

## HVAD ER RESILIENCE ENGINEERING? FRA SIKKERHED I TIL SIKKERHED II

Professor Erik Hollnagel,

Syddansk Universitet/Mines ParisTech og vitenskapelig rådgiver  
Institut for industriell økonomi og teknologiledelse, NTNU

### Sikkerhed I: At undgå at noget går galt

Sikkerhed har traditionelt været defineret gennem sin modsætning, dvs., manglende sikkerhed. En virksomhed anses for at være sikker, hvis der ikke er noget der går galt eller kan gå galt. I konsekvens af denne definition har Sikkerhed I traditionelt – og med god grund – fokuseret på f.eks. utilsigtede hændelser og ulykker. Denne tankegang betyder, at sikkerhed kan opnås ved først at finde årsagerne til,

være utilstrækkelige instruktioner, manglende information, for lidt tid, og ressourcer der ikke passer helt til kravene – eller omvendt. For at udføre en aktivitet er det derfor hele tiden nødvendigt at tilpasse arbejdet til situationen. Denne tilpasning er normalt både effektiv og nyttig, men kan nu og da føre til, at udviklingen forløber anderledes end forventet. Sikkerhed I kan imidlertid ikke beskrive disse forhold, og derfor ikke effektivt bidrage til at forbedre situationen.

### Hvad er Resilience Engineering?

Resilience Engineering er siden begyndelsen af det 21. århundrede blevet udviklet for at imødegå de nye sikkerhedsmæssige problemer, der opstår i komplekse socio-tekniske systemer. Resilience

4. Sikkerhed kan ikke isoleres fra produktivitet og kvalitet, eller omvendt. Sikkerhed er en forudsætning for produktivitet og kvalitet, lige som produktivitet og kvalitet er en forudsætning for sikkerhed.

En sikker virksomhed kan tilpasse sin funktion, så den kan fungere i forskellige - og vanskelige - situationer. Resilience kan defineres som 'et systems evne til at tilpasse sin måde at fungere på før, under eller efter ændringer og forstyrrelser, således at det kan opretholde sin virksomhed under både forventede og uventede forhold.' Dette kræver at virksomheden:

- Kan  *reagere*  på det, der sker. Dvs. vide hvad der skal gøres efter regelmæssige og uregelmæssige afbrydelser og forstyrrelser, enten ved at handle på en forberedt måde, eller ved at tilpasse sin normale funktion til situationen.
- Kan holde øje med (*monitere*) det, der kan påvirke og forstyrre den daglige funktion i den nærmeste fremtid. Overvågningen skal dække både det, der sker i omgivelserne, og det der sker i selve systemet, dvs. dets egen præstation.
- Kan  *lære*  af hvad der er sket, hvilket betyder at lære af erfaring, og især vælge de rigtige situationer at lære fra - både når det går godt og når det går galt.
- Kan vide hvad man kan *forvente*, dvs. hvordan man kan foregribe udviklingen, trusler og muligheder længere ud i fremtiden, såsom mulige ændringer, forstyrrelser, pres, og deres konsekvenser.

### Sikkerhed II: At sikre at noget går godt

Resilience Engineering leder til et forslag om Sikkerhed II, hvor definitionen af sikkerhed ændres fra at være 'at undgå at noget går galt' til at blive 'at sikre at noget går godt.' Denne ændring har flere interessante konsekvenser.

- Når man prøver at forhindre, at noget går galt, fremmer man ikke samtidigt, at noget går godt. Det er fordi, Sikkerhed I antager, at uheld og skader har specielle årsager, som man skal forsøge at eliminere eller svække. I modsætning hertil antager Sikkerhed II og resilience engineering at det er de samme tilpasninger, der ligger bag alle hændelser. Sikkerhed kan derfor opnås ved at fremme, at noget går godt.
- Ved at gå fra Sikkerhed I til Sikkerhed II mindskes forskellen mellem sikkerhed og kvalitet. Formålet er i begge tilfælde at noget lykkes og at man gør det rigtige. Men hvis formålet med kvalitet og sikkerhed er det samme, er der ikke nogen egentlig grund til at bruge to forskellige begreber. Sikkerhed og kvalitet er dermed ikke længere noget som skal forfølges i to parallelle spor, men i stedet to perspektiver på eller tolkninger af det daglige arbejde.
- Hvor Sikkerhed I som regel opfattes som en tilstand eller en kvalitet, så er Sikkerhed II noget der sker. Sikkerhed er ikke hvad man har, men hvad man gør! Man kan ikke være sikker, men man kan fungere på en sikker måde. Sikkerhed kan derfor ikke måles som resultater (eller som manglende resultater, f.eks. færre

ulykker). Sikkerhed må måles ved at karakterisere processen, dvs. den måde, hvorpå et arbejde udføres eller et forløb sker.

Formålet med Sikkerhed II og Resilience Engineering er at sikre sig, at enhver aktivitet går godt. En forudsætning for dette er, at man ved – eller kan få viden om – hvordan arbejdet rent faktisk sker. Sikkerhed I har søgt efter viden om hvorfor, hvornår og hvordan noget ikke virker. Men der er mere brug for viden om hvorfor, hvornår og hvordan noget virker! Forskningen må derfor fokusere på det, der faktisk sker i hverdagen – dvs. fokusere på processer snarere end resultater – og må omfatte alle niveauer af en virksomhed såvel som virksomheden som helhed. Det giver også god mening, fordi det er processerne man skal styre for at ændre resultaterne. Og man kan som bekendt kun styre noget, hvis man ved, hvordan det sker.

### Litteratur

Hollnagel, E., Paries, J., Woods, D. D. & Wreathall, J. (2011). Resilience engineering in practice: A guidebook. Farnham, UK: Ashgate.



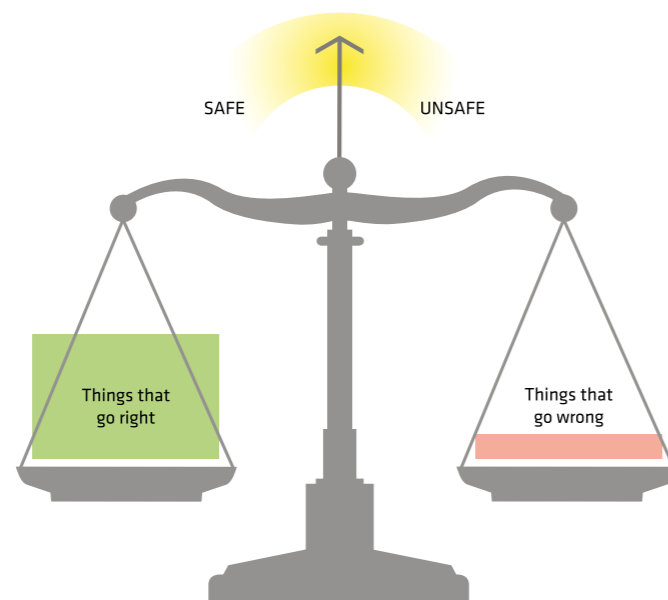
Foto: Mines ParisTech

### SAFETY AND RESILIENCE

#### MANAGE RESILIENCE

Solution:  
Enhance the abilities to respond, monitor, anticipate and learn

The goal of resilience management is to increase the number of things that go right.



#### MANAGE SAFETY

The goal of safety management is to reduce the number of things that go wrong

Solutions:  
Constrain performance by rules, procedures, barriers, and defences.

Illustrasjon: Erik Hollnagel

at noget går galt; dernæst at fjerne årsagerne eller svække mulige årsags-virknings relationer; og endelig at tælle hvor mange færre ting som går galt. Fordi Sikkerhed I primært har beskæftiget sig med det, der kan gå galt, har forskningen stort set negligeret det, der går godt, til trods for at dette sker langt oftere.

Sikkerhed I blev udviklet gennem det 19 og 20. århundrede, og var dominerende i slutningen af 1970'erne. Sikkerhed I har fra starten naturligt nok været rettet mod fejl og ulykker i tekniske systemer. Udviklingen siden 1970'erne har imidlertid gjort det nødvendigt at beskrive virksomheder som socio-tekniske snarere end som tekniske systemer. I et socio-teknisk system afhænger den daglige funktion af et effektivt samspil mellem sociale og tekniske faktorer, og det er derfor ikke længere tilstrækkeligt at teknologien fungerer sikkert. Socio-tekniske systemer er siden 1980'erne blevet stadig mere komplekse dels på grund af den uhæmmede teknologiske og samfundsmæssige udvikling og dels på grund af øget vertikal og horisontal integration. I en konkret situation vil der derfor typisk

Engineering har som udgangspunkt følgende forudsætninger:

1. Arbejdssituationer kan aldrig beskrives i alle detaljer fordi de socio-tekniske systemer er for komplekse. Enkeltpersoner og organisationer må derfor tilpasse, hvad de gør, så det passer til de aktuelle krav og ressourcer. Da ressourcer og tid er begrænsede, vil tilpasningerne aldrig kunne blive helt præcise men vil altid være tilnærmede.
2. Selv om mange uønskede hændelser kan forklares som resultat af fejl og mangler ved komponenter og funktioner, er der et stadigt voksende antal, for hvilke dette ikke er tilfældet. Disse hændelser kan i stedet forklares som et resultat af uventede sammenfald af tilnærmede tilpasninger, dvs., den uundgåelige variabilitet i hvordan et arbejde udføres.
3. Sikkerhed kan ikke opnås ved kun at reagere på det, der går galt. Fremtidige hændelser kan opstå på grund af en kombination af den variabilitet i udførelsen, der ellers opfattes som irrelevant for sikkerhed. Sikkerhedsarbejdet skal derfor være både proaktivt og reaktivt.