BIJLAGE VI

Veiligheidsvoorschriften voor complexe elektronische voertuigcontrolesystemen

1. INLEIDING

Deze bijlage bevat de voorschriften en testprocedures voor de veiligheidsaspecten van complexe elektronische voertuigcontrolesystemen.

2. DOCUMENTATIEVOORSCHRIFTEN

2.1. **Algemene voorschriften**

De fabrikant verstrekt een documentatiepakket dat een beschrijving geeft van het basisontwerp van het instrumentele beveiligingssysteem en van de middelen waarmee het verbonden is met andere voertuigsystemen of waarmee het de uitgangsvariabelen direct controleert. De functie(s) van het systeem en het veiligheidsconcept, zoals vastgesteld door de fabrikant, moeten in de documentatie worden toegelicht. Met het oog op inspecties moet de documentatie aangeven met welke middelen de werking van het systeem kan worden gecontroleerd.

De documentatie moet ter beschikking worden gesteld in twee delen:

a) de formele documentatie van het instrumentele beveiligingssysteem met het oog op de goedkeuring, die de in de punten 2.2 tot en met 2.4 vermelde informatie bevat. Zij zal dienen als basisreferentie voor het in punt 3 beschreven goedkeuringsproces;

b) alle aanvullend materiaal en analysegegevens die relevant zijn voor de goedkeuring van het instrumentele beveiligingssysteem.

2.2. **Beschrijving van de functies van het instrumentele beveiligingssysteem**

Er moet een beschrijving worden verstrekt met een eenvoudige verklaring van alle controlefuncties van het instrumentele beveiligingssysteem en de methoden die zijn toegepast om de doelstellingen te verwezenlijken, inclusief een beschrijving van de mechanismen waardoor controle wordt uitgeoefend, d.w.z.:

a) een lijst van alle ingangs- en gemeten variabelen en hun werkbereik;

b) een lijst van alle uitgangsvariabelen die door het instrumentele beveiligingssysteem worden gecontroleerd en voor elke variabele een indicatie of de controle direct is of via een ander voertuigsysteem. Het op elke variabele uitgeoefende controlebereik moet worden beschreven;

c) de grenzen van de functionele werking, als deze relevant zijn voor de prestaties van het systeem.

2.3. **Lay-out en schematische voorstellingen van het systeem**

2.3.1. *Inventaris van de onderdelen*

Er moet een lijst worden verstrekt van alle eenheden van het instrumentele beveiligingssysteem, met vermelding van de andere voertuigsystemen die nodig zijn om de desbetreffende controlefunctie te verwezenlijken. Er moet een schema worden verstrekt met de contouren van deze eenheden zoals ze zijn gecombineerd, waarop de verdeling van de apparatuur en de onderlinge verbindingen duidelijk zijn aangegeven.

2.3.2. *Functies van de eenheden*

De functie van elke eenheid van het instrumentele beveiligingssysteem moet worden toegelicht en de signalen die ze met andere eenheden of andere voertuigsystemen verbinden, moeten worden aangegeven. Dit kan door middel van een blokschema met opschriften of een andere schematische voorstelling of ook via een beschrijving vergezeld van een dergelijk blokschema.

2.3.3. *Interconnecties*

Een schakelschema moet de interconnecties binnen het instrumentele beveiligingssysteem tonen voor de elektrische transmissieverbindingen, door middel van een leidingschema voor pneumatische of hydraulische transmissieverbindingen en een vereenvoudigde schematische lay-out voor mechanische transmissieverbindingen.

2.3.4. *Signaalstroom en prioriteiten*

Er moet een duidelijke overeenkomst bestaan tussen deze transmissieverbindingen en de signalen die tussen eenheden worden overgedragen. De prioriteit van signalen op multiplexe data paths moet worden aangegeven als een dergelijke prioriteit van invloed is op de prestaties of de veiligheid.

2.3.5. *Identificatie van eenheden*

Elke eenheid moet duidelijk en ondubbelzinnig kunnen worden geïdentificeerd om het verband te kunnen leggen met de overeenkomstige hardware en documentatie. Wanneer functies binnen één eenheid of zelfs binnen één computer worden gecombineerd, maar in het blokschema voor alle duidelijkheid en gemakshalve in verschillende blokken worden aangegeven, mag slechts één hardware-identificatiemarkering worden gebruikt. Door gebruik te maken van deze identificatie bevestigt de fabrikant dat de geleverde apparatuur in overeenstemming is met het desbetreffende document.

2.3.5.1. De identificatie definieert de hardware- en softwareversie en, als er een nieuwe versie komt waardoor de functie van de eenheid wordt gewijzigd, moet ook de identificatie worden gewijzigd.

2.4. **Veiligheidsconcept van de voertuigfabrikant**

2.4.1. De fabrikant moet garanderen dat de gekozen strategie om de doelstellingen van het instrumentele beveiligingssysteem te verwezenlijken, de veilige werking van systemen die onder de voorschriften van dit reglement vallen, niet in het gedrang zal brengen zolang er geen storingen optreden.

2.4.2. Wat de in het instrumentele beveiligingssysteem toegepaste software betreft, moet de algemene architectuur worden toegelicht en moeten de ontwerpmethoden en -instrumenten worden geïdentificeerd. De fabrikant moet bereid zijn om op verzoek bewijzen te leveren van de manier waarop hij in het ontwerp- en ontwikkelingsproces voor de verwezenlijking van de systeemlogica is te werk gegaan.

2.4.3. De fabrikant moet de technische dienst een toelichting verstrekken bij de ontwerpvoorschriften die in het instrumentele beveiligingssysteem zijn geïntegreerd, om bij het optreden van storingen een veilige werking te realiseren. Mogelijke ontwerpvoorschriften voor storingen in het instrumentele beveiligingssysteem zijn:

a) terugvallen op een werking waarbij een gedeelte van het systeem wordt gebruikt;

b) overschakelen op een afzonderlijk back-upsysteem;

c) opheffing van de functie op een hoger niveau.

2.4.3.1. Als de gekozen ontwerpvoorziening onder bepaalde storingsvoorwaarden een werkwijze kiest met een gedeeltelijk vermogen, moeten deze voorwaarden worden aangegeven en moeten de daaruit voortvloeiende beperkingen van de doeltreffendheid worden gedefinieerd.

2.4.3.2. Als de gekozen ontwerpvoorziening een tweede middel (back-up) kiest om de doelstelling van het voertuigcontrolesysteem te verwezenlijken, moeten de principes van het overschakelingsmechanisme, de redundantielogica en het niveau ervan en alle geïntegreerde back-upcontrolekenmerken worden toegelicht en de daaruit voortvloeiende beperkingen van de doeltreffendheid worden gedefinieerd.

2.4.3.3. Als de gekozen ontwerpvoorziening voor opheffing van het systeem/de functie op een hoger niveau kiest, moeten alle overeenkomstige uitgangscontrolesignalen die met deze functie verband houden, worden stopgezet om de overgangsstoringen te beperken.

2.4.3.4. Systemen/functies op een hoger niveau moeten toelaten dat complexe systemen hun doelstellingen automatisch veranderen met een prioriteit die afhankelijk is van de gedetecteerde omstandigheden.

2.4.4. De documentatie moet vergezeld gaan van een analyse waaruit algemeen blijkt hoe het systeem zich zal gedragen bij het optreden van een van de genoemde storingen die op de voertuigcontroleprestaties of de veiligheid van invloed zullen zijn. Deze mag gebaseerd zijn op een falingstoestand- en effectenanalyse, een foutenboomanalyse of een soortgelijke, voor systeemveiligheidsoverwegingen geschikte procedure. De gekozen analytische benadering moet door de voertuigfabrikant worden vastgesteld en bewaard en moet aan de technische dienst worden verstrekt.

2.4.5. In de documentatie moeten de gecontroleerde parameters worden gespecificeerd en moet voor elke in punt 2.4.3 beschreven storing worden aangegeven welk waarschuwingssignaal moet worden geactiveerd.

3. TESTPROCEDURES

3.1. De functionele werking van het instrumentele beveiligingssysteem, zoals toegelicht in de in punt 2 gevraagde documenten, moet als volgt worden getest:

3.1.1. *Verificatie van de functie van het instrumentele beveiligingssysteem*

Om de normale werkingsniveaus vast te stellen, moet de verificatie van de prestaties van het voertuigsysteem zonder optredende storingen worden uitgevoerd en aan de basisspecificatie van de fabrikant worden getoetst.

3.1.2. *Verificatie van het veiligheidsconcept van punt 2.4*

De reactie van het instrumentele beveiligingssysteem moet naar keuze van de technische dienst worden gecontroleerd onder invloed van een storing in een individuele eenheid door overeenkomstige uitgangssignalen op elektrische eenheden of mechanische elementen toe te passen om de effecten van interne storingen binnen de eenheid te simuleren.

3.1.3. De resultaten van de verificatie moeten op zodanige wijze met de gedocumenteerde samenvatting van de foutenanalyse overeenkomen dat het veiligheidsconcept en de uitvoering ervan geschikt worden bevonden.

3.2. Aan de voorschriften voor het waarschuwingssignaal in punt 2.4.3 kan over het algemeen worden voldaan door één optisch signaal per complex voertuigsysteem, tenzij andere wetgeving die op dezelfde apparatuur van toepassing is, specifiek meervoudige signalen voorschrijft.

4. AANVULLENDE VOORSCHRIFTEN

4.1. In geval van een storing moet de bestuurder worden gewaarschuwd door een waarschuwingssignaal of een melding op een display. De waarschuwing moet aanwezig zijn zolang de storing zich voordoet, tenzij het systeem door de bestuurder wordt gedeactiveerd door bijvoorbeeld de voertuigactiveringsschakelaar naar „off" te draaien of door die specifieke functie uit te schakelen als daarvoor een speciale schakelaar voorhanden is.