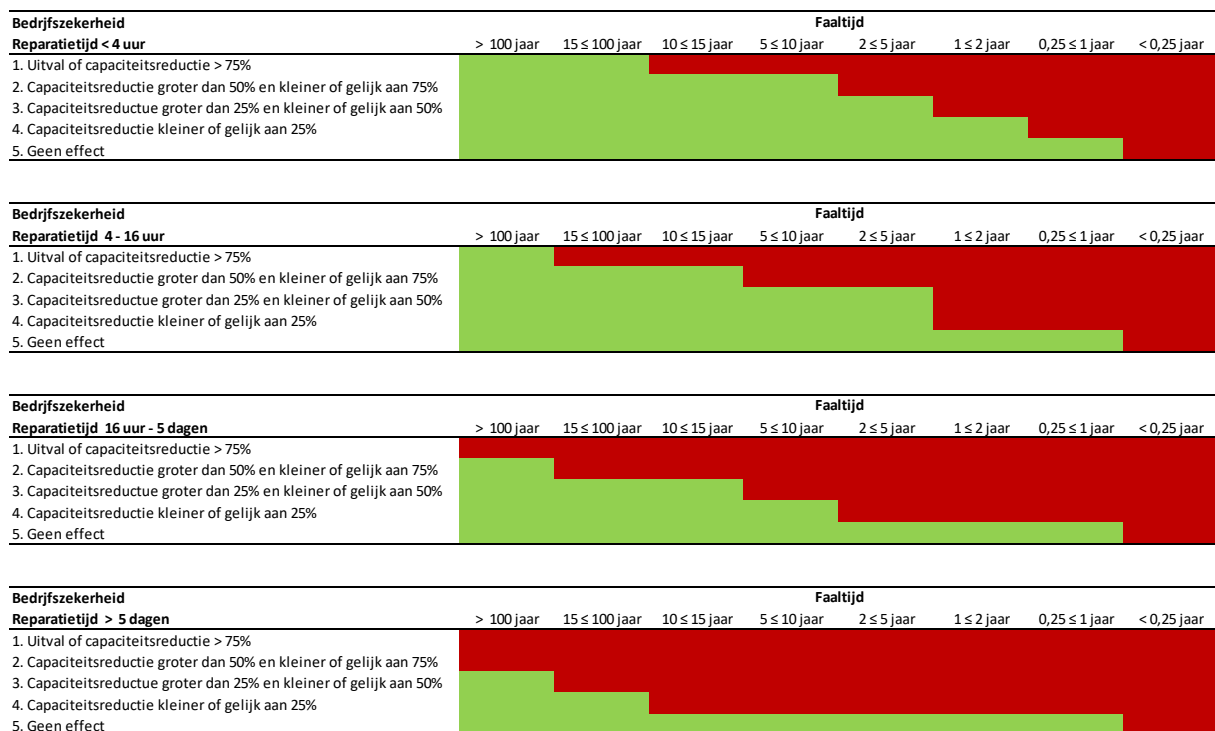


## Voldoet een ontwerp aan de eisen voor bedrijfszekerheid?

Bij de bouw van infrastructuur toont een opdrachtnemer aan dat het ontwerp aan de gestelde eisen voldoet. De opdrachtgever verstrekt hiervoor risicomatrices waarin de eisen besloten liggen. Risicomatrices geven bijvoorbeeld aan hoe vaak functioneel falen mag voorkomen en met welke uitvalsduur. Een voorbeeld van risicomatrices gericht op bedrijfszekerheid is opgenomen in Figuur 1.

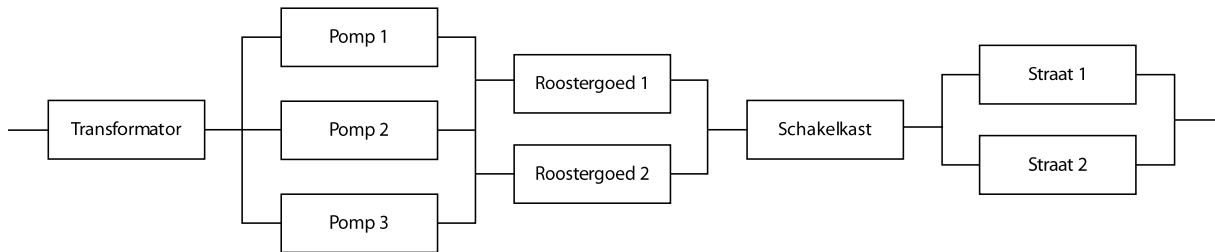
Een lastig probleem is de interpretatie van de eisen en de inzet van de risicomatrices. De opdrachtnemer stelt dat het ontwerp, dus het systeem, aan de eisen moet voldoen terwijl een opdrachtgever vaak alleen de afzonderlijke installaties toetst aan de risicomatrices. Zo komt het voor dat de installaties afzonderlijk al dan niet in een redundante opstelling aan de risicomatrices voldoen, maar het systeem als geheel niet. Dit komt omdat bij het beoordelen van afzonderlijke installaties de plek van deze installaties in het systeemontwerp niet wordt meegewogen. Installaties die in een parallelle opstelling staan zullen bij uitval minder kans geven op systeemuitval dan installaties in serie. Risicomatrices alleen zijn niet voldoende om dit risico in te schatten. Ook een systeemberekening is nodig.



Figuur 1: Voorbeeld van risicomatrices gericht op bedrijfszekerheid (bron: iAMPro)

### Systeemberekening

Een systeemberekening maakt het probleem en de oplossing helder. Wij volgen hier de internationale standaard IEC 61078: 2016 : Reliability Blok Diagrams en combineren deze met het gebruik van de risicomatrices. Om de aanpak toe te lichten gebruiken we een vereenvoudigde case van een afvalwatersysteemontwerp zoals geschetst in Figuur 2.



*Figuur 2: Vereenvoudigd en illustratief ontwerp van een waterzuiveringsinstallatie*

De faaltijd en faalduur van de afzonderlijke installaties is opgenomen in Tabel 1. De storingsfrequentie volgt meestal uit analyse van historische gegevens of uit faalfrequentiebibliotheken bijvoorbeeld die van RWS. De storingsfrequentie per uur is omgerekend naar gemiddelde tijd tussen faalgebeurtenissen in jaren. Deze faaltijden gaan uit van tijdig preventief onderhoud en vervanging. Maar dan nog, gaat er wel eens iets kapot. De reparatietijd volgt uit ervaringen van onderhoudsmonteurs en leveranciers. De laatste kolommen beoordelen de installaties aan de hand van de risicomatrices uit Figuur 1. Voor deze beoordeling zijn twee indicatoren nodig: de faaltijd en de reparatietijd of uitvalsduur. De beoordeling op deelsysteem en systeemniveau (kolommen E en F in Tabel 1) is het resultaat van een systeemberekening die in Tabel 2 is weergegeven.

*Tabel 1: Faaldata van de installaties*

Installaties	A. Storings- frequentie $\lambda$ (per uur)	B. Faaltijd MTBF (jaar)	C. Reparatietijd MTTR (uur)	D. Voldoet aan risicomatrix?	E. Voldoet aan risicomatrix?	F. Voldoet aan risicomatrix?
Transformator	1,10E-06	104	8	Ja	Ja	
Pomp 1	7,60E-05	2	24	Nee	Ja	
Pomp 2	7,60E-05	2	24	Nee	Ja	
Pomp 3	7,60E-05	2	24	Nee	Ja	
Roostergoed 1	1,10E-05	10	12	Nee	Ja	Nee
Roostergoed 2	1,10E-05	10	12	Nee	Ja	
Schakelkast	5,00E-07	228	8	Ja	Ja	
Straat 1	1,00E-05	11	24	Nee	Ja	
Straat 2	1,00E-05	11	24	Nee	Ja	

*Tabel 2: Systeemberekening*

Installaties	G. MTBF (jaar)	H. MTTR (uur)	I. Av. (-)	J. Av. (-)	K. BIF (-)	L. %BIF	M. CIF (-)	N. %CiF
Transformator	104	8	0,999991	0,999991	0,999996	49,98%	0,68317	67,86%
Pomp 1	2	24	0,998179	1,000000	0,000003	0,00%	0,00047	0,05%
Pomp 2	2	24	0,998179	1,000000	0,000003	0,00%	0,00047	0,05%
Pomp 3	2	24	0,998179	1,000000	0,000003	0,00%	0,00047	0,05%
Roostergoed 1	10	12	0,999868	1,000000	0,000132	0,01%	0,00135	0,13%
Roostergoed 2	10	12	0,999868	1,000000	0,000132	0,01%	0,00135	0,13%
Schakelkast	228	8	0,999996	0,999996	0,999991	49,98%	0,31053	30,84%
Straat 1	11	24	0,999760	1,000000	0,000240	0,01%	0,00447	0,44%
Straat 2	11	24	0,999760	1,000000	0,000240	0,01%	0,00447	0,44%
<b>Systeem</b>	<b>71</b>	<b>8</b>		<b>0,999987</b>				

Kolom G en H in Tabel 2 geven nogmaals de faaltijd en reparatietijd weer. Dit is de invoer die nodig is voor een systeemberekening en een risicobeoordeling op het niveau van installaties. De laatste regel geeft de systeem MTBF (71 jaar) en systeem MTTR (8 uur). We zien dat deze niet voldoen aan de risicomatrices in Figuur 1.

Kolom I geeft de gemiddelde beschikbaarheid van de installaties. Dit is het aandeel van de tijd waarin de installaties gemiddeld genomen functioneel zijn of de kans dat we op een willekeurige tijd een installatie werkend aantreffen. We moeten de systeemberekening op basis van beschikbaarheid maken omdat we te maken hebben met repareerbare systemen die na reparatie weer meedraaien in het systeem. Kolom J geeft opnieuw de beschikbaarheid weer, maar nu ook van de redundante opstellingen (de pompen, de roostergoedinstallaties en de zuiveringsstraten). De laatste regel van deze kolom geeft de systeembeschikbaarheid weer.

Kolom K geeft een indicator die we niet vaak tegenkomen in systeemberekeningen maar wel veel informatie geeft: de Birnbaum Importance Factor (BIF). De BIF geeft de kans dat een installatie kritiek wordt voor systeemfalen. We zien dat de transformator een zeer hoge BIF heeft. Dit kunnen we eenvoudig verklaren uit het systeemontwerp. Als de transformator faalt, dan faalt het systeem. Dit geldt ook voor de schakelkast. Kolom L laat procentueel zien wat de relatieve bijdrage van de installaties is aan systeemfalen. De transformator en de schakelkast nemen ieder bijna 50% voor hun rekening. Kortom, als we de beschikbaarheid van het systeem willen verbeteren dan kijken we het eerst naar deze twee. Hun onderlinge prioriteit halen we uit de volgende twee kolommen.

Kolom M (absoluut) en N (procentueel) geven een tweede informatieve indicator: de Criticality Importance Factor (CIF). De CIF is afgeleid van de BIF en weegt ook de faalkans (hier de niet-beschikbaarheid) van de installaties mee. Deze indicator vertelt ons wat de kans is dat het systeem faalt doordat de betreffende installatie faalt op het moment dat deze kritiek is. Omdat de transformator een hogere niet-beschikbaarheid heeft dan de schakelkast krijgt de transformator een hogere CIF. Als we op basis van CIF, keuzes moeten maken voor ontwerpaanpassing, maar ook voor onderhoud dan beginnen we bij de transformator, gevolgd door de schakelkast, daarna straat 1 en 2, de roostergoedinstallaties en de pompen.

De CIF is als indicator interessanter dan de BIF. We hebben de BIF echter nodig om de CIF te kunnen berekenen. Ook hebben we de BIF nodig om de MTBF van het systeem (laatste regel Tabel 2) te berekenen. Alleen de beschikbaarheid van het systeem vertelt ons niet zo veel. We weten immers nog niet hoe vaak en hoe lang het systeem gemiddeld stoort. De systeem MTBF en systeem MTTR nodig hebben om met de risicomatrices te beoordelen of het systeem aan de gestelde eisen voldoet.

### Conclusies

- Als eisen worden vastgelegd in risicomatrices dan is het ook goed om vast te leggen op welk niveau de risicomatrices gelden: component, installatie, installaties in redundante opstelling of systeem.
- Risicomatrices alleen zijn niet voldoende om aan te tonen dat een ontwerp aan de eisen voldoet. Aanvullend zijn systeemberekeningen nodig conform de IEC 61078: 2016
- De CIF is niet alleen een prachtige indicator voor ontwerpaanpassingen maar ook om prioriteiten in onderhoudsactiviteiten aan te brengen.

### Referentie

IEC 61078: 2016. International Standard Reliability Block Diagrams. Geneva, Switzerland: International Electrotechnical Commission (IEC).