

# BELGIAN STRESS TESTS

FANCO 

federal agency for nuclear control

National report for  
nuclear power plants

Man-made events



18<sup>th</sup> January 2012

NL versie

**Belgische weerstandstests**

**Nationaal verslag over de kerncentrales**

**Door de mens veroorzaakte gebeurtenissen**

**(“man-made events”)**

Dit nationaal verslag wordt verstrekt door de Belgische veiligheidsautoriteit (FANC en Bel V) als een onderdeel van het weerstandstestsprogramma dat van toepassing is op de Belgische kerncentrales in antwoord op het Fukushima-Daiichi ongeval.

<b>Revisie</b>	<b>Datum revisie</b>	<b>Beschrijving van de wijziging</b>	<b>Door</b>
0	2011-12-23	Eerste uitgave	FANC-Bel V

# Inleiding

België telt zeven kernreactoren voor elektriciteitsproductie verdeeld over twee sites :

- De site van Doel, gelegen langs de Schelde in de nabijheid van Antwerpen (Vlaanderen), herbergt vier reactoren :
  - Doel 1/2: tweelingeenheid van 433 MWe elk, in bedrijf gesteld in 1975;
  - Doel 3: eenheid van 1 006 MWe, in bedrijf gesteld in 1982;
  - Doel 4: eenheid van 1 039 MWe, in bedrijf gesteld in 1985.
- De site van Tihange, gelegen langs de Maas, nabij Luik (Wallonië) herbergt drie reactoren :
  - Tihange 1: eenheid van 962 MWe, in bedrijf gesteld in 1975;
  - Tihange 2 : eenheid van 1 008 MWe, in bedrijf gesteld in 1983;
  - Tihange 3 : eenheid van 1 054 MWe, in bedrijf gesteld in 1985.

Deze installaties worden uitgebaat door Electrabel, filiaal van de groep GDF-SUEZ.

Na het ongeval dat zich op 11 maart 2011 in de Japanse kerncentrale van Fukushima-Daiichi heeft voorgedaan, werd er een omvangrijk veiligheidsherevaluatieprogramma opgestart in de lidstaten van de Europese Unie die over dergelijke installaties op hun grondgebied beschikken.

Dit weerstandstestsprogramma ("stress tests") is een herevaluatie van de aanwezige veiligheidsmarges van de Europese nucleaire installaties t.a.v. extreme natuurlijke gebeurtenissen (aardbeving, overstroming,...) om hieruit de gepaste lessen te kunnen trekken.

Daarnaast heeft België het toepassingsgebied van deze evaluaties willen uitbreiden tot andere mogelijke bedreigingen die verband houden met menselijke activiteiten (toxische en explosieve gassen, schokgolven) en tot andere kwaadwillige handelingen (cyber-attack, vliegtuiginslag) met als doel een meer volledige balans op te stellen van de veiligheid van de Belgische installaties.

De evaluaties van deze door de mens veroorzaakte gebeurtenissen behoorden evenwel niet tot het toepassingsgebied van de Europese weerstandstestsprogramma's en daarom worden ze in een apart nationaal verslag uitgewerkt dat geen deel zal uitmaken van een internationale peer review.

Het Belgisch weerstandstestsprogramma omvat de zeven nucleaire reactoren van ELECTRABEL (met inbegrip van voor elk van hen hun opslagbekken voor gebruikte splijtstof), evenals de twee installaties voor de opslag van gebruikte splijtstof die gemeenschappelijk op elk van de sites gebruikt worden:

- het gebouw SCG te Doel (droge opslag in containers);
- en het gebouw DE te Tihange (opslag in splijtstofdokken).

Overeenkomstig de Belgische weerstandstests specificaties voor "door de mens veroorzaakte gebeurtenissen" omvat het Belgisch weerstandstestsprogramma twee opeenvolgende fasen:

- Fase 1: uitvoering van de weerstandstests (deadline: 31/10/2011).  
De exploitant voert de weerstandstests uit voor zijn installaties en noteert zijn resultaten in technische verslagen die hij overmaakt aan het Federaal Agentschap voor Nucleaire Controle (FANC).
- Fase 2: Analyse van de resultaten op nationaal niveau (deadline: 31/12/2011).  
In samenwerking met zijn technisch filiaal Bel V bestudeert het FANC de verslagen, evalueert de goedgekeurde aanpak en analyseert de verkregen resultaten. Op deze basis stelt het FANC een nationaal verslag op.

Fase 1 van het weerstandstestsprogramma liep ten einde op 31 oktober 2011 en de exploitant heeft zijn verplichtingen binnen de toegekende termijn nagekomen. De eindverslagen van de exploitant voor de kerncentrales van Doel en Tihange omvatten een (publiek) addendum m.b.t. de "door de mens veroorzaakte gebeurtenissen". Bepaalde van deze thema's die betrekking hebben op de door de

mens veroorzaakte gebeurtenissen dienen evenwel omwille van veiligheidsredenen (wet van 11 december 1998) geheim te blijven.

Fase 2 van het programma werd uitgevoerd door deskundigen van het FANC en Bel V. De verstrekte verslagen werden grondig onderzocht om zo een uitspraak te kunnen doen over de kwaliteit van de argumentering en de geldigheid van de door de exploitant voorgestelde resultaten. Technische vergaderingen en gerichte inspecties op de site werden geprogrammeerd naargelang ze nodig zijn om de realiteit, de pertinentie en de robuustheid van bepaalde gegevens en hypothesen waarmee de exploitant in zijn onderzoeken rekening heeft gehouden, te bevestigen. Dit proces leidde tot de opmaak van dit nationaal verslag inzake de 'door de mens veroorzaakte gebeurtenissen'.

Zoals vereist in de Belgische weerstandstests specificaties, dekt het Belgisch nationaal verslag m.b.t. de 'door de mens veroorzaakte gebeurtenissen' de volgende risico's:

- Accidentele of moedwillige vliegtuiginslag;
- Toxische en explosieve gassen en schokgolven;
- Cyberaanvallen.

Om een op zichzelf staand nationaal verslag te kunnen aanbieden, worden de relevante data die hieromtrent door de exploitant in zijn weerstandstestsverslagen worden verstrekt, samengevat. De evaluatie door de Belgische veiligheidsautoriteit (FANC en Bel V) wordt aan het einde van elk hoofdstuk gegeven.

De door de exploitant voorgestelde acties, evenals de bijkomende verbeteringen die vereist worden door de veiligheidsautoriteit zullen in de kortst mogelijke tijd geïmplementeerd worden, rekening gehouden met de complexiteit van de werkzaamheden die moeten worden ondernomen en hun belang ervan voor de veiligheid van de installaties. Om dit te bereiken zal de exploitant een geconsolideerd actieplan updaten en deadlines voorstellen die samen met de veiligheidsautoriteit zullen worden besproken.

Op basis hiervan zal de veiligheidsautoriteit een specifieke follow-up van de implementatie van het actieplan opstellen, met inbegrip van:

- Een regelmatige update door de exploitant van de vorderingen van het actieplan die periodiek aan de veiligheidsautoriteit zal worden meegedeeld;
- Periodieke informatievergaderingen tussen de veiligheidsautoriteit en de exploitant om de status van het actieplan te bespreken, evenals mogelijke moeilijkheden/vertragingen;
- On-site inspecties door de veiligheidsautoriteit, op periodieke basis en ook na de belangrijkste verwezenlijkingen, om zo op het terrein de vorderingen van de werkzaamheden na te gaan, alsook hun overeenstemming met de verwachtingen.

Deze follow-up zal de veiligheidsautoriteit de mogelijkheid bieden om de eigenlijke implementatie van het actieplan van de exploitant na te gaan en er zich van te vergewissen dat het engagement van de exploitant tijdig wordt nageleefd.

Als onderdeel van het transparantiebeleid van de veiligheidsautoriteit is dit nationaal verslag toegankelijk voor het publiek en de media op de website van de Belgische veiligheidsautoriteit (<http://www.fanc.fgov.be>).

# **1. (Accidentele of moedwillige) vliegtuiginslag**

## **1.1. Herevaluatie door de exploitant uitgevoerd in het kader van de weerstandstests**

Een volledige herevaluatie van het risico op vliegtuiginslag van terroristische oorsprong voor de eenheden van Doel en Tihange werd reeds door de exploitant uitgevoerd in 2002-2004 in antwoord op de terroristische aanslagen van 11 september 2001 in de Verenigde Staten.

In het kader van het weerstandstestsprogramma heeft de exploitant de beschikbare studies opnieuw onderzocht en de draagwijdte ervan uitgebreid tot met name de faling van de elektrische stroomvoorzieningsbronnen en van de koelingsbronnen van de eenheden, evenals tot het tegelijkertijd uitvallen van verschillende uitrustingen ingevolge het feit dat het vliegtuig nog over een bepaalde afstand over de grond verder schuift.

Er werden dan ook bijkomende maatregelen voor de verbetering van de veiligheid in geval van een vliegtuiginslag voorgesteld.

## **1.2. Belangrijkste door de exploitant voorgestelde resultaten**

De door de exploitant voorgestelde resultaten zijn, globaal gezien, gemeenschappelijk voor beide sites van Doel en Tihange.

Naar analogie met de aanpak voorzien voor het Europese weerstandstestsprogramma werd hierbij specifieke aandacht besteed aan het risico van de faling van de veiligheidsfuncties van de kerncentrales (elektrische stroomvoorzieningsbronnen en van de koelingsbronnen), en dit als gevolg van een vliegtuiginslag (in plaats als gevolg van een extreme natuurgebeurtenis zoals in het Europese weerstandstestsprogramma).

Gebaseerd op de informatie in de weerstandstestsverslagen van de exploitant en de bijkomende informatie verstrekt tijdens de technische vergaderingen en on-site inspecties, zijn de belangrijkste resultaten voor het onderwerp "vliegtuiginslag" de volgende:

- De mogelijke impact van een vliegtuiginslag op de veiligheidsfuncties van de kerncentrale (behoud van koeling en elektrische voeding) werd geanalyseerd. Voor verschillende inslagscenario's (glijpad en invalshoek) werd de mogelijke impact op de hiervoor relevante installaties (bv. gevolg van vliegtuigcrash op elektrische gebouwen en hoogspanningsposten, hulpkoeltorens,...) onderzocht. De reactoren beschikken over 2 verschillende niveaus van veiligheidssystemen om deze veiligheidsfuncties te verzekeren: de veiligheidssystemen van het eerste niveau, bedoeld voor incidenten en ongevallen van interne oorsprong en de veiligheidssystemen van het tweede niveau, bestemd voor externe risico's. De 2e niveau noodsystemen bevinden zich in gebunkerde gebouwen en zijn geografisch duidelijk gescheiden van de 1e niveau veiligheidssystemen, zodat het nagenoeg onmogelijk is dat een vliegtuiginslag beide niveaus van veiligheidssystemen gelijktijdig zou uitschakelen.
- De reactorgebouwen van de meest recente eenheden (Doel 3 en 4, Tihange 2 en 3), die werden voorzien van een dubbel containment in beton, zijn bestand tegen de impact van een lijnvliegtuig, en dit dus zonder beschadiging van het primaire circuit.
- Voor de reactorgebouwen van de oudere eenheden (Doel 1/2, Tihange 1) kan belangrijke schade van de externe structuur in beton, met de mogelijkheid van projectielen die binnen het

containment dringen, niet worden uitgesloten. Deze schade aan het containment impliceert evenwel niet noodzakelijk een aantasting van het primaire circuit, noch van de koelings- en back-ups systemen, rekening gehouden met de bijkomende bescherming door de talrijke structuren en kazematten in beton die aanwezig zijn binnen het reactorgebouw.

- De splijtstofdokken zijn weinig kwetsbaar voor een vliegtuiginslag, rekening gehouden met de dikte van de betonnen muren van de dokken en hun ligging op een hoogte zeer dicht bij de grond. Een mogelijkheid om de dokken opnieuw van water te voorzien in geval van barsten in de funderingen van de dokken wordt bestudeerd voor de eenheden Doel 1/2 en Tihange 1.
- De opstelling van bijkomende, voldoende hoge fysieke obstakels (pylonen...) rondom de sites wordt bestudeerd voor het intercepteren van een vliegtuig op lage hoogte, waardoor er tegelijkertijd een rechtstreekse botsing met de installaties kan worden vermeden en ervoor gezorgd wordt dat het brandstofverlies buiten de gebouwen plaatsvindt.
- Er zijn blusmiddelen voorzien op elke site om een kerosinebrand te doven. Er zijn evaluaties lopende om de capaciteit van de blusmiddelen voor een kerosinebrand verder te optimaliseren.
- Voor de eenheid van Tihange 1 wordt de oprichting van een nieuw « bunkergebouw » dat bestand is tegen vliegtuiginslag onderzocht waarin dan een meer compleet veiligheidssysteem van tweede niveau zal worden ondergebracht.

### **1.3. Resultaten van de evaluatie van de verslagen van de exploitant**

De door de exploitant gekozen aanpak voor de herevaluatie van het risico van een vliegtuiginslag beantwoordt aan de voorziene en door de veiligheidsautoriteit vooraf goedgekeurde methodologie.

Het is zeer onwaarschijnlijk dat een vliegtuig per ongeluk neerstort op een kerncentrale.

Toch werd er in België een hoog beschermingsniveau voorzien tegen vliegtuiginslag voor de recente kerninstallaties en werd er voor de eerste kerncentrales overgegaan tot maatregelen waardoor hun veiligheid kon worden verbeterd, en dit met name ter gelegenheid van de tienjaarlijkse herzieningen. Het is evenwel niet mogelijk om in de centrales technische verbeteringen door te voeren die een totale weerstand garanderen tegen terroristische aanslagen van het type dat zich in het World Trade Center heeft voorgedaan. Overeenkomstig de internationale praktijk maken terroristische vliegtuiginslagen deel uit van een zeker restrisico.

Indien één van de Belgische kerncentrales een aanval zou ondergaan van dezelfde aard als deze van 11 september 2001, dan zal het « noodplan voor nucleaire risico's op het Belgisch grondgebied » in werking treden.

Rekening gehouden met, enerzijds, de bouw van de Belgische kerncentrales, waarbij reeds van bij het ontwerp in grote mate met de diepteverdediging of defence-in-depth rekening werd gehouden en, anderzijds, met de maatregelen die voorzien zijn in het kader van het nucleair noodplan, is de veiligheidsautoriteit van oordeel dat in het geval van een terroristische aanslag het zeer weinig waarschijnlijk is dat een vliegtuig een kritische plaats van de centrale kan bereiken. Indien dit ondanks alles toch zou gebeuren, dan zouden de radiologische gevolgen voor de bevolking en het leefmilieu binnen aanvaardbare grenzen blijven.

Verschuillende factoren spelen immers een rol die de waarschijnlijkheid en de mogelijke gevolgen van een directe impact van een vliegtuig op een kritisch doelwit van een kerncentrale beperken:

- Alle reactoren beschikken over 2 verschuillende niveaus van veiligheidssystemen: de veiligheidssystemen van het eerste niveau bedoeld voor incidenten en ongevallen van interne oorsprong en de veiligheidssystemen van het tweede niveau bestemd voor externe risico's.

Deze 2e niveau noodsystemen bevinden zich in gebunkerde gebouwen of zijn geografisch duidelijk gescheiden van de 1e niveau veiligheidssystemen zodat het nagenoeg onmogelijk is dat een vliegtuiginslag beide niveaus van veiligheidssystemen gelijktijdig zou uitschakelen.

- De gebouwen die potentieel kritische doelwitten bevatten, hebben relatief beperkte afmetingen, zeker in vergelijking met de doelwitten van de aanslagen van 11 september 2001.
- Om het reactorgebouw te kunnen binnendringen, moet de impact met een hoge snelheid plaatsvinden en hoe hoger de snelheid, des te moeilijker - zelfs bijna onmogelijk - is het om een relatief klein doelwit (bv. een reactorgebouw) op een kritisch punt te raken zodat er belangrijke schade optreedt.
- De vele structuren rondom (bv. hoogspanningsmasten, omliggende gebouwen) en binnen de gebouwen (bv. talrijke structuren en kazematten in beton binnen de gebouwen) maken het praktisch onmogelijk om een directe impact op een potentieel kritisch systeem te bereiken.

De gedetailleerde analyse van de weerstandstestsverslagen van de exploitant en de daaropvolgende technische vergaderingen en inspecties door de veiligheidsautoriteit leiden tot de conclusie dat deze aanpak en het eruit resulterende verbeteringsactieplan adequaat zijn.

Algemeen is het belangrijk om enerzijds bijkomende preventieve maatregelen te voorzien om te vermijden dat potentieel kritische doelwitten kunnen bereikt worden door het optimaal plaatsen van obstakels zoals reeds voorgesteld door de uitbater, en om anderzijds de bestaande correctieve/mitigerende maatregelen te versterken indien een vliegtuigcrash toch plaats zou vinden, onafhankelijk ervan of het nu om een vrijwillige of onvrijwillige crash gaat.

De veiligheidsautoriteit identificeerde bijkomende vereisten om de robuustheid van de eenheden en de site verder te verbeteren tegen het risico op een vliegtuiginslag:

1. De **noodplannen en -procedures** voor elke eenheid moeten verder aangevuld worden met de specifieke vereiste maatregelen om doeltreffend te reageren op een vliegtuiginslag op de site. Bijvoorbeeld moet de richtlijn "Responsstrategie in geval van een vliegtuigrisico" volledig geïntegreerd worden in de noodplanprocedures. Specifieke noodplanoefeningen dienen georganiseerd te worden waarbij een vliegtuiginslag gesimuleerd wordt.
2. De exploitant moet de **middelen** die nodig zijn bij een vliegtuiginslag (blusmiddelen om een kerosinebrand te doven, obstakels, toevoer naar de splijtstofdokken) beschouwen als veiligheidsgebonden middelen voor zover deze een rol spelen in de leniging van de gevolgen van een vliegtuiginslag. In deze context dient de exploitant de specifieke voorschriften te bepalen die, daar waar nodig, van toepassing zijn op deze uitrusting (inspecties en tests, preventief onderhoud...).
3. De « **Extensive damage mitigation guidelines** » van de Amerikaanse Nuclear Regulatory Commission, die werden uitgewerkt ingevolge de ervaringsfeedback van 11 september 2001 en die tevens het gebruik van niet-conventionele noodmiddelen voorzien in geval van een vliegtuiginslag of een uitgebreide brand, moeten als referentiebasis gebruikt worden voor een toepassing op de Belgische centrales. Op basis van een benchmarking van de bestaande niet-conventionele noodmiddelen met deze EDMG moeten de nodige verbeteringen worden uitgevoerd.

## **2. Toxische of explosieve gassen, schokgolven**

### **2.1. Herevaluatie door de exploitant uitgevoerd in het kader van de weerstandstests**

De herevaluatie van de risico's verbonden met het afdrijven van toxische of explosieve gassen, evenals met de vorming van een schokgolf is hoofdzakelijk gebaseerd op de onderzoeken die voor elke eenheid in het kader van de tienjaarlijkse herzieningen gebeurden.

De gebeurtenissen en combinaties van gebeurtenissen die tot gevaarlijke situaties kunnen leiden, werden opnieuw onderzocht tijdens de meest recente tienjaarlijkse herzieningen, met inachtnaam van de verschillende risicobronnen die aanwezig zijn in een straal van 8 km rondom de centrales:

- toxische producten of explosieven die vervoerd of opgeslagen worden in de buurt van de sites: industriële installaties, buizen en pijpleidingen, vervoer over het water-, spoor- en wegennetwerk;
- toxische producten of explosieven die op de site worden opgeslagen.

De robuustheid van de installaties tegen de bestudeerde agressies wordt vervolgens geanalyseerd en de gepaste verbeteringsacties worden, indien nodig, voorgesteld om de controle van de eenheden te garanderen.

### **2.2. Belangrijkste door de exploitant voorgestelde resultaten**

Gebaseerd op de informatie in de weerstandstestsverslagen van de exploitant en de bijkomende informatie verstrekt tijdens de technische vergaderingen en on-site inspecties, zijn de belangrijkste resultaten voor het onderwerp "toxische en explosieve gassen en schokgolven" de volgende:

- Er zijn middelen voorzien om het personeel dat de eenheden bestuurt in geval van het afdrijven van een toxisch gas naar de site te beschermen. Deze middelen omvatten met name gasdetectoren in de ventilatieleidingen, isolatievoorzieningen voor de toevoer van de buitenlucht, of individuele beschermingsmiddelen (filterende of isolerende maskers) in voldoende aantal;
- De "bunkergebouwen" (reactorgebouwen, gebouwen waarin de splijtstofdokken zijn ondergebracht, noodgebouwen) zijn zodanig bemeten dat ze weerstand kunnen bieden aan een referentie-explosie, of aan de bijbehorende projectielen buiten de gebouwen.
- Bepaalde bunkergebouwen en niet-bunkergebouwen zijn uitgerust met gasdetectoren in de ventilatieleidingen waardoor men zich kan beschermen tegen de aanzuiging in deze gebouwen van explosieve gassen afkomstig van buiten.

Bijkomend hierbij voegt de exploitant eraan toe dat hij voorziet om bijkomende detectoren voor toxische gassen op de site van Doel te installeren.

### **2.3. Resultaten van de evaluatie van de verslagen van de exploitant**

De door de exploitant gekozen aanpak voor de herevaluatie van het risico op het afdrijven van toxische of explosieve gassen en op schokgolven beantwoordt aan de voorziene en door de veiligheidsautoriteit vooraf goedgekeurde methodologie.



De gedetailleerde analyse van de weerstandstestsverslagen van de exploitant en de daaropvolgende technische vergaderingen en inspecties door de veiligheidsautoriteit leiden tot de conclusie dat deze aanpak en het eruit resulterende verbeteringsactieplan adequaat zijn.

De veiligheidsautoriteit identificeerde evenwel bijkomende vereisten om de robuustheid van de eenheden en de site verder te verbeteren tegen het risico op toxische en explosieve gassen en schokgolven:

1. De **bewoonbaarheid van de (hoofd en nood-)controlezalen**: het personeel in de controlezalen moet op post kunnen blijven en doeltreffend beschermd worden bij het aanzuigen van een toxische of radioactieve gaswolk, a fortiori in een noodsituatie; hiertoe moet de lekdichtheid van de controlezalen ten opzichte van de buitenlucht, gegarandeerd worden voor elke eenheid; deze bepaling moet worden begeleid door de invoering van aangepaste en performante meetmiddelen om de aanwezigheid van een externe atmosferische vervuiling te meten, en door isolatiemiddelen voor de ventilatie van de betrokken lokalen, indien nodig, voor het nastreven van een goede lekdichtheid van de betrokken lokalen. De veiligheidsautoriteit vraagt in dit kader verbeteringen door te voeren voor de volgende specifieke aspecten:
  - Noodcontrolezaal Doel 1&2: bescherming tegen toxische gassen;
  - Hoofdcontrolezaal Tihange 1: automatische isolatie van ventilatie bij detectie van toxische gassen;
  - Hoofdcontrolezaal Doel 1&2: verbetering lekdichtheid.
2. De veiligheidsautoriteit vraagt dat ook de langetermijnbewoonbaarheid van de **lokalen** die bemand worden voor de **noodplanning** door de exploitant meer diepgaand zouden geëvalueerd worden. Hierbij moet afdoende rekening gehouden worden met noodplansituaties die meerdere of alle installaties van een bepaalde site moeten dekken. De evaluatie van de bewoonbaarheid van deze lokalen moet alle aspecten behandelen (in het bijzonder radiologische belasting en toxische gassen). Dit is geldig voor alle eenheden.
3. Als aanvulling op de uitgevoerde analyses vraagt de veiligheidsautoriteit dat de exploitant eveneens een onderzoek zou uitvoeren naar de gevolgen van ernstige gebeurtenissen (zoals bv. een aardbeving), waarbij niet kan worden uitgesloten dat verschillende toxische of explosieve gassen zouden vrijkomen door een **meervoudige breuk** van opslagtanks uit industriële installaties in de omgeving, met als gevolg een bedreiging van de bewoonbaarheid van essentiële lokalen of ernstige complicaties voor de noodplanmaatregelen. Er wordt gevraagd aan de exploitant om terzake een aanpak voor te stellen voor het inschatten van dergelijk risico.
4. De opvolging van de **evolutie van de industriële omgeving rondom de sites**: de exploitant moet actief toezien op de nieuwe industriële toepassingen en het vervoer die zich ontwikkelen rondom de sites; hij moet indien nodig de risico's herevalueren en er zo nodig de gepaste antwoorden op bieden of de bevoegde federale of regionale overheden sensibiliseren. Restricties met betrekking tot het gebruik van de grond rondom de sites moeten tevens proactief besproken worden tussen de exploitanten, de veiligheidsautoriteit en de regionale overheden om een toename van de risico's in de nabijheid van de installaties te voorkomen.
5. De ventilatiesystemen van de gebouwen van Doel 1&2 en Tihange 1, en de gebouwen van de veiligheidssystemen van het eerste niveau van Doel 3 en 4 en Tihange 2 en 3 zijn niet uitgerust met detectoren voor **explosieve gassen**. De exploitant dient een evaluatie, en indien nodig een haalbaarheidsstudie, uit te voeren over de installatie van detectoren van explosieve gassen die dienen om de ventilatie te isoleren zodat er geen explosieve gassen worden aangezogen binnen de gebouwen.

## **3. Cyberaanval**

### **3.1. Herevaluatie door de exploitant uitgevoerd in het kader van de weerstandstests**

De exploitant heeft de risico's verbonden met vier soorten computeraanvallen geanalyseerd:

- een externe aanval van buiten het computernetwerk van het bedrijf;
- een aanval buiten site, via het computernetwerk van het bedrijf;
- een aanval op de site, via het computernetwerk van de centrale;
- een aanval op de site door de rechtstreekse fysieke toegang tot de computers en systemen op de netwerken van de centrale.

De exploitant heeft vervolgens de mogelijkheden onderzocht van een verlies van controle van de centrale door de operator, rekening gehouden met de bestaande veiligheidsbepalingen.

### **3.2. Belangrijkste door de exploitant voorgestelde resultaten**

Gebaseerd op de informatie in de weerstandstestsverslagen van de exploitant en de bijkomende informatie verstrekt tijdens de technische vergaderingen en on-site inspecties, zijn de belangrijkste resultaten voor het onderwerp "cyberaanval" de volgende:

Volgens de evaluatie van de exploitant kan een cyberaanval niet leiden tot een verlies van de veiligheidsfuncties van de Belgische kerncentrales omdat:

- de besturings- en beschermingssystemen van de reactoren noch met het computernetwerk van de centrale, noch met dat van het bedrijf verbonden zijn;
- de bijna-totaliteit van de besturings- en beschermingssystemen van de reactoren gebruik maakt van een analoge technologie via kabels die niet kwetsbaar is voor cyberaanvallen;
- er maatregelen (met inbegrip van de fysieke beveiliging) voorzien zijn om de informaticasystemen die de veiligheidsfuncties ondersteunen, te beschermen.
- Er een verbeteringsprogramma werd ingevoerd om het beveiligingsniveau te verhogen.

### **3.3. Resultaten van de evaluatie van de verslagen van de exploitant**

De door de exploitant gekozen aanpak voor de herevaluatie van het risico voor de veiligheidsfuncties van de kerncentrales van Doel en Tihange veroorzaakt door cyberaanvallen, beantwoordt aan de door de exploitant bepaalde en door de veiligheidsautoriteit goedgekeurde methodologie.

Een gedetailleerde analyse van de weerstandstestsverslagen van de exploitant leidt tot de conclusie dat de voorgestelde aanpak bevredigend is, want de conclusies ervan, die stellen dat een cyberaanval niet tot een verlies van de veiligheidsfuncties van de Belgische kerncentrales kan leiden, zijn coherent met engineering judgment.

De exploitant voert een informaticabeveiligingsstrategie die vergelijkbaar is met deze van andere bedrijven die zich bewust zijn van de gebruikelijke risico's voor de gevoelige systemen (segmentatie van netwerken volgens toegang via firewalls, monitoring, hardening van de systemen, preventie van malware, procedures, opleidingen,...).

Cyberbeveiligingsaspecten veranderen evenwel continu en de bijbehorende technologieën evolueren constant zodat de beveiligingsaspecten regelmatig moeten worden opgevolgd. In het bijzondere geval van de nucleaire industrie zijn IT en ICS (Industrial Control Systems) minder beschikbaar dan in andere industrieën en zijn ze dus minder onderworpen aan wijzigingen.

De volgende cyberbeveiligingsrisico's moeten in het bijzonder van nabij worden opgevolgd:

- De kwetsbaarheid/het risico verhoogt meer en meer naarmate de IT van de installaties verder moderniseert.
- De kwetsbaarheid/het risico verhoogt met de toename van de onderaanneming. Dit risico wordt gedeeltelijk beheerd door de oppuntstelling van interne normen voor de omkadering van de externe intervenanten.
- De kwetsbaarheid van de industriële systemen van het type SCADA (Supervisory Control and Data Acquisition) verhoogt met het opduiken van nieuwe malware die ontwikkeld wordt om deze systemen aan te vallen.

De veiligheidsautoriteit heeft evenwel een bijkomend thema geïdentificeerd waar verdere verbeteringen van de robuustheid van de centrale en de site tegen cyberaanvallen wenselijk zijn.

De meeste veiligheidsfuncties maken gebruik van analoge technologie en slechts een klein gedeelte van de uitrusting maakt gebruik van digitale en computergebaseerde technologie. Gezien er meer en meer nieuwe digitale en computergebaseerde technologieën worden geïnstalleerd, beveelt de veiligheidsautoriteit aan om, met de assistentie van IT-specialisten, een beveiligingsevaluatie in de lokalen van de exploitant door te voeren. Deze **externe onafhankelijke audit** zal bestaan in de verificatie van de maatregelen die voor de beperking van het risico op cyberaanvallen door de exploitant op de computergebaseerde veiligheidsfuncties worden toegepast. Onafhankelijke IT-beveiligingsnormen (ISO, COBIT of andere) moeten toelaten om de beveiliging via objectieve en door derden (externe audit) controleerbare criteria te meten, zoals dit gebeurt voor de niet IT-gerelateerde industriële processen.