Beredskapsøvelser for IT-sikkerhet

Maria Bartnes Line og Nils Brede Moe

maria.b.line@sintef.no
nils.b.moe@sintef.no

SINTEF | NTNU
Det skapende universitet

God og effektiv hendelseshåndtering krever:

- Kryssfunksjonelle, selvstyrte team
- Evnen til å lære

Hvorfor må vi øve på å håndtere IT-angrep?

Hendelser er komplekse

Hvorfor må vi øve på å håndtere IT-angrep?

Effektiv håndtering begrenser konsekvensene

Hvorfor må vi øve på å håndtere IT-angrep?

IT-sikkerhetshendelser og målrettede angrep
er høyaktuelle trusler

”There are too many other tasks, so we haven’t had the time for it. Maybe that’s wrong, not to prioritize it.”

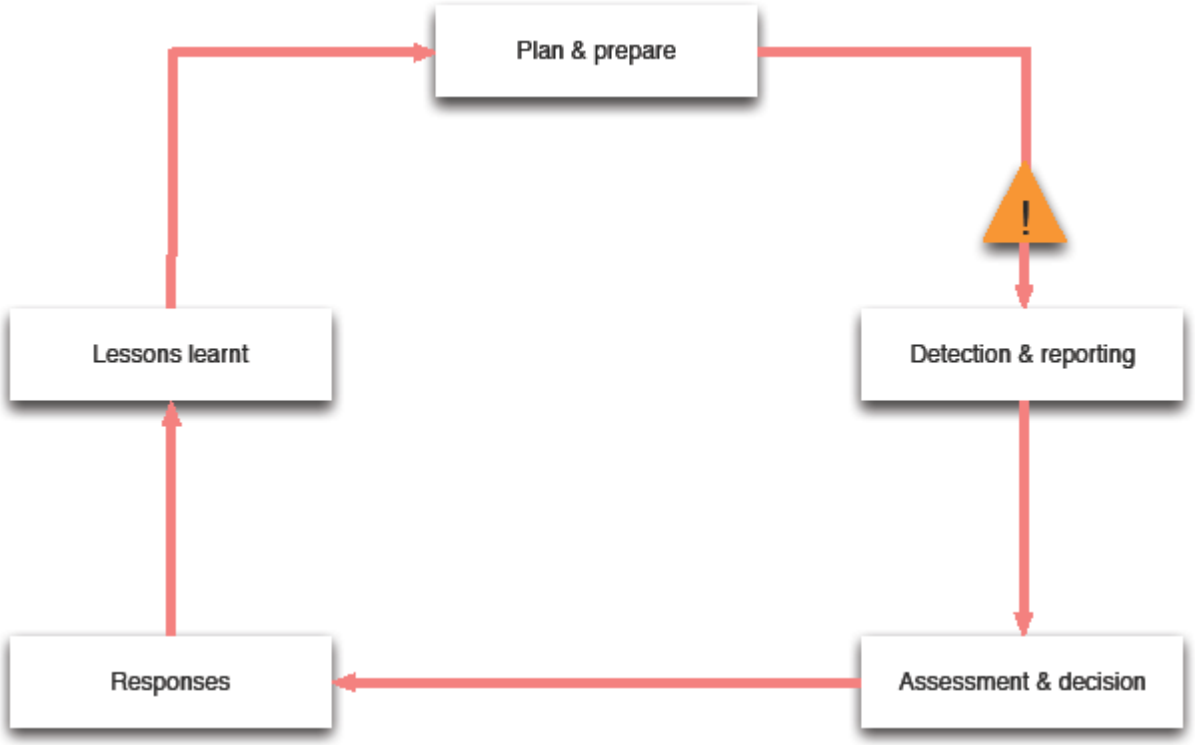
Control system manager in a large DSO

”As long as there has been no major attacks against the power industry in Norway, we consider the probability of an attack to be low. As soon as something happens, we will consider the probability to be increased.”

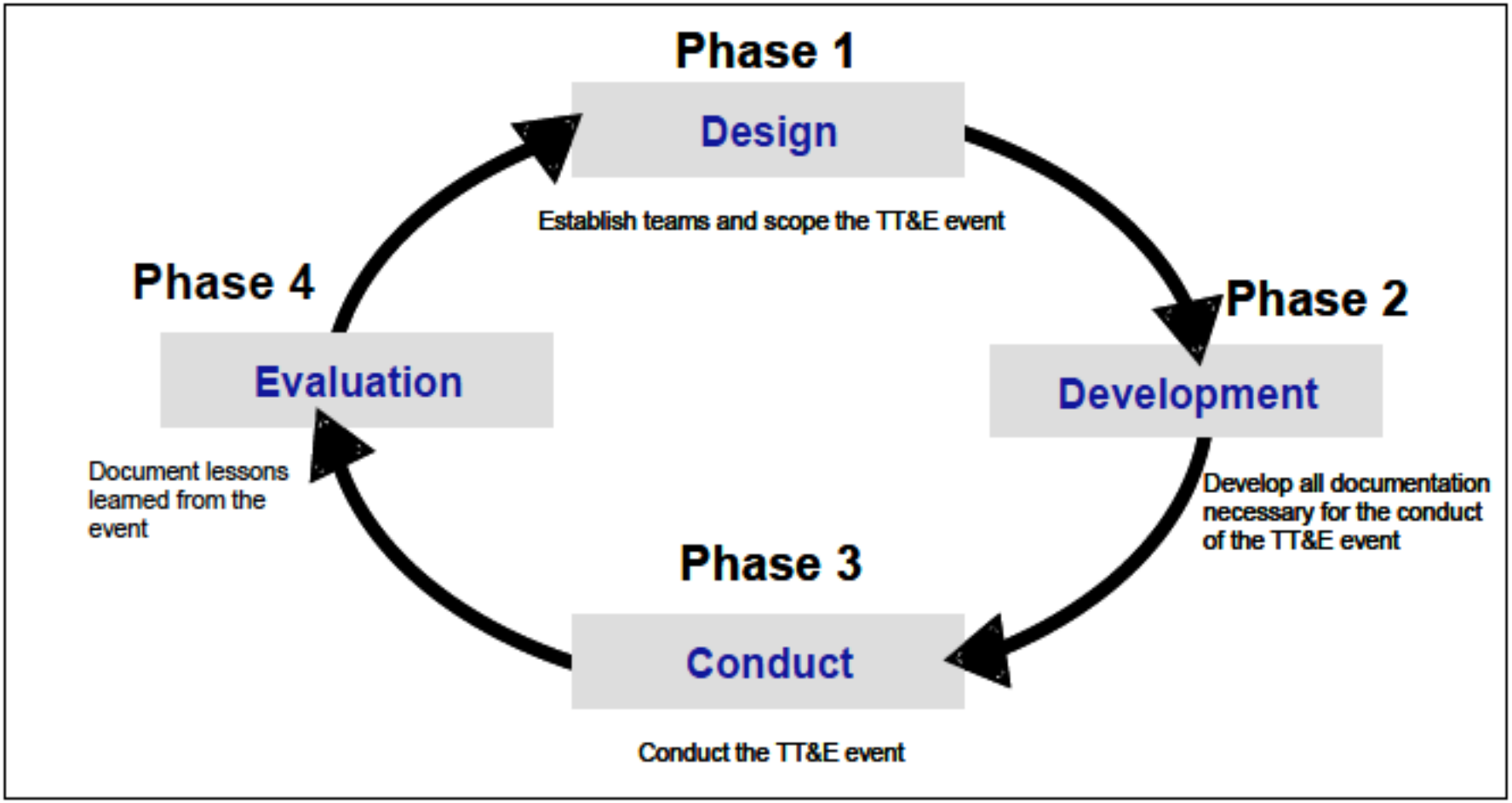
Control manager in a large DSO

(before the Dragonfly attack)

ISO/IEC 27035 – Information security incident management



SINTEF | NTNU
Det skapende universitet



Fra NIST SP 800-84: Guide to Test, Training and Exercise Programs for IT Plans and Capabilities

Øvelser

En veiledning i planlegging og gjennomføring av øvelser i NVE

53
2013

RAPPORT

SINTEF | NTNU
Det skapende universitet

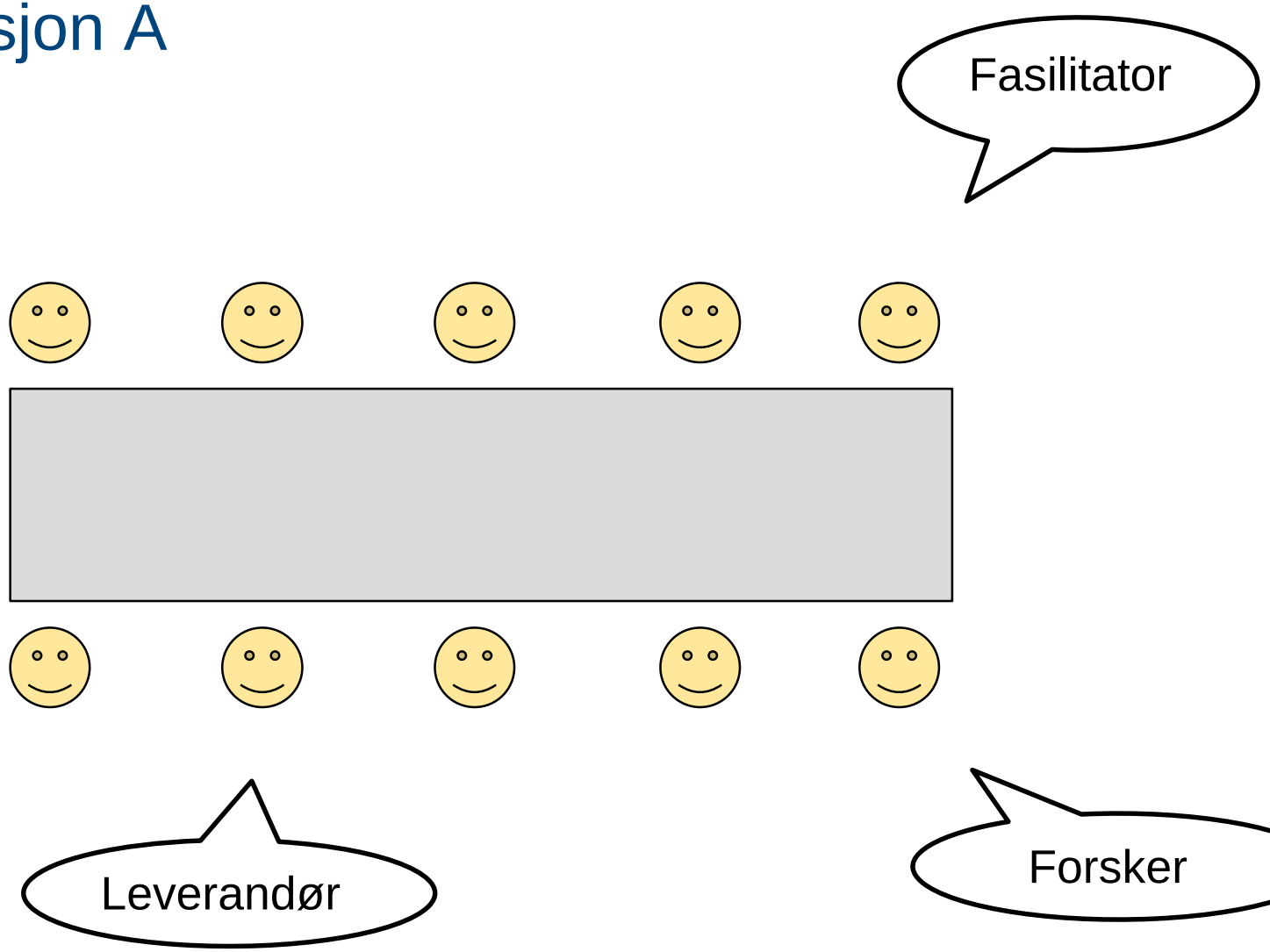
Observasjonsstudie av skrivebordsøvelser

- Hvilke utfordringer møter selskapet under gjennomføring av øvelsen?
- Hvordan kan disse utfordringene påvirke en reell hendelseshåndteringsprosess?
- Hvordan kan disse utfordringene imøtekommes under en øvelse?

Scenario i fem faser

1. Unormalt mye trafikk ut fra nettverket
2. To uker senere: SCADA-leverandør vil patche
3. Tre mnd etter første fase: strømløst i ett område, men ingen alarm
4. Strømløst i flere områder, fortsatt ingen alarmer
5. Mobilnett og Internett har falt ut

Organisasjon A

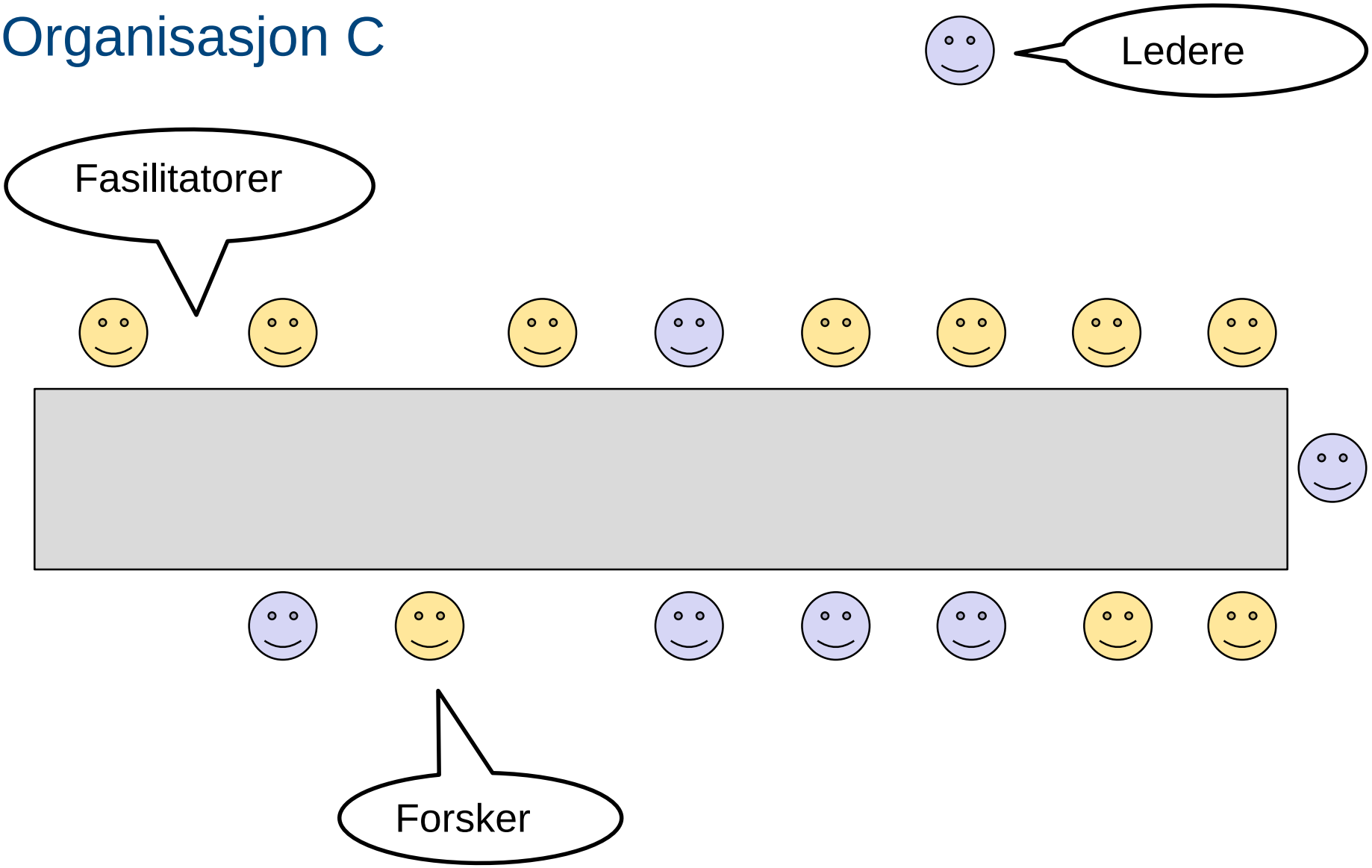


Organisasjon B

- Tre grupper, en observatør i hver gruppe.
- Beredskapsleder tilstede.

<bilder er fjernet>

Organisasjon C



”It is crucial to us as a small organization to have a professional, large, and competent IT supplier on which we can rely on in such situations.”

IT/IT security manager in a small DSO

God og effektiv hendelseshåndtering krever:

- Kryssfunksjonelle, selvstyrte team
- Evnen til å lære

Kryssfunksjonelle team

Driftsoperatør

Kommunikasjon/PR

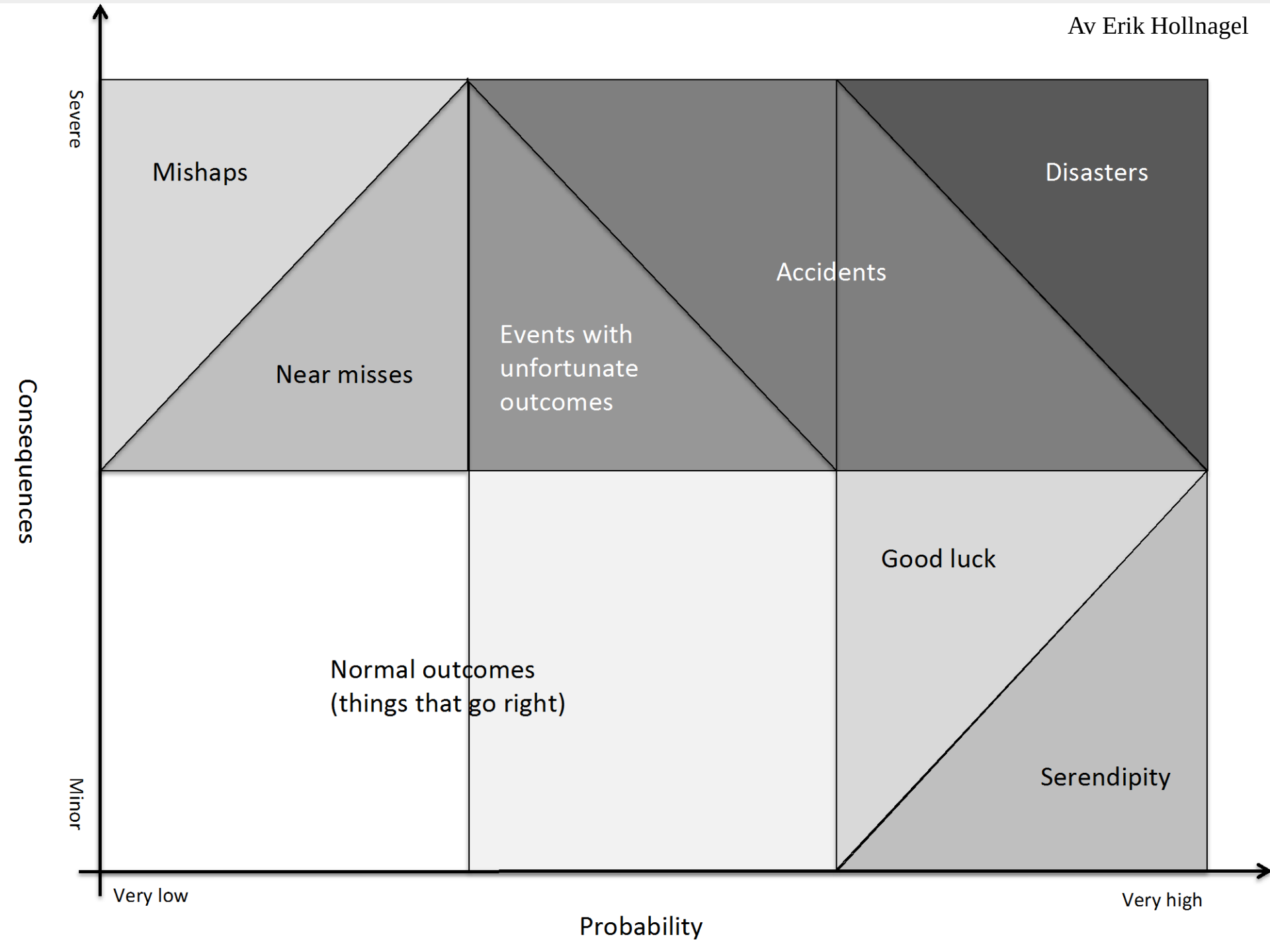
Beredskaps-
koordinator

IT-sikkerhetsansvarlig

Evnen til å lære

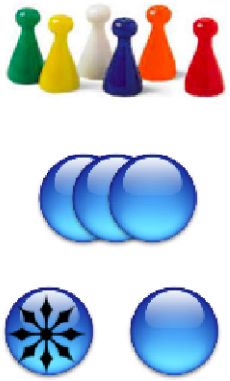
Enkeltløkke vs. dobbelløkke

Av Erik Hollnagel

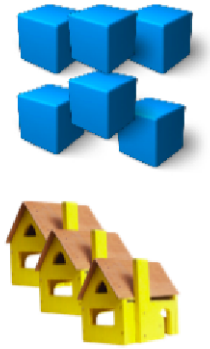


God og effektiv hendelseshåndtering krever:

- Kryssfunksjonelle, selvstyrte team
- Evnen til å lære



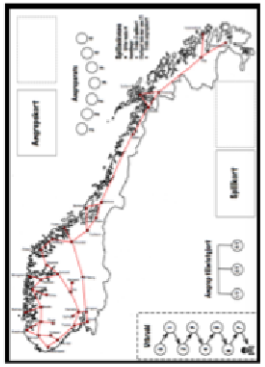
(a) 6 Spillerbrikker og 5 markører



(b) 30 Angrepskuber og 5 forskningstasjoner

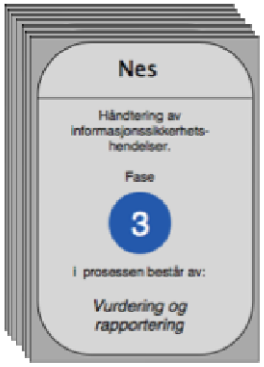
(c) 6 Rollekort

(d) 6 Angrep!!-kort



(a) Spillbrett

(b) 38 angrepskort med by



(c) 38 spillkort med by og fase

(d) Utvalg scenarie, spørsmål og "Visste du at.."-kort.

SINTEF | NTNU
Det skapende universitet

@SINTEF_Infosec

@mariabline

infosec.sintef.no

SINTEF | NTNU Det skapende universitet