

Fukushima in de polder

Of het nu over veilig vrijen, brandveiligheid, of veilige kerncentrales gaat, het is altijd vechten om veiligheid op de agenda te krijgen en houden. Het kost veel praten, overtuigen, redeneren, druk zetten, tot zelfs ingrijpen om betrokkenen van hoog tot laag in de modus te krijgen dat veiligheid een integraal onderdeel van het denken, ontwerpen, bouwen en beheren is en moet blijven. Het is daarom niet voor niets dat veiligheidsexperts in Nederland verzuchten: geef ons heden ons dagelijks brood en af en toe een watersnood. Je ziet dit fenomeen direct aan de actualiteit. Een ramp trof Japan waarbij een aardbeving en een tsunami elkaar opvolgden. Op zich is dat laatste niet geheel ongebruikelijk omdat een tsunami veroorzaakt wordt door een aardbeving. We hebben inmiddels geleerd dat in Japan bij een aardbeving kerncentrales automatisch worden uitgeschakeld. Dan moet de hete kern gekoeld worden en daar zijn maar liefst vier redundante koelsystemen voor om te voorkomen dat de koeling uitvalt. Wat volgens Japanse deskundigen dit voorval uniek maakt, is dat er gebrek is aan stroom waardoor koeling niet kan worden gecontinueerd, met een mogelijke meltdown tot gevolg.



Veiligheid is een zaak van loven en bieden geworden

Ongetwijfeld heeft men dit allemaal goed doordacht via gevarenanalyses en uitwerking daarvan in het voorkomen van allerlei rampscenario's. Neem nu het scenario: hevige aardbeving met tsunami. Dan mag je verwachten dat alle kerncentrales uitgaan, en dat er dus geen stroom is in de verre omgeving van de centrales. En inderdaad, er vielen elf centrales uit. Bij dit scenario weet je dus dat er geen stroom zal zijn. Dat moet je dan oplossen in het ontwerp van de kerncentrales. Ik had dus vier verschillende redundante energiebronnen meeontworpen naast de viervoudige noodkoeling. Bijvoorbeeld, naast een lokale voorraad brandstof moeten er ook meerdere aardbevingbestendige hooggelegen dieseldpots worden gerealiseerd die onbereikbaar zijn voor een tsunami, met pijpleidingen richting de kerncentrales. Voor het geval dat die leidingen het begeven, zijn modderbestendige tankauto's en zelfs helikopters nodig zodat er nooit en te nimmer een gebrek aan energie kan optreden en dieselgeneratoren lang genoeg ingezet kunnen worden om ten koste van alles de viermaal redundante koeling in stand te houden. Er moeten noodolieleidingen klaarliggen, in een hoger gelegen bunker. Uiteraard moet je ook een noodvoorziening voor het koelwater zelf meeontwerpen in de vorm van bassins die reeds klaarliggen. Je kunt zelfs denken aan het realiseren van reactorvaten onder de waterlijn zodat in het ernstigste geval koeling als vanzelf door zeewater kan worden gerealiseerd. Dit ontwerpprincipe is ook bij de Nederlandsche Bank gebruikt waar de kluisen vollopen in geval van ongeoorloofd bezoek.

Door rekening te houden met het onmogelijke, zit je voordat je het weet aan inhibitief hoge kosten om een veiligheidskritisch systeem te realiseren. Veiligheid is daarmee een kwestie van loven en bieden geworden. Daarnaast spelen politiek-bestuurlijke belangen een belangrijke rol. Neem nu de Challenger-spaceshuttle. Die ontplofte doordat een O-ring faalde. Engineers waarschuwden dat door de lage temperatuur die dag er bij een lift-off risico's aan deze O-ringen zaten. We weten de afloop. De geschiedenis herhaalde zich met de Columbia, ditmaal bij terugkomst waar de shuttle desintegreerde omdat bij lift-off een hittebestendige tegel te zwaar was beschadigd door loslatend materiaal van de brandstoftanks tijdens het opstijgen.

De actualiteit van Japan laat duidelijk zien dat nu ineens centrales worden stilgelegd, dat er een stresstest komt, dat de discussie tussen voor- en tegenstanders oplaait. Wat vooral opvalt, is dat iedereen zich haast te zeggen dat wat in Japan kan ook alleen in Japan kan en niet hier.

Een van de argumenten is dat we geen tsunami's kennen. Een tsunami is een staande golf, ook wel seiche genaamd, als gevolg van een zeebeving. Seiches kunnen ook door andere oorzaken ontstaan, bijvoorbeeld door luchtdrukverschillen of koufronten boven zee. Op de

Noordzee is de hoogte van die seiches zo'n decimeter maar bij het bereiken van de havens van IJmuiden of Rotterdam kan de hoogte oplopen tot een kleine twee meter. In Rotterdam zien we dit verschijnsel vanaf 25 centimeter zo'n acht keer per jaar. In de periode 1995-2001 waren er in de haven van Rotterdam 51 seiches, met een hoogte tussen de 25 centimeter oplopend tot maar liefst 1 meter 69. Diepliggende schepen worden dan aan de grond gezet, lagades overstromen. Een seiche kan tijdens een sluiting van de Maeslantkering tijdelijk achter de kering een hogere waterstand veroorzaken dan voor de kering en zodoende de integriteit van de constructie bedreigen, aldus Rijkswaterstaat. Bij oplevering was geen rekening gehouden met dit fenomeen. Dat lijkt later toch ingebouwd te zijn, maar dat is geen 'safety by design'.

Als die constructie in de rivier komt te liggen, dan overstroomt het achterland omdat het rivierwater niet weg kan. Daarmee bereikt de constructie het omgekeerde waarvoor die bedoeld is: 1,3 miljoen mensen in het achterland beschermen, en de infrastructuur van een van de grootste havens ter wereld. In Japan was sprake van een 'compound disaster': aardbeving, tsunami en kerncentrale. Hier kan dat zijn: stormvloed, seiche en waterkering.

Er is ook een kerncentrale in ons land. Die is door firma Siemens gebouwd. Diezelfde fabrikant heeft ook meegewerkt aan de nucleaire faciliteit in Iran. Die fabriek wordt momenteel bedreigd door de Stuxnet-worm. Dat is een computervirus dat aangrijpt op het besturings-systeem van Siemens dat waarschijnlijk in die centrale zit. Het zou het besturingssysteem stil kunnen leggen. Maar dat virus duikt dus ook op andere plekken op, en zou via besmetting Borssele kunnen bereiken. Een combinatie van onderhoud aan de centrale en besmetting door de Stuxnet-worm kan leiden tot gevaarlijke situaties waarbij de installatie onbestuurbaar is geworden.

Naast computervirussen is de vraag of de software in de centrale überhaupt wel veilig is. Bij tunnelprojecten is het veiligheidssysteem de achilleshiel maar ook bij de HSL is dat het onderdeel dat mankeert. Verder ligt de faalkans van de Maeslantkering waarschijnlijk veel hoger dan wat is geëist. Dus hoe veilig zijn die veiligheidssystemen dan precies? In de actualiteit horen we dat de specificaties van een nieuw te bouwen kerncentrale zijn dat een meltdown minder dan eens per miljoen jaar mag optreden. We hebben nog maar een halve eeuw van dit soort faciliteiten, en er zijn er nu al drie waar een majeur ongeluk heeft plaatsgevonden. Dus we halen bij lange na de eens per miljoen jaar niet. Ook al tellen we alle operationele jaren van alle kerncentrales op. De faalkans ligt veel hoger. Dus eisen opschrijven is blijkbaar iets anders dan ze waarmaken. De eis dat er geen onderdelen mogen losrammelen van de brandstoftank van de spaceshuttle bleek ook van papier.

Wat zegt het Internationaal Atoom Agentschap over de veiligheid van software? Letterlijk staat in een van hun standaarden dit te lezen: "the quantitative evaluation of the reliability of software based systems is more difficult than that for non-programmable systems and this may raise specific difficulties in demonstrating the expected safety of a computer based system. Claims of high software reliability are not demonstrable at the present time. Hence, designs requiring a single computer based system to achieve probabilities of failure on demand of lower than 10⁻⁴ for the software should be treated with caution." In het kort zegt men hier: het is onmogelijk om de betrouwbaarheid van software in maat en getal te vatten en iedereen die dat claimt moet je niet zomaar op zijn woord geloven, zeker als het gaat om faalkansen van een op de tienduizend keer dat je een systeem aanspreekt.

Met andere woorden, de veiligheid van de software in kerncentrales, maar ook die van de gecomputeriseerde waterkeringen, tunnels, sluizen, bruggen, procesfabrieken, en wat dies meer zij, is kennelijk maar lastig in cijfers uit te drukken. Daarom is het van groot belang om deze infrastructuur die essentieel afhankelijk is van betrouwbaar werkende ICT tegen het licht te houden. In geval van kerncentrales is naast een stresstest een diepgaand onderzoek naar de kwaliteit, en met name de veiligheid en beveiliging van de operationele software een must.

Prof. dr. Chris Verhoef is hoogleraar Informatica aan de Vrije Universiteit Amsterdam