 'isolation mode' de inzet van het treinstel niet belemmeren. Dus wel 'tractievrijgave' en geen actieve 'stroomafnemer neer' of 'snelschakelaar uit' commando in de 'isolation mode'.	M14, Reduceert impact, TIU: outputs - overbrugging	
M15	Reduceert impact	Geen EB in sleeping mode	ETCS-3561	Op het dat een ETCS installatie in een gekoppeld treinstel faalt kan deze een snelremming geven. Dit is een hinderlijk storing in de praktijk. Om deze reden is opgenomen in de PVE een defect in 'sleeping mode' niet mag leiden tot een 'snelremming'.	M15, Reduceert impact, Geen EB in sleeping mode	
M16	Voorkomt falen	Bewaking confidence level	ETCS-1575	De diagnosefunctie van de ETCS bewaakt de confidence level. Bij een afwijking volgt een diagnosemelding, hiermee kan de onderhoudsorganisatie proactief handelen.	M16, Voorkomt falen, Bewaking confidence level	
M17	Reduceert impact	Bewaking wielband correctie	ETCS-6301	Bij onderhoud aan de wielen dient vaak een correctiefactor ingevoerd te worden in de odometrie. In het PVE is een eis opgenomen dat een onjuist correctie factor gesignaleerd wordt. Hiermee kan geanticipeerd worden het afwijkende gedrag.	M17, Reduceert impact, Bewaking wielband correctie	
M18	Reduceert impact	Redundante DMI	ETCS-3524	Een redundant beeldscherm in een vereiste om de benodigde RAM performance te halen. Om deze reden is als concrete eis opgenomen.	M18, Reduceert impact, Redundante DMI	
M19						
M20	Reduceert impact	Inrichten ketenmonitoring / beheer	Infra	Een defecte BTM of GSMR aan boord van het materieel is niet direct eenduidig te scheiden van een defect in balise of het GSMR netwerk. Keten monitoring + beheer helpt beide partijen (baan/materieel) het onderhoud effectiever en efficiënter in te richten	M20, Reduceert impact, Inrichten ketenmonitoring / beheer	
M21	Reduceert impact	Geen system failure bij defect servicebrake.	xxx	Het is niet gewenst dat een defecte aansturing van de service brake leidt tot een system failure en isolation mode. In principe is ETCS mogelijk zonder een service brake aansturing. Het is dus niet nodig om naar de 'isolation mode' te schakelen.	M21, Reduceert impact, Geen system failure bij defect servicebrake.	