

Hands on ICT

Continuïteit in de industrie

Waarom IT en telecom onlosmakelijk verbonden zijn



Inleiding

De industrie is de afgelopen jaren sterk gedigitaliseerd. Productieprocessen zijn afhankelijk geworden van ERP-systemen, cloudapplicaties, mobiele devices, datastromen, netwerkverbindingen, telefonie en security. Deze digitalisering biedt organisaties meer inzicht, flexibiliteit en efficiëntie. Tegelijkertijd zorgt zij voor een groeiende afhankelijkheid van technologie en connectiviteit. Wanneer bereikbaarheid wegvalt, valt er namelijk meer weg dan alleen communicatie. Productieprocessen vertragen, medewerkers verliezen toegang tot systemen en verstoringen werken direct door in de operatie.

Waarom bereikbaarheid meer is dan communicatie

In veel productieomgevingen wordt bereikbaarheid nog geassocieerd met telefonie of internettoegang. In de praktijk is bereikbaarheid uitgegroeid tot een essentiële productiefactor. Een operator die een storing niet kan escaleren, een planner die geen actuele informatie ontvangt of een magazijnmedewerker die geen orders kan verwerken: het zijn voorbeelden van situaties waarin een verbingsprobleem direct gevolgen heeft voor de continuïteit van de organisatie.

Omdat systemen, connectiviteit en communicatie steeds sterker met elkaar verweven zijn, kunnen IT, telecom en bereikbaarheid niet langer los van elkaar worden gezien. Om grip te houden op continuïteit is inzicht nodig in de afhankelijkheden binnen deze digitale keten.

Doel van de whitepaper

Deze whitepaper laat zien waar kwetsbaarheden ontstaan binnen moderne productieomgevingen en waarom IT, telecom en connectiviteit onlosmakelijk met elkaar verbonden zijn. Daarnaast biedt het document praktische handvatten om risico's rondom bereikbaarheid, continuïteit en downtime inzichtelijk te maken.

Om deze inzichten te vertalen naar de eigen organisatie bevat deze whitepaper twee praktische checks. De Bereikbaarheidscheck helpt bij het beoordelen van de vier lagen van industriële bereikbaarheid, terwijl de Single Point of Failure Check inzicht geeft in kritieke afhankelijkheden die een productieomgeving kwetsbaar kunnen maken.

Bereikbaarheid is meer dan telefonie

Wanneer organisaties over bereikbaarheid praten, gaat het vaak als eerste over telefonie. Kunnen klanten ons bellen? Zijn collega's bereikbaar? Werkt de vaste of mobiele telefonie nog?

In een moderne productieomgeving is die definitie te beperkt. Bereikbaarheid gaat niet alleen over mensen die elkaar kunnen spreken, maar over de volledige keten die nodig is om de operatie draaiende te houden.

Een planner is afhankelijk van actuele informatie uit de productie. Een operator moet een storing kunnen melden of escaleren. Een magazijnmedewerker gebruikt scanners of tablets om orders te verwerken. Een monteur op locatie heeft toegang nodig tot de juiste systemen.

Ondertussen moeten ERP, MES, cloudapplicaties, netwerkverbindingen en beveiligingsoplossingen continu blijven samenwerken.

Als één van die schakels hapert, ontstaat er direct frictie in het proces. Een medewerker kan dan misschien nog wel bellen, maar niet bij de juiste data. Een applicatie draait nog, maar reageert te traag. Of een machine functioneert fysiek nog, maar wisselt geen actuele informatie meer uit met centrale systemen.

Bereikbaarheid gaat dus niet om één middel of één verbinding. Het gaat om de beschikbaarheid van de volledige digitale keten achter het productieproces. En juist daar ontstaat de kwetsbaarheid.



De industrie is afhankelijker geworden van digitale processen

Productiebedrijven zijn de afgelopen jaren sterk veranderd. Processen zijn slimmer, sneller en meer datagedreven geworden. Machines communiceren met systemen, orders worden digitaal verwerkt, planningen worden realtime aangepast en cloudapplicaties ondersteunen steeds vaker de dagelijkse operatie.

Die ontwikkeling biedt veel voordelen. Organisaties krijgen meer inzicht in hun productieproces, kunnen sneller schakelen en efficiënter werken. Data helpt om betere beslissingen te nemen. Mobiele devices maken medewerkers minder afhankelijk van een vaste werkplek. Cloudoplossingen zorgen voor meer flexibiliteit en schaalbaarheid.

Maar deze digitalisering heeft ook een keerzijde.

Hoe meer processen digitaal worden aangestuurd, hoe groter de afhankelijkheid van stabiele connectiviteit, betrouwbare systemen en veilige toegang.

Productie draait daardoor niet meer alleen op fysieke machines, maar op een samenspel van IT, telecom, netwerk, cloud en security.

Een storing in één onderdeel raakt zelden maar één proces.

Wanneer één onderdeel in die keten verstoord raakt, kan dat direct effect hebben op meerdere processen tegelijk. Een probleem dat technisch klein lijkt, kan daardoor operationeel veel groter worden. Daar komt bij dat veel IT-, telecom- en cloudomgevingen in de loop der jaren zijn opgebouwd uit losse onderdelen. Daardoor is niet altijd direct duidelijk waar een verstoring ontstaat, welke processen geraakt worden en wie verantwoordelijk is voor herstel.

De vraag is daarom niet meer alleen of de IT werkt.

De betere vraag is: blijft de operatie bereikbaar wanneer er iets misgaat?



Wat onbereikbaarheid kost

De kosten van productiestilstand worden vaak onderschat. Niet omdat organisaties de impact niet serieus nemen, maar omdat er meestal vooral wordt gekeken naar de duur van de storing zelf.

Een systeem ligt één uur stil. Een verbinding valt tijdelijk weg. Een applicatie is kort niet bereikbaar. Op papier lijkt de schade dan overzichtelijk. In de praktijk werkt een verstoring vaak veel langer door.

Na een storing moeten productielijnen opnieuw worden opgestart, planningen worden aangepast en medewerkers moeten processen handmatig herstellen. Levermomenten komen onder druk te staan, logistiek moet opnieuw worden afgestemd en IT-teams zijn tijd kwijt aan analyse, herstel en afstemming met leveranciers.

De werkelijke impact zit dus niet alleen in de storing, maar in de kettingreactie daarna.

Stel: een productiebedrijf werkt met een centrale ERP-omgeving voor planning, orderverwerking, voorraadbeheer en logistiek. Voor veel productiebedrijven vormt ERP het centrale punt waar deze processen samenkomen. Zodra dat systeem niet betrouwbaar bereikbaar is, ontstaat er direct onzekerheid op de werkvloer.

Welke orders moeten worden geproduceerd? Welke materialen zijn beschikbaar? Welke zendingen moeten vandaag nog vertrekken? En welke voorraadgegevens zijn nog actueel?

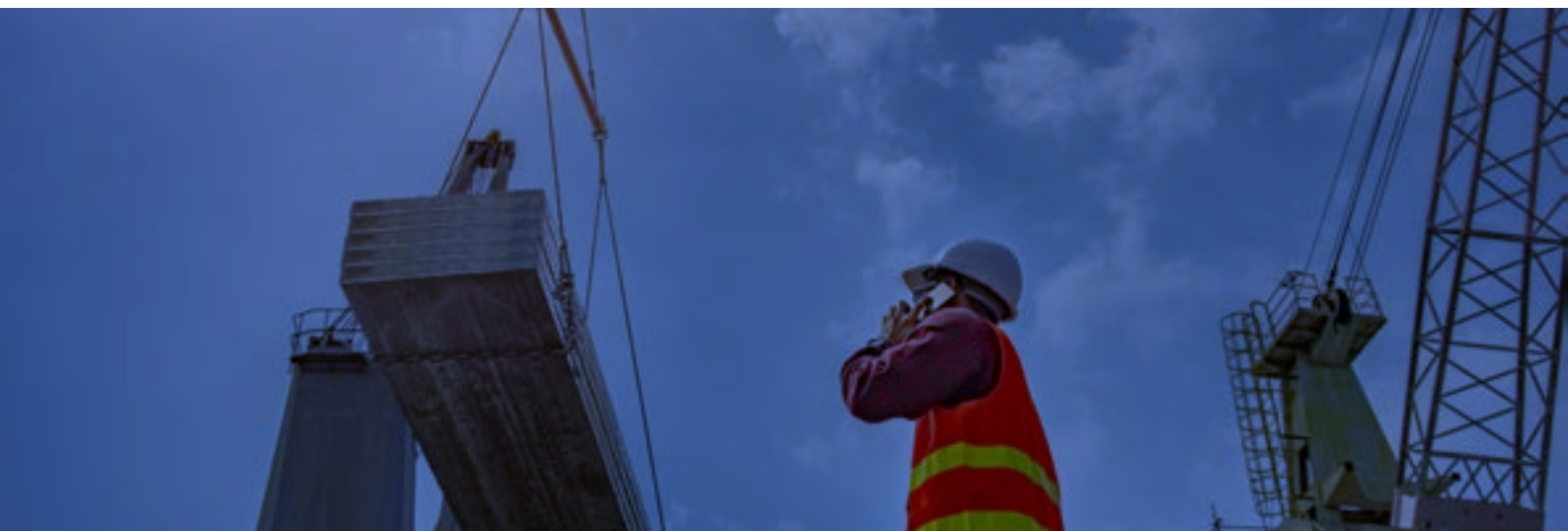
De lijn valt misschien niet volledig stil, maar het proces hapert. Medewerkers gaan bellen, mailen of handmatig lijsten bijwerken. De planning schuift, het magazijn loopt achter en de kans op fouten neemt toe. Naarmate een verstoring langer duurt, groeit ook de impact op productie, logistiek en levering.

Een ERP-storing hoeft daarbij niet altijd veroorzaakt te worden door het ERP-systeem zelf. De oorzaak kan ook liggen in de internetverbinding, het netwerk, authenticatie, storage, cloudservices of een onderliggende koppeling. Juist daardoor is het belangrijk om niet alleen naar één applicatie te kijken, maar naar de volledige keten die nodig is om die applicatie beschikbaar te houden.

Dat is waarom onbereikbaarheid zo kostbaar is.

Niet elke storing leidt direct tot volledige stilstand, maar zelfs gedeeltelijke verstoring kan genoeg zijn om productie, logistiek en planning uit balans te brengen. De kosten zitten dan niet alleen in verloren productie-output, maar ook in herstelwerk, handmatige correcties, spoedoplossingen, productiviteitsverlies en reputatieschade richting klanten of ketenpartners.

Daarom is het belangrijk om bereikbaarheid niet te zien als technische randvoorwaarde, maar als directe voorwaarde voor bedrijfscontinuïteit.



De vier lagen van industriële bereikbaarheid

Om grip te krijgen op bereikbaarheid, is het belangrijk om verder te kijken dan losse verbindingen of losse diensten. In de industrie bestaat bereikbaarheid uit meerdere lagen die samen bepalen of de operatie kan blijven draaien.

Mensen

De eerste laag is de bereikbaarheid van mensen. Medewerkers op kantoor, in productie, in het magazijn, in de buitendienst en in het management moeten elkaar snel kunnen bereiken. Wanneer communicatie hapert, vertraagt besluitvorming. Storingen worden later opgepakt en informatie blijft hangen bij één persoon of afdeling. Zeker in een productieomgeving, waar tijd en afstemming cruciaal zijn, heeft dat direct effect op de operatie.

Systemen

De tweede laag is de bereikbaarheid van systemen. ERP, MES, cloudapplicaties, planningssystemen en voorraadbeheer vormen het digitale hart van veel productiebedrijven. Als deze systemen niet bereikbaar zijn, ontstaat direct impact op orders, planning, voorraad en logistiek. Daarbij hoeft een systeem niet volledig uit te vallen om problemen te veroorzaken. Traagheid, haperingen of onbetrouwbare verbindingen kunnen al genoeg zijn om processen te vertragen.

Devices

De derde laag bestaat uit machines en devices. Machines, sensoren, scanners, tablets, mobiele telefoons en andere devices zijn steeds sterker verbonden met centrale systemen. Zij leveren data, ontvangen instructies en ondersteunen medewerkers in hun dagelijkse werk. Wanneer deze communicatie wordt onderbroken, ontstaan fouten of vertragingen. Een scanner zonder verbinding, een tablet die niet synchroniseert of een machine die geen data kan uitwisselen, kan het proces al verstoren.

Locaties

De vierde laag is de bereikbaarheid van locaties. Veel productiebedrijven werken met meerdere vestigingen, magazijnen, buitenterreinen of mobiele teams. Een locatie die tijdelijk geen toegang heeft tot centrale systemen, raakt geïsoleerd. Een buitenterrein met slechte mobiele dekking zorgt voor handmatige processen. Een magazijn met instabiele wifi vertraagt orderverwerking.

Industriële bereikbaarheid vraagt daarom om een inrichting die rekening houdt met de werkelijkheid van de operatie. Niet alleen kantoorplekken moeten goed verbonden zijn, maar ook productiehallen, machines, loodsen, magazijnen, buitenterreinen en mobiele medewerkers.

Bereikbaarheidscheck

Wil jij weten of alle lagen binnen jouw organisatie goed bereikbaar zijn? Doe dan de bereikbaarheidscheck en ontdek waar mogelijke kwetsbaarheden zitten in jouw IT-, telecom- en connectiviteitsomgeving.

[Doe de check](#)



Waarom één verbinding geen continuïteitsstrategie is

Veel organisaties hebben een betrouwbare internetverbinding en gaan ervan uit dat daarmee de basis goed geregeld is. Maar in moderne productieomgevingen is één verbinding vaak niet voldoende.

Veel productiebedrijven hebben ongemerkt één of meerdere single points of failure in hun omgeving. Dat klinkt technisch, maar de impact is allesbehalve technisch. Een single point of failure is een onderdeel waarvan uitval direct leidt tot verstoring van een groter proces.

Denk aan een internetverbinding die wegvalt, een firewall die uitvalt of een cloudomgeving die tijdelijk niet bereikbaar is. Wanneer productie, ERP, cloudapplicaties, telefonie en machinecommunicatie afhankelijk zijn van hetzelfde onderdeel, kan één storing voldoende zijn om de operatie stil te leggen.

Het risico zit daarbij niet alleen in de kans dat iets uitvalt, maar vooral in de impact wanneer dat gebeurt. De vraag is daarom niet of een organisatie internet heeft geregeld. De vraag is: wat gebeurt er wanneer die verbinding wegvalt?

Veel organisaties investeren in een tweede verbinding, mobiele fallback of 4G/5G-oplossing. Dat is een belangrijke stap, maar nog geen garantie voor continuïteit. Redundantie is pas effectief wanneer verkeer automatisch kan

overschakelen, verbindingen technisch voldoende gescheiden zijn en vooraf duidelijk is welke processen prioriteit krijgen bij uitval.

In de praktijk blijkt een tweede verbinding namelijk niet altijd echte continuïteit te bieden. Soms lopen beide verbindingen via dezelfde onderliggende infrastructuur, dezelfde provider of zelfs hetzelfde fysieke traject. In andere situaties is failover wel mogelijk, maar moet deze handmatig worden geactiveerd. Op papier is er dan een alternatief aanwezig, terwijl de organisatie tijdens een storing nog steeds kwetsbaar blijft.

Daarom draait continuïteit niet om dubbele componenten, maar om inzicht in afhankelijkheden. Welke systemen zijn bedrijfskritisch? Welke verbindingen ondersteunen die systemen? Welke processen moeten blijven draaien? En hoe snel moet herstel plaatsvinden voordat productie, planning of logistiek geraakt wordt?

Beschikbaarheid is geen toeval. Het is een ontwerpkeuze.

De eerste stap begint met inzicht. Want pas wanneer duidelijk is waar mogelijke single points of failure zich bevinden, kunnen organisaties gericht werken aan een omgeving die bestand is tegen verstoringen en downtime.

Single Point of Failure Check

Wil je weten waar de grootste risico's binnen jouw organisatie zitten? Doe dan de Single Point of Failure Check en ontdek welke afhankelijkheden een bedreiging vormen voor de continuïteit van jouw productieomgeving.

[Doe de check](#)



Losse leveranciers vertragen herstel

Veel IT- en telecomomgevingen zijn in de loop der jaren opgebouwd uit losse onderdelen. De internetverbinding wordt geleverd door de ene partij, telefonie door een andere, cloudbeheer door een derde en security door weer een andere specialist.

Zolang alles werkt, lijkt dat beheersbaar. Maar bij een storing wordt de kwetsbaarheid zichtbaar.

Een applicatie die niet bereikbaar is, kan worden veroorzaakt door een cloudprobleem, netwerkprobleem, firewallinstelling, wifi-issues, mobiele verbinding of storing bij een leverancier. In een versnipperde omgeving kijkt iedere partij vaak naar het eigen onderdeel. Daardoor ontstaat vertraging in analyse en herstel.

De operatie heeft daar weinig aan. Voor een productiebedrijf telt niet welke leverancier technisch gelijk heeft. Het telt hoe snel de productie weer stabiel draait.

Wanneer niemand verantwoordelijkheid neemt voor de totale keten, wordt de IT-manager al snel coördinator tussen leveranciers. Er wordt gebeld, doorgeschakeld, nagevraagd en geëscaleerd, terwijl de oorzaak nog steeds niet helder is. Ondertussen merkt de operatie vooral dat herstel langer duurt dan nodig.

Een single point of failure hoeft bovendien niet altijd technisch te zijn. Ook kennis, documentatie of verantwoordelijkheid kan een kwetsbaar punt vormen. Wanneer maar één leverancier, beheerder of medewerker weet hoe een kritieke koppeling werkt, ontstaat er alsnog afhankelijkheid van één schakel.

Centrale regie helpt om die afhankelijkheden zichtbaar te maken voordat ze een risico worden. Niet omdat alle technologie van één leverancier moet komen, maar omdat iemand overzicht moet hebben over de volledige keten: van verbinding tot werkplek, van telefonie tot cloud, van firewall tot monitoring.

Een geïntegreerde aanpak zorgt voor meer grip, snellere afstemming en duidelijkere verantwoordelijkheid.



Security hoort bij bereikbaarheid

Bereikbaarheid en security worden nog vaak als aparte onderwerpen behandeld. In werkelijkheid zijn ze nauw met elkaar verbonden.

Een omgeving die niet veilig is ingericht, is uiteindelijk ook niet betrouwbaar bereikbaar.

In productieomgevingen zijn de gevolgen van securityrisico's groot. Niet alleen omdat data beschermd moet worden, maar omdat verstoringen in systemen, toegang of netwerk direct invloed kunnen hebben op de operatie. Een security-incident kan leiden tot uitval, afsluiting van systemen, verlies van toegang of vertraging in herstel.

Daarom moet bereikbaarheid altijd veilig worden ingericht.

Dat betekent dat toegang tot systemen en applicaties goed geregeld moet zijn, dat firewalls en netwerken logisch moeten worden ingericht en dat mobiele devices beschermd moeten zijn. Ook netwerksegmentatie, monitoring, rechtenbeheer en het tijdig bijwerken van systemen spelen hierin een belangrijke rol.

In de industrie gaat security niet alleen over bescherming tegen dreigingen. Het gaat ook over het borgen van beschikbaarheid.

Een bereikbare omgeving moet dus stabiel, schaalbaar én veilig zijn.



Monitoring: weten wat er gebeurt voordat productie geraakt wordt

Veel organisaties ontdekken bereikbaarheidsproblemen pas wanneer medewerkers ze melden. Een applicatie reageert traag, een verbinding valt weg, wifi werkt niet goed in een deel van het magazijn of telefonie hapert. Op dat moment is de impact vaak al voelbaar in de operatie.

Monitoring helpt om problemen eerder zichtbaar te maken. Niet alleen nadat iets uitvalt, maar juist wanneer prestaties beginnen af te wijken. Denk aan oplopende vertraging, capaciteitsproblemen, instabiele verbindingen, terugkerende storingen of afwijkend netwerkgedrag.

Voor productiebedrijven is dat belangrijk, omdat kleine signalen snel kunnen uitgroeien tot grote verstoringen.

Met centrale monitoring ontstaat inzicht in de beschikbaarheid van verbindingen, prestaties van netwerk en internet, status van kritische systemen, werking van fallback en terugkerende verstoringen. Daardoor wordt sneller duidelijk waar risico's ontstaan en waar preventief moet worden ingegrepen.

Naast monitoring is testen essentieel. Een fallback- of failoveroplossing die nooit wordt getest, biedt vooral schijnzekerheid. In de praktijk ontdekken organisaties vaak pas tijdens een echte storing hoe hun omgeving reageert.

Daarom is het belangrijk om periodiek te testen of alternatieve verbindingen, herstelprocedures en escalatieafspraken werken zoals bedoeld. Niet alleen om te controleren of de techniek functioneert, maar ook om te zien wat de impact is op gebruikers, systemen en productieprocessen.

Een test maakt vaak afhankelijkheden zichtbaar die op papier niet direct opvallen.

Samen veranderen monitoring en testen de aanpak van reactief naar proactief. In plaats van wachten tot productie hinder ondervindt, kan eerder worden ingegrepen. Daardoor wordt niet alleen de kans op downtime kleiner, maar ook de hersteltijd wanneer er toch iets misgaat.



De rol van KPN en Hands on ICT

Industriële bereikbaarheid vraagt om een sterke basis én om regie over de volledige omgeving.

KPN biedt de stabiele communicatie- en connectiviteitsbasis. Denk aan internetverbindingen, mobiele telefonie, vaste telefonie en oplossingen voor moderne communicatie zoals Microsoft Teams Telefonie.

Hands on ICT zorgt voor de vertaling naar de praktijk van de organisatie. Niet alleen door diensten te leveren, maar door IT, telecom, security, monitoring en beheer in samenhang te brengen.

Die combinatie is belangrijk.

Een verbinding op zichzelf voorkomt geen productiestilstand. Een telefoonabonnement op zichzelf maakt een organisatie niet bereikbaar. Een fallback verbinding heeft pas waarde wanneer die goed is ontworpen, getest en beheerd.

De kracht zit in de samenhang.

Samen zorgen KPN en Hands on ICT voor een omgeving waarin internetverbindingen aansluiten op kritische processen, vaste en mobiele telefonie onderdeel zijn van één communicatieaanpak en medewerkers bereikbaar zijn op kantoor, mobiel en op de werkvloer. Zo ontstaat geen verzameling losse diensten, maar een geïntegreerde bereikbaarheidsomgeving.

Een omgeving die past bij de realiteit van moderne productie: digitaal, verbonden, mobiel, afhankelijk van data en gevoelig voor verstoring.

Wil je weten hoe bereikbaar jouw productieomgeving echt is?

Laat je huidige IT- en telecommunrichting toetsen en ontdek waar kwetsbaarheden zitten in connectiviteit, telefonie, mobiele bereikbaarheid, redundantie en beheer.

[Neem contact met ons op](#)

Contactgegevens

Hands on ICT
info@handsonict.nl
www.handsonict.nl
+31(0)88 - 181 1300

Weesp

Nesland 5a
1382 MZ Weesp

Zwolle

Schrevenweg 5
8024 HB Zwolle

Venlo

Prinsessesingel 20-26
5911 HT Venlo

