Veilig? Volgens wie? – waarom compliance geen vertrouwen garandeert.

door Arjan van Dijk, TU Delft, faculteit Technology, Policy & Management

1. De wereld waarin we ons bevinden



Goedemiddag allemaal.

Stel u even een willekeurige moderne procesinstallatie voor. Misschien een raffinaderij. Misschien een chemische fabriek. Misschien een opslagterminal, een waterstofproject, een ammoniakinstallatie, een fabriek met ATEX-zones, druksystemen, sensoren, barrières en procedures.

Wie daar dagelijks werkt, weet: dit is geen wereld van improvisatie. Dit is een wereld van normen, inspecties, vergunningen, audits, HAZOPs, LOPA's, ATEX-zoneringen, onderhoudsregimes, Management of Change, noodplannen en veiligheidsstudies.

En eerlijk is eerlijk: de procesindustrie is technisch indrukwekkend geworden. We hebben meer data dan ooit. We hebben betere detectie, betere monitoring, betere engineering, betere modellen, betere opleiding, betere incidentanalyse, betere software en steeds meer predictive analytics.

We kunnen druk, temperatuur, explosiegrenzen, barrièrestatussen en afwijkingen in real time volgen. We hebben dashboards waarop zwakke signalen zichtbaar worden. We hebben digitale twins, sensoren, drones, simulaties en algoritmen die ons helpen voorspellen waar risico's kunnen ontstaan.

En toch wil ik vandaag beginnen met een ongemakkelijke observatie: ondanks al die vooruitgang is de maatschappelijke acceptatie van industriële risico's kwetsbaarder dan ooit. Vergunde projecten stranden. ESG-rapportages overtuigen niet altijd. Omwonenden vertrouwen cijfers niet vanzelf. Nieuwe energietransitieprojecten — waterstof, ammoniak, CCS, elektrificatie, batterijen — worden technisch onderbouwd, juridisch vergund en bestuurlijk verdedigd, maar roepen toch weerstand op.

Dus de vraag van vandaag is niet: zijn we veiliger geworden? De vraag is scherper: **Veilig? Volgens wie?**

2. Veilig? Volgens wie?



In veel bedrijven betekent het woord “veilig” iets heel specifieks. Het betekent: we voldoen aan wet- en regelgeving. De vergunning is op orde. De ATEX-classificatie is gedaan. De inspectie is afgerond. De audit is gesloten. De KPI’s staan op groen. De procedures zijn beschikbaar. De incidentfrequentie daalt. De rapportage is ingediend.

En dat is allemaal belangrijk. Laat daar geen misverstand over bestaan. Compliance is noodzakelijk. Zonder compliance is er geen basis. Maar buiten het hek van de fabriek betekent “veilig” vaak iets anders.

> Voor een omwonende betekent veilig misschien: kan ik mijn kinderen hier laten opgroeien zonder mij zorgen te maken? Word ik eerlijk geïnformeerd als er iets misgaat? Begrijpt dit bedrijf eigenlijk wat het voor mij betekent om naast deze installatie te wonen?
>
> Voor een maatschappelijke organisatie betekent veilig misschien: worden onzekerheden benoemd, of alleen de gunstige cijfers? Is de risicobeoordeling onafhankelijk? Wordt er ook gekeken naar cumulatieve blootstelling, historische incidenten en machtsverhoudingen?
>
> Voor een journalist betekent veilig misschien: klopt het verhaal dat het bedrijf vertelt met wat insiders zeggen? Voor een bestuurder: kan ik dit uitleggen aan de raad, de Kamer, de media? Voor een rechter: is niet alleen de procedure gevolgd, maar is de belangenafweging geloofwaardig?

En daar ontstaat de breuk. Binnen de industrie wordt compliance vaak ervaren als bewijs van verantwoordelijkheid. In de samenleving wordt compliance regelmatig ervaren als: het minimale dat je moet doen.

Dat verschil is geen communicatiedetail. Dat verschil is strategisch.

> Want als wij zeggen: “Wij voldoen aan de norm,” dan hoort de buitenwereld soms: “Wij doen precies genoeg om legaal te zijn.”
>
> Als wij zeggen: “Het risico is acceptabel,” dan vraagt de samenleving: “Acceptabel voor wie?”
>
> Als wij zeggen: “Er is geen onaanvaardbaar risico,” dan vraagt de omwonende: “Wie heeft bepaald wat aanvaardbaar is, en mocht ik daar iets van vinden?”

Dat is de paradox van deze tijd. We zijn technisch steeds beter in staat risico’s te beheersen, maar maatschappelijk steeds minder zeker dat onze beheersing ook wordt geloofd.

3. Waarom meer van hetzelfde ons verder van de oplossing brengt



Wat doen organisaties meestal als vertrouwen onder druk staat? Ze gaan meer uitleggen. Ze publiceren meer cijfers. Ze maken een betere ESG-paragraaf. Ze voegen indicatoren toe. Ze verwijzen naar vergunningen. Ze laten zien dat ze voldoen aan normen. Ze organiseren een informatieavond. Ze maken een Q&A. Ze maken een animatie. Ze zeggen: “We moeten het beter communiceren.”

En soms helpt dat. Maar vaak niet genoeg. Waarom niet? Omdat wantrouwen zelden ontstaat door een tekort aan informatie alleen. Wantrouwen ontstaat vaak door een ervaren kloof tussen drie dingen.

> Eén: wat een bedrijf feitelijk doet en presteert.
>
> Twee: wat een bedrijf expliciet of impliciet belooft.
>
> Drie: wat stakeholders waarnemen, voelen, vrezen en geloven.

Als die drie niet op elkaar aansluiten, wordt zelfs correcte informatie verdacht. Laat me dat concreet maken:

> Een bedrijf kan technisch uitstekende veiligheidsbarrières hebben. Maar als omwonenden eerder een incident hebben meegemaakt, als zij zich niet serieus genomen voelen, of als zij pas informatie krijgen nadat de media erover berichten, dan is de technische kwaliteit van die barrières niet genoeg om vertrouwen te herstellen.
>
> Een bedrijf kan een prachtig ESG-rapport publiceren. Maar als dat rapport vooral successen toont en onzekerheden vermijdt, dan kan transparantie juist averechts werken. Dan voelt het niet als openheid, maar als reputatiemanagement.
>
> Een bedrijf kan voldoen aan alle normen. Maar als de maatschappelijke norm verschuift, kan juridische toestemming onvoldoende zijn voor sociale legitimiteit.

Dat zien we steeds vaker bij energietransitieprojecten. Waterstof is technisch interessant en noodzakelijk in bepaalde ketens. Ammoniak kan een rol spelen in opslag en transport van energie. CCS kan belangrijk zijn in klimaatbeleid. Maar voor de samenleving zijn dit geen neutrale technologieën. Het zijn nieuwe risico’s, nieuwe installaties, nieuwe transportbewegingen, nieuwe onzekerheden en vaak ook nieuwe beloftes. En nieuwe beloftes trekken nieuwe aandacht.

In het verleden kon een industrieel risico relatief lokaal blijven. Nu kan één incident, één foto, één geurklacht, één klokkenluider, één video vanaf een smartphone binnen minuten een nationaal verhaal worden. Die sociale amplificatie van risico is geen theorie meer voor in de literatuur. Het is dagelijkse realiteit.

De reflex “we moeten gewoon beter uitleggen hoe veilig het is” schiet dan tekort. Want de onderliggende vraag is niet alleen: begrijpt men onze techniek? De onderliggende vraag is: gelooft men onze intenties, onze competentie, onze eerlijkheid en onze bereidheid om te leren?

4. Veiligheid is ook een vertrouwensvraagstuk



Het kantelpunt in mijn eigen denken kwam toen ik de zogenaamde “Social License to Operate” van Seveso-bedrijven niet alleen ben gaan bekijken als een communicatievraagstuk, maar als een governancevraagstuk.

De vraag is dan niet: hoe krijgen we stakeholders zover dat ze ons veiligheidsverhaal accepteren? De vraag is: hoe organiseren we dat ons veiligheidsverhaal geloofwaardig verbonden is met onze werkelijke prestaties én met de manier waarop stakeholders risico’s beoordelen? Dat is een fundamenteel andere vraag. Het betekent dat vertrouwen niet iets is wat je achteraf toevoegt aan veiligheid. Vertrouwen is geen sausje over een technisch systeem. Vertrouwen is onderdeel van de maatschappelijke werking van dat systeem.

U kunt een installatie technisch veilig ontwerpen, maar als mensen de informatie niet geloven, de besluitvorming oneerlijk vinden, de risicoverdeling onrechtvaardig vinden of het bedrijf niet competent achten, dan is de legitimiteit kwetsbaar. En legitimiteit is voor high hazard industries geen luxe:

Het is operationele continuïteit.

Het is vergunningverlening.

Het is projectdoorlooptijd.

Het is financierbaarheid.

Het is politieke ruimte.

Het is de mogelijkheid om te blijven opereren in een omgeving waar risico’s nooit nul zijn.

Daarom is de kernvraag van deze keynote: Hoe bouwen we een brug tussen technische veiligheid en maatschappelijk vertrouwen?

5. Drie wegen die moeten samenkomen



In mijn promotieonderzoek werk ik met een eenvoudig maar krachtig uitgangspunt.

Vertrouwen ontstaat niet doordat één element goed is. Vertrouwen ontstaat wanneer drie informatie wegen (“lanen”) met elkaar in lijn komen.

De eerste laan is de realiteitslaan: de feitelijke SHE-prestaties. Wat gebeurt er werkelijk in de fabriek? Hoe gezond zijn de barrières? Hoe vaak worden afwijkingen gevonden? Hoe snel worden ze opgevolgd? Hoe voorspelbaar zijn prestaties? Zijn audits papieren rituelen of leren we er echt van? Zien we zwakke signalen op tijd?

Voor het ATEX- en process safety-publiek is dit vertrouwd terrein. Dit gaat over incidentanalyse, preventie, normen, richtlijnen, risicobeoordeling en procesveiligheidsbeheer. Maar de vraag wordt scherper: kunnen we niet alleen aantonen wat er gisteren goed ging, maar ook geloofwaardig voorspellen waar morgen de kwetsbaarheid ontstaat? Daar komt technologie in beeld: real-time barrier monitoring, predictive analytics, near miss-analyse, integratie van auditdata en operationele data. Maar let op: voorspellende technologie versterkt vertrouwen alleen als de voorspellende waarde expliciet, uitlegbaar en eerlijk is. Een dashboard dat intern indrukwekkend is, maar extern onbegrijpelijk, bouwt nog geen vertrouwen.

De tweede laan is de narratieve laan: de expliciete en impliciete veiligheidsbeloften. Wat beloven wij eigenlijk? Niet alleen in slogans. Niet alleen in ESG-rapportages. Ook in vergunningaanvragen, bewonersbrieven, websites, directietoespraken, veiligheidsbeleid, stakeholdergesprekken en zelfs in stilte. Want ook niet-communiceren is een boodschap.

Als een bedrijf zegt: “Safety first,” wat betekent dat dan bij een onderhoudsstop met tijdsdruk? Als een bedrijf zegt: “Wij nemen geen risico’s,” klopt dat dan eigenlijk wel in een industrie waar risico’s nooit nul zijn? Als een bedrijf zegt: “Wij zijn transparant,” worden onzekerheden dan ook gedeeld?

En hier komt ook de “risk appetite” in beeld. Veel organisaties hebben impliciet grenzen aan wat men accepteert, tolereert, uitstelt of escaleert. Maar die grenzen zijn vaak intern, technisch of bestuurlijk geformuleerd.

Stakeholders horen vooral de belofte. En als die belofte ambitieuzer is dan de voorspelbaarheid van de prestatie, ontstaat overpromising. Overpromising is gevaarlijk voor vertrouwen. Niet omdat mensen perfectie eisen, maar omdat mensen eerlijkheid eisen over onzekerheid, dilemma’s en grenzen.

De derde laan is de perceptielaan: hoe stakeholders risico’s waarnemen en beoordelen.

Risicoperceptie door leken is niet irrationeel omdat zij anders is dan een technische risicoanalyse. Risicoperceptie is een andere vorm van beoordeling. Mensen kijken niet alleen naar kans maal effect. Ze kijken naar vrijwilligheid, controle, eerlijkheid, eerdere ervaringen, vertrouwen in instituties, verdeling van baten en lasten, en de vraag of hun zorgen serieus worden genomen.

Een expert kan zeggen: “De kans is zeer klein.”

Een bewoner kan antwoorden: “Maar ik draag wel het gevolg als het misgaat.”

Beiden kunnen tegelijk rationeel zijn vanuit hun eigen positie.

Dat is lastig voor technici, omdat techniek zoekt naar objectivering. Maar vertrouwen vraagt ook erkenning van subjectieve ervaring. Het gaat dus niet om de keuze tussen feiten en gevoelens.

Vertrouwen ontstaat wanneer de drie lanen samenkomen, want:

Als de drie lanen uit elkaar lopen, wordt vertrouwen fragiel.

Als prestaties goed zijn, maar beloften overdreven: fragiel.

Als beloften zorgvuldig zijn, maar prestaties onvoorspelbaar: fragiel.

Als prestaties en beloften kloppen, maar stakeholders zich genegeerd voelen: fragiel.

Het gaat om de vraag hoe feiten betekenis krijgen in een sociale context.

6. Een governance-benadering: INTEGRIS



Daarom werk ik aan een governance-benadering die ik INTEGRIS noem. Niet als extra communicatielaag. Niet als reputatie-instrument. Maar als een dynamisch diagnose- en besluitvormingsraamwerk dat vijf vragen met elkaar verbindt.

Eerste vraag: kunnen we onze SHE-prestaties voorspelbaar maken? Niet alleen terugkijken naar incidenten, maar vooruitkijken naar barrièregezondheid, afwijkingen, onderhoudscondities, auditbevindingen, near misses en zwakke signalen. Voor ATEX en process safety betekent dit: verschuiven van lagging indicators naar leading en predictive indicators. Niet alleen vragen: wat is er gebeurd? Maar: waar neemt de kans op falen toe voordat het incident zichtbaar wordt?

Tweede vraag: weten we wat we beloven? Welke veiligheids-, gezondheids- en milieubeloften doen we expliciet en impliciet? Hoe ambitieus zijn die? Zijn ze consistent met onze risk appetite? En durven we helder te zijn over wat we wel en niet kunnen garanderen? Voor

leiderschap is dit cruciaal. Want vertrouwen wordt niet alleen beschadigd door slechte prestaties. Het wordt ook beschadigd door onduidelijke of ongeloofwaardige beloften.

Derde vraag: begrijpen we hoe vertrouwen ontstaat? Hoe vormen stakeholders hun oordeel over risico's? Welke rol spelen eerdere incidenten, media, emoties, rechtvaardigheid, identiteit, politieke context en vertrouwen in instituties? Dit vraagt van veiligheidsprofessionals iets extra's. Niet alleen technische analyse, maar maatschappelijke analyse.

Vierde vraag: is onze informatie geloofwaardig? Informatie moet niet alleen correct zijn. Zij moet ook relevant, eerlijk, begrijpelijk en toetsbaar zijn. Er is een belangrijk verschil tussen "klopt de kennis?" en "kan ik erop vertrouwen dat u mij vertelt wat ik moet weten, ook als dat voor u ongemakkelijk is?" Veel organisaties investeren in het eerste. Maar stakeholders beoordelen vaak het tweede.

Vijfde vraag: weten we wie wanneer belangrijk is? Stakeholdermanagement moet dynamisch worden. Wie vandaag weinig invloed lijkt te hebben, kan morgen urgent worden door een incident, een mediabericht, een politieke motie, een rechtszaak of een online campagne. De omgeving staat niet stil. Daarom is engagement geen jaarlijkse sessie met een verslag. Het is een continu leerproces.

Wat betekent dit voor de praktijk? Ik wil drie overwegingen meegeven.

De eerste overweging: **performance versus belofte**. Vraag uzelf af: zijn onze publieke SHE-beloften realistischer of ambitieuzer dan onze voorspelbaarheid toelaat? Zeggen we "we hebben het onder controle", terwijl intern bekend is dat bepaalde barrières structureel aandacht vragen? Zeggen we "de risico's zijn beheerst", terwijl we eigenlijk bedoelen: binnen de wettelijke kaders achten wij het risico acceptabel? Dat verschil lijkt klein. Maar maatschappelijk is het enorm.

De tweede overweging: **data versus geloofwaardigheid**. Vraag uzelf af: delen we indicatoren die stakeholders begrijpen en relevant vinden? Of delen we vooral indicatoren die wij technisch of juridisch comfortabel vinden? Een omwonende heeft weinig aan een abstracte KPI als die niet uitlegt wat het betekent voor geur, geluid, explosierisico, incidentrespons of gezondheid. Meer data is niet automatisch meer vertrouwen. Betekenisvolle data is data die aansluit bij de vraag van de stakeholder.

De derde overweging: **engagement versus afvinken**. Vraag uzelf af: is onze stakeholderdialoog echt tweerichtingsverkeer? Of is het vooral reputatiemanagement met inspraakvormgeving? Luisteren is pas governance als het invloed kan hebben op besluiten. Als participatie niets kan veranderen, wordt het decor. En mensen herkennen decor sneller dan wij denken.

7. Wat betekent “Veiligheid vooruit” dan echt?



Het thema van dit congres is: “*Veiligheid vooruit: omarm technologie, bouw aan vertrouwen.*”

Dat thema is goed gekozen. Maar het bevat ook een waarschuwing. Als we technologie omarmen zonder vertrouwen te bouwen, vergroten we misschien de technische beheersing, maar niet automatisch de maatschappelijke legitimiteit.

> Een predictive dashboard kan intern revolutionair zijn, maar extern niets betekenen als niemand begrijpt wat het voorspelt, wat de onzekerheid is, wie erop acteert en wat er gebeurt als de indicator rood wordt.
>
> Een ESG-rapport kan volledig zijn volgens een standaard, maar toch ongeloofwaardig voelen als dilemma’s ontbreken.
>
> Een vergunning kan juridisch robuust zijn, maar sociaal kwetsbaar als betrokkenen het proces als oneerlijk ervaren.

Veiligheid vooruit betekent daarom voor mij meer dan slimmer meten.

> Het betekent voorspelbaarder presteren.
>
> Het betekent explicieter zijn over risk appetite.
>
> Het betekent eerlijker communiceren over onzekerheid.
>
> Het betekent stakeholderanalyse dynamisch maken.
>
> Het betekent engagement organiseren als leerproces.

Het betekent erkennen dat veiligheid niet alleen wordt bepaald in de controlekamer, maar ook in de relatie tussen bedrijf en samenleving. En dat brengt mij bij mijn slotboodschap.

De procesindustrie heeft veel geleerd van grote incidenten. We hebben technische barrières gebouwd. Organisatorische barrières. Procedurele barrières. Culturele barrières. En, die blijven allemaal noodzakelijk. Maar de volgende veiligheidsbarrière is geen technische barrière. Het is vertrouwen.

> Niet vertrouwen als gevoelige bijzaak.
>
> Niet vertrouwen als communicatieprobleem.
>
> Niet vertrouwen als iets wat de buitenwereld ons verschuldigd is omdat wij aan de regels voldoen.

Maar vertrouwen als strategische, bestuurlijke en morele opdracht.

Want uiteindelijk is de vraag niet alleen of wij kunnen aantonen dat iets veilig is. De vraag is: of anderen goede redenen hebben om ons te geloven.

Dus als u morgen teruggaat naar uw organisatie, stel dan niet alleen de vraag: Voldoen we aan de norm? Stel ook de vragen: Welke belofte doen wij eigenlijk? Kunnen we die voorspelbaar waarmaken? En voor wie is ons bewijs overtuigend?

Compliance geeft u een vergunning. Maar vertrouwen geeft u ruimte.

De volgende veiligheidsbarrière is geen technische barrière. Het is vertrouwen!

Dank u wel.