A Case Study: Preparing for the Smart Grids

Identifying Current Practice for Information Security Incident Management in the Power Industry

Maria B. Line

PhD student/Research Scientist

NTNU/SINTEF

maria.b.line@item.ntnu.no

SINTEF | NTNU Det skapende universitet

And the next 40 minutes will be about…

- Smart Grids in brief
- A case study in the power industry
- Resilience Engineering

SINTEF | NTNU
Det skapende universitet

About NTNU/ITEM and SINTEF

- Norwegian Uni of Science and Technology, Dept of Telematics
  - Offers MSc/PhD in communication tech
  - Information security
  - 26 Profs, 41 PhD/PostDocs
- SINTEF
  - Largest independent, non-commercial research organization in Scandinavia
  - ~2000 employees
  - Contract research

Photo: Roger Midtstraum

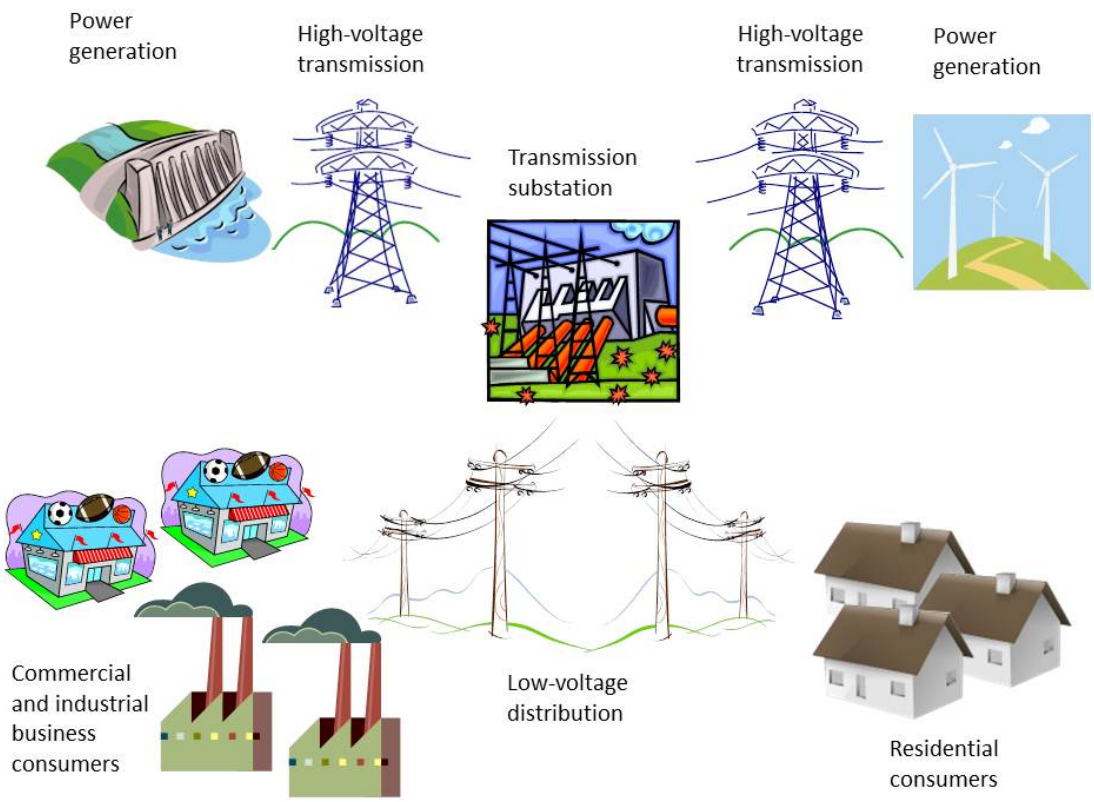
Photo: SINTEF

Technology for a better society

SINTEF | NTNU Det skapende universitet

Smart Grids in brief

- Modernization of the distribution grid (low voltage)
  - Monitoring and control
- Smart Meters: two-way communication
  - Automatic reading every hour
    ➡more correct invoicing
- Consumers will also be producers – prosumers:
  - Solar panels, wind mills, water heaters, electric cars



SINTEF | NTNU
Det skapende universitet

Main projects in Norway:

Smart Energy Hvaler, Smart City Halden, Demo Steinkjer, DeVID

NTE

DEMO STEINKJER
SMARTE ENERGILØSNINGER

smartgrid The Norwegian Smartgrid Centre

Lyse

Ruller ut AMS i skjærgården

Hytteparadiset Hvaler blir et slaraffenland også for smartgrid-entusiaster.

Skriv ut | Tips en venn | Motta nyheter på e-post | Tips redaksjonen | Facebook | Tweet

Av Leif Hamnes Publisert: 10.06.2011 kl. 12:50

Fredrikstad Energi skal bytte ut alle de 6700 strømmålerne på Hvaler allerede denne sommeren.

Det hyttetunge skjærgårdsparadiset egner seg spesielt som «testlaboratorium» for AMS.

Hvaler opplever ikke bare ekstreme forskjeller mellom effektbunner- og topper på grunn av den unormalt store variasjonen i folketallet.

Lokal kraftproduksjon (solcellepaneler) er også mer utbredt her enn det ville vært i et vanlig boligfelt.

Les også:

- AMS: Små nettselskaper kan få svarteper

AMS

- Olje- og energidepartementet (OED) vil framskynde innføringen av automatisk strømmåling (AMS) i Midt-Norge til 2013.

http://www.tu.no/it/article287762.ece

Smart Energi Hvaler

FEAS Fredrikstad EnergiNett AS

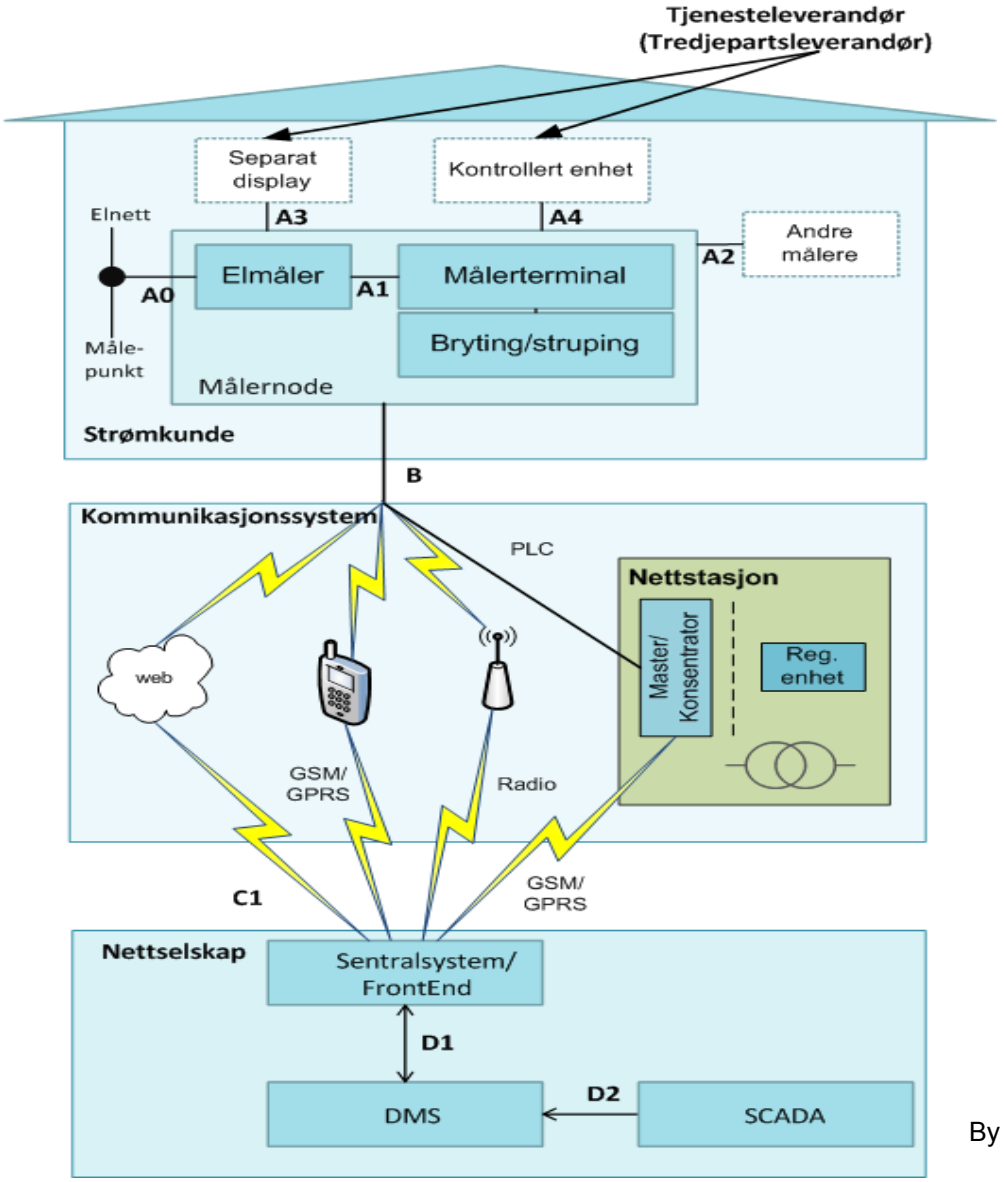
Fakta

- Demo Steinkjer er et nasjonalt pilotprosjekt
- Første trinn gjennomføres med 772 NTE-kunder i området Guldbergaunet og Byafossen på Steinkjer
- Resultatene fra prosjektet vil ha betydning for utvikling av fremtidens energisystem i Norge
- NTE og The Norwegian Smartgrid Centre star bak prosjektet

SINTEF | NTNU Det skapende universitet

AMI

Advanced metering infrastructure



By Hanne Sæle, SINTEF Energy

SINTEF | NTNU Det skapende universitet

Goals for Norway

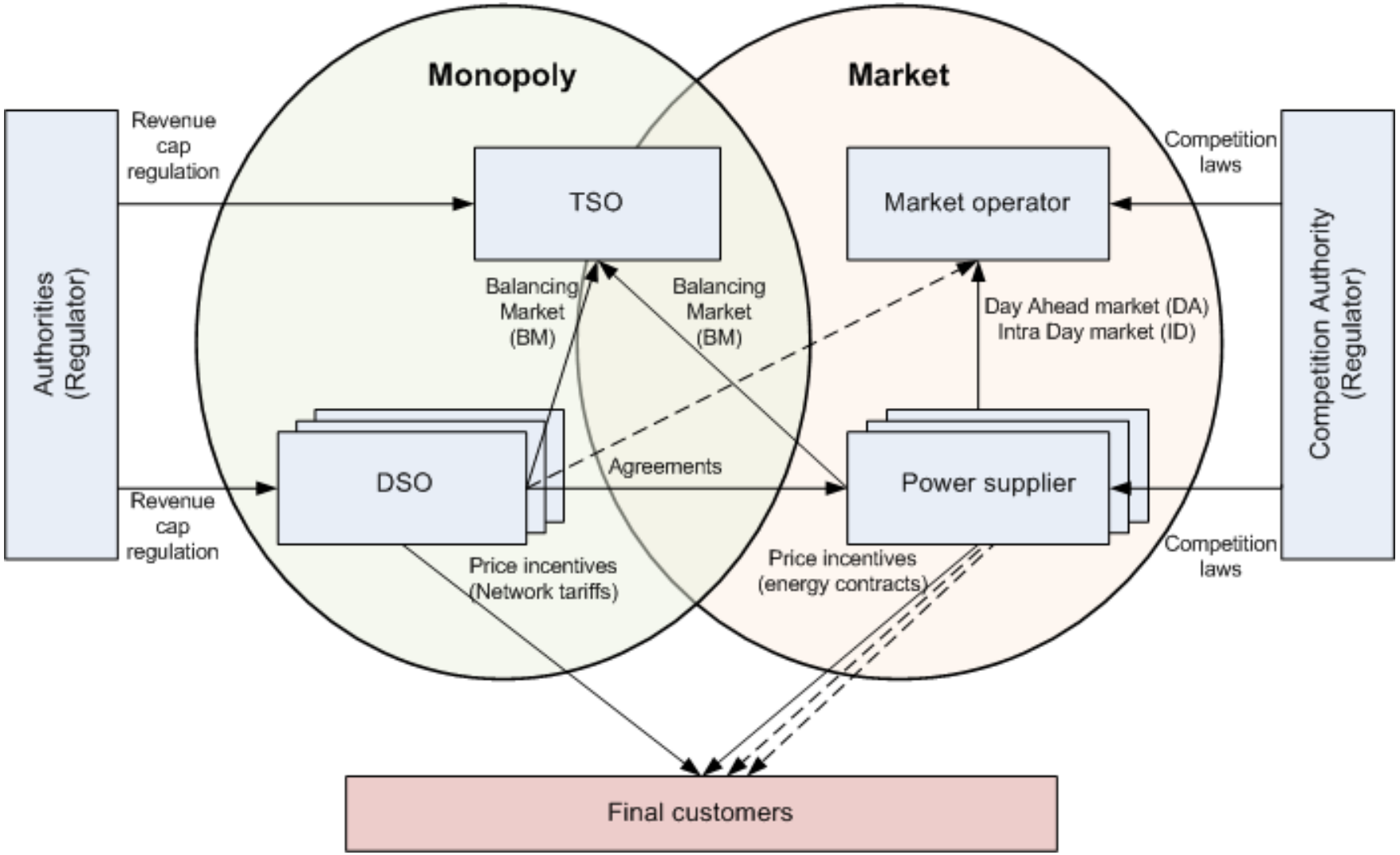
- AMI – smart meters – is the first step towards smart grids:
  - 2015-12-31(?): 80% of all power consumers should have a smart meter
  - 2019-1-1: Close to 100% should have a smart meter
- This is the responsibility of the distribution system operators.

Kamstrup

Aidon

SINTEF | NTNU Det skapende universitet

The power industry in Norway



By Hanne Sæle, SINTEF Energy

SINTEF | NTNU Det skapende universitet

Problem

USB drives left in car park as corporate espionage attack vector

A number of infected USB flash drives were recently left in the car park of Dutch chemical firm DSM in a failed corporate espionage attempt. According to a report from Dutch newspaper Dagblad De Limburger, these drives were planted by an unknown party in hopes that one or more of the company's employees would insert them into their office systems.

However, instead of plugging it into one of the company's systems, an employee who found one of the USB sticks turned it over to DSM's IT department. Upon examination, they discovered that the drives contained malware that was set to automatically run upon being inserted into a computer. The malware is said to have been a key logger designed to capture usernames and passwords, and access the company network to send them to an external site.

Upon finding this, the company blocked all access to the IP addresses which the malware attempted to contact. Because, they say, it was a clumsy attempt to steal data and as no damage was done, DSM decided not to contact the police.

FBI Warns Smart Meter Hacking May Cost Utility Companies $400 Million A Year

The FBI has seen an increase of smart meter hacks which allow consumers to reduced power bills by 50-75%. Crazy hacking skills are not required and can be accomplished by using a magnet to fake readings or hiring hackers to attack smart meters. The FBI warned the cost of smart meter fraud may cost utility companies $400 million per year.

By Ms. Smith on Tue, 04/10/12 - 2:47pm.

1 Comment Print + Briefcase What's this?

While smart meters going dumb has been called an "urban myth," and some Americans have padlocked their dumb meters to stop smart meters from being installed, others have happily welcomed and hacked smart meters in order to significantly reduce power bills by 50-75%. The FBI warned that hacking smart meters and the resulting fraudulent power bills may end up costing utility companies about $400 million per year.

Krebs on Security posted an FBI cyber intelligence bulletin in which the Feds report seeing an increase of smart meter hacking which allows "power theft" by consumers who want free electricity. In fact, hacking smart meters does not require mad skills, only modest hacking skills or hiring it done for a modest fee. Not all smart meters are equally smart, nor can all "block unauthorized modifications." The "FBI warns that insiders and individuals with only a moderate level of computer knowledge are likely able to compromise meters with low-cost tools and software readily available on the Internet."

Brian Krebs reported, "Citing confidential sources, the FBI said it believes former employees of the meter manufacturer and employees of the utility were altering the meters in exchange for cash and training others to do so. 'These individuals are charging $300 to $1,000 to reprogram residential meters, and about $3,000 to reprogram commercial meters,' the alert states."

ELEKTRISK KULTURSJOKK: Norske kraftingeniører vil få nærkontakt med en strøm av it-folk med smartgrid i tankene i årene som kommer.

– IT vil invadere kraftbransjen

AMS er bare starten på en strøm av enorme it-prosjekter som skal snu kraftbransjen på hodet.

Skriv ut Tips en venn Motta nyheter på e-post Tips redaksjonen Facebook +1 Tweet

Av Leif Harnes Publisert: 23.02.2011 kl. 09:31

Stjeler kontrakter, tegninger, passord og hemmelige data

Ti datainnbrudd er oppdaget i norske selskaper innen forsvar, olje og energi. Dette er den største dataspionasjesaken som er avdekket i Norge. - Meget alvorlig, sier en PST-sjef.

Råd mot dataspioner

Washington Post slår nå fast at det var USA og Israel som stod bak Flame.

FOTO: Hardware.no

– USA og Israel står bak kyberangrepet

«Flame»-viruset skulle bremse Irans atomprogram.

Anbefal 37 personer anbefaler dette.

Hackere kan ta over norske styringssystemer

Hevder de har innloggingsinformasjon til kontrollsystemer for infrastruktur og industri i Norge.

Anbefal 27 personer anbefaler dette.

SINTEF | NTNU Det skapende universitet

Research questions

- RQ 1:

  Which elements comprise current practice for ICT and ICS security incident management among distribution system operators (DSOs) in the power industry?

- RQ 2:

  Which non-conformities can be identified when comparing current practice among distribution system operators (DSOs) in the power industry with standards and recommended practice?

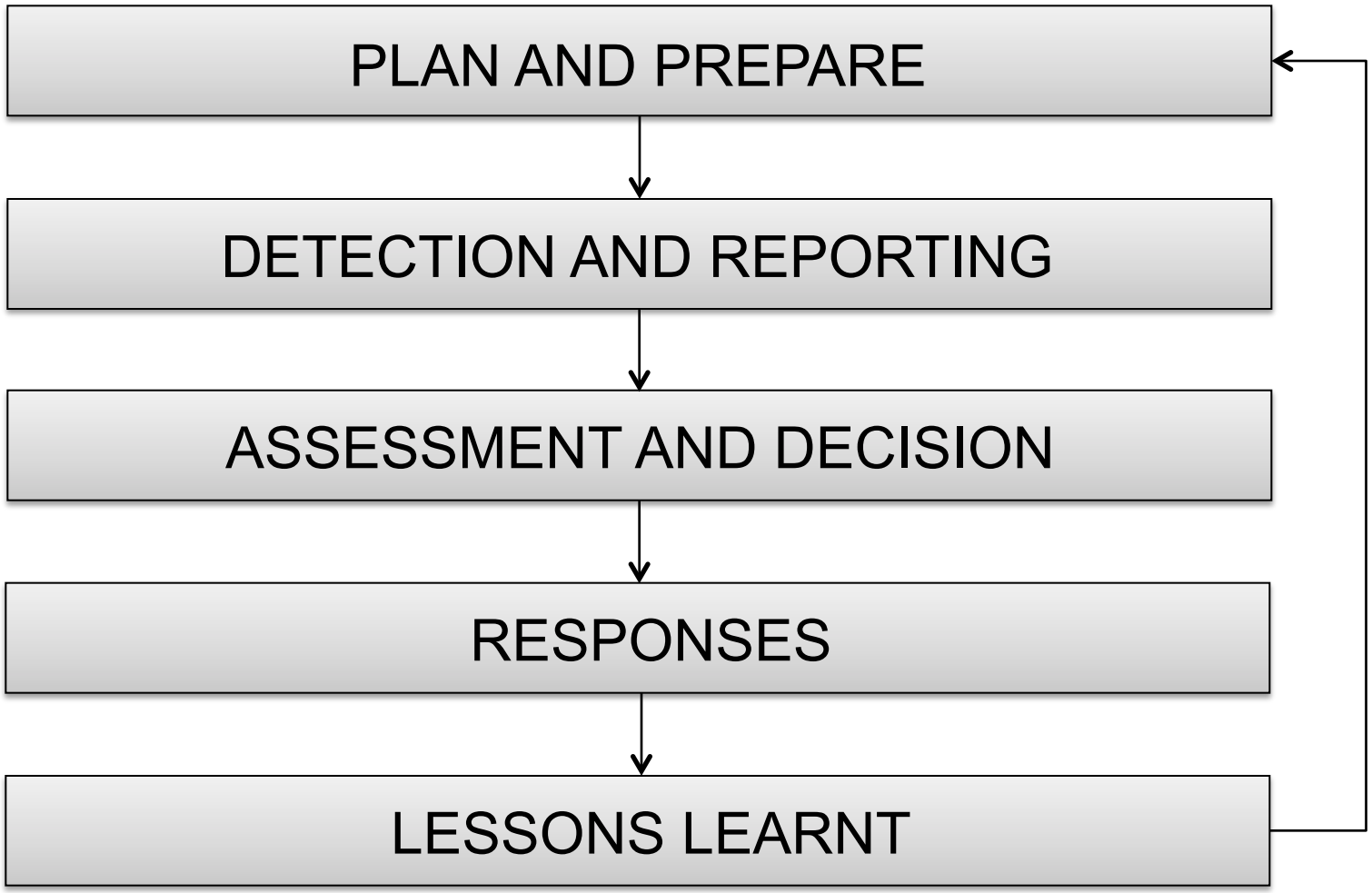
- RQ 3:

  How can incident management be measured?

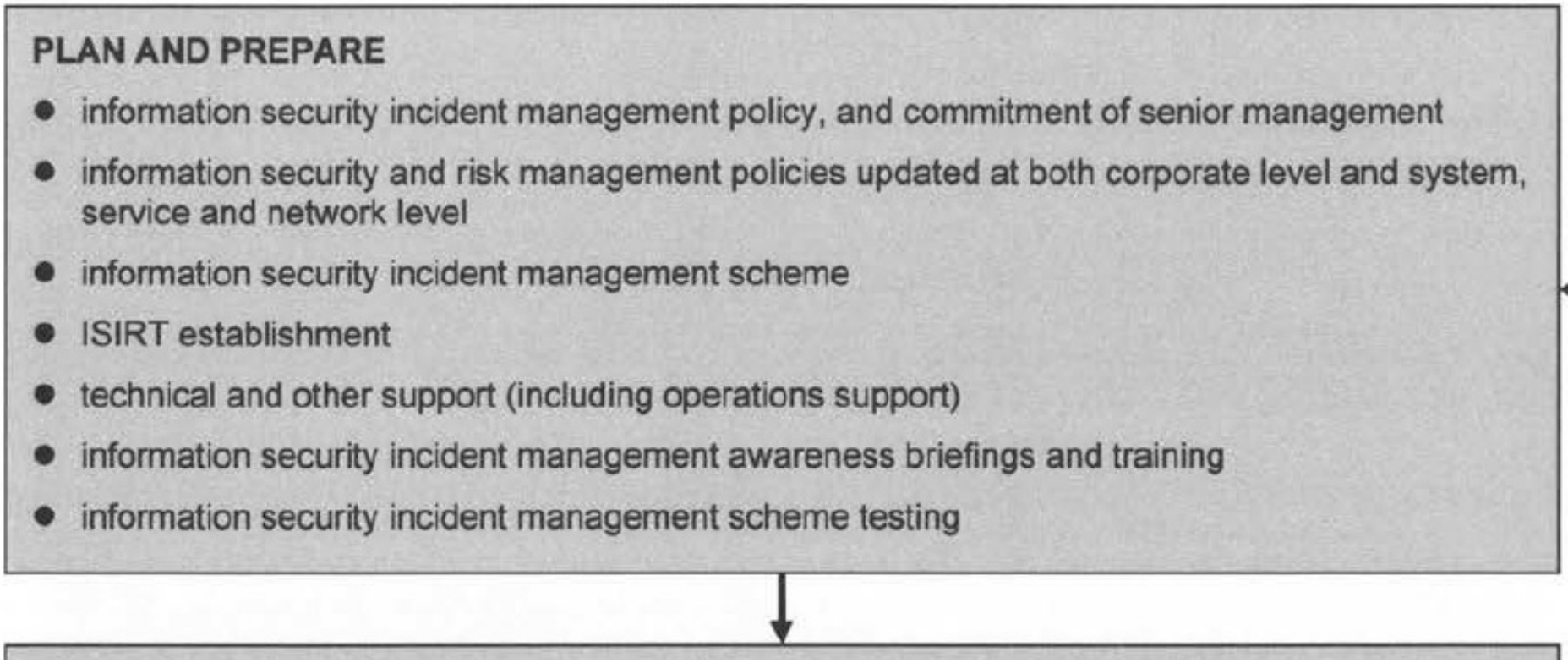
Method: Case study – semi-structured interviews

- Studying current practice in the power industry on information security incident management
  - Large DSOs – Distribution System Operators
    - IT, IT security, Automation and control
  - 19 interviews performed

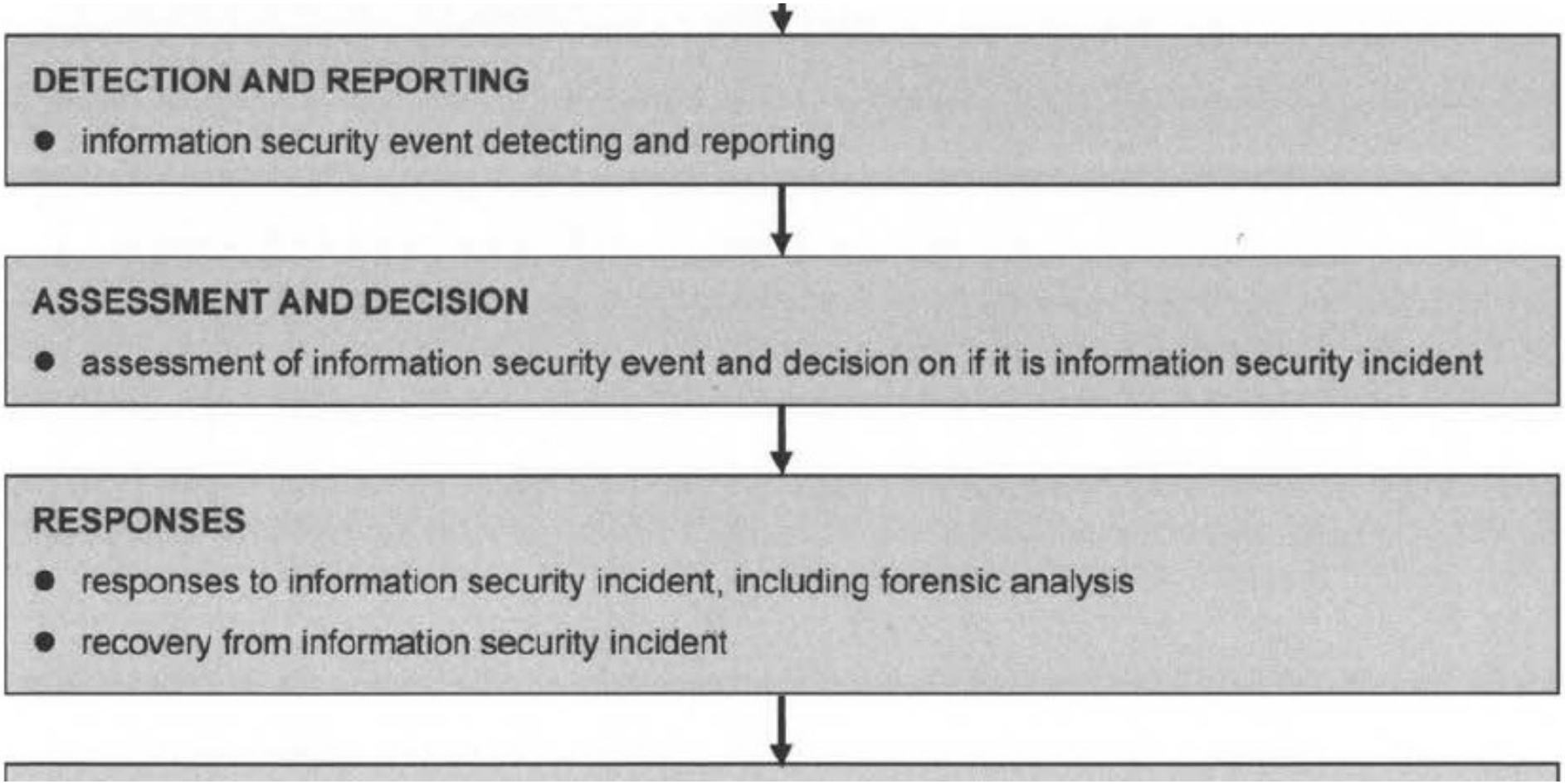
- To do: Transcribe and analyse thoroughly



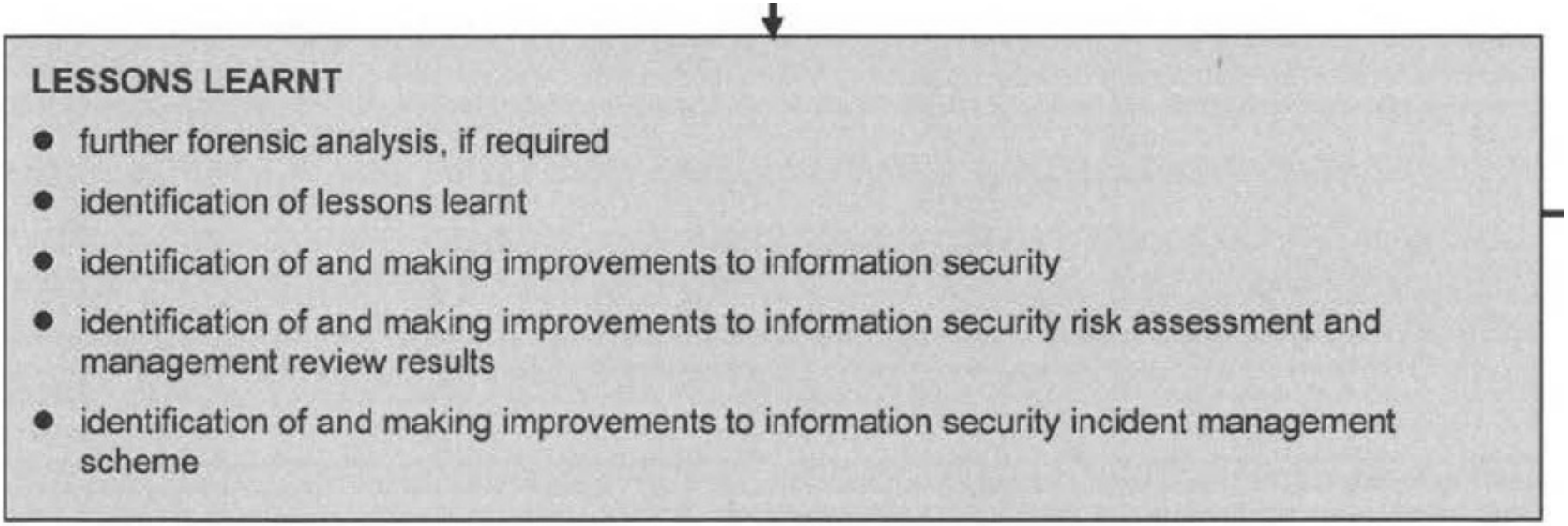
From ISO/IEC 27035: The five phases of information security incident management



From ISO/IEC 27035: The first phase – Plan and prepare



From ISO/IEC 27035: The next phases – Detection and reporting; Assessment and decision; Responses



From ISO/IEC 27035: The fifth phase – Lessons learnt

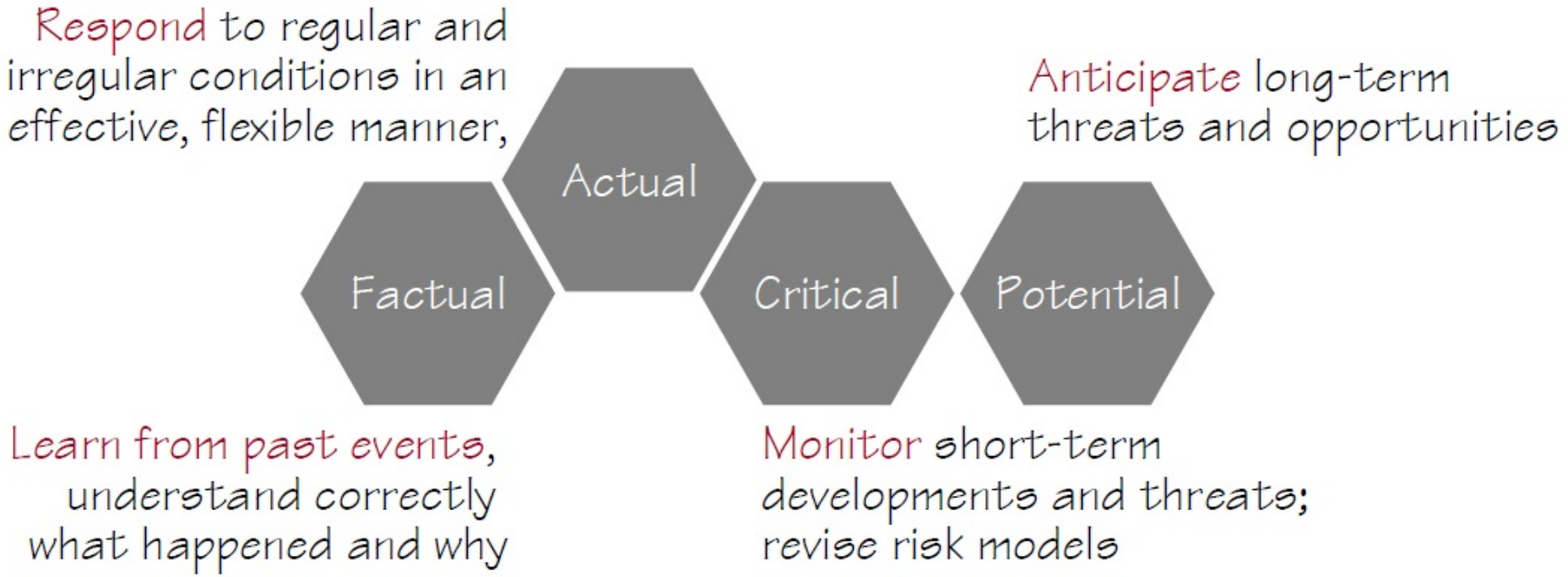
Preliminary conclusions

- Lack of systematic approach to incident management
- Lack of cooperation between IT and power automation staff
- Still, they seem to succeed…
  - Low turnover
  - The worst incidents are still to come…?

Resilience Engineering

- Immanent property of a system. Can not be implemented over night.
- Notice the things that go right, learn from them, as opposed to things that go wrong. Increase the number of things that go right.
- Resilience in three levels:
  - The ability to prevent something bad from happening
  - The ability to prevent something bad turning into something worse
  - The ability to successfully recover after something bad happened
- Being able to recognize a situation that requires a response. Being preoccupied with failure. Categorize the situation properly. Escalate at the right time.

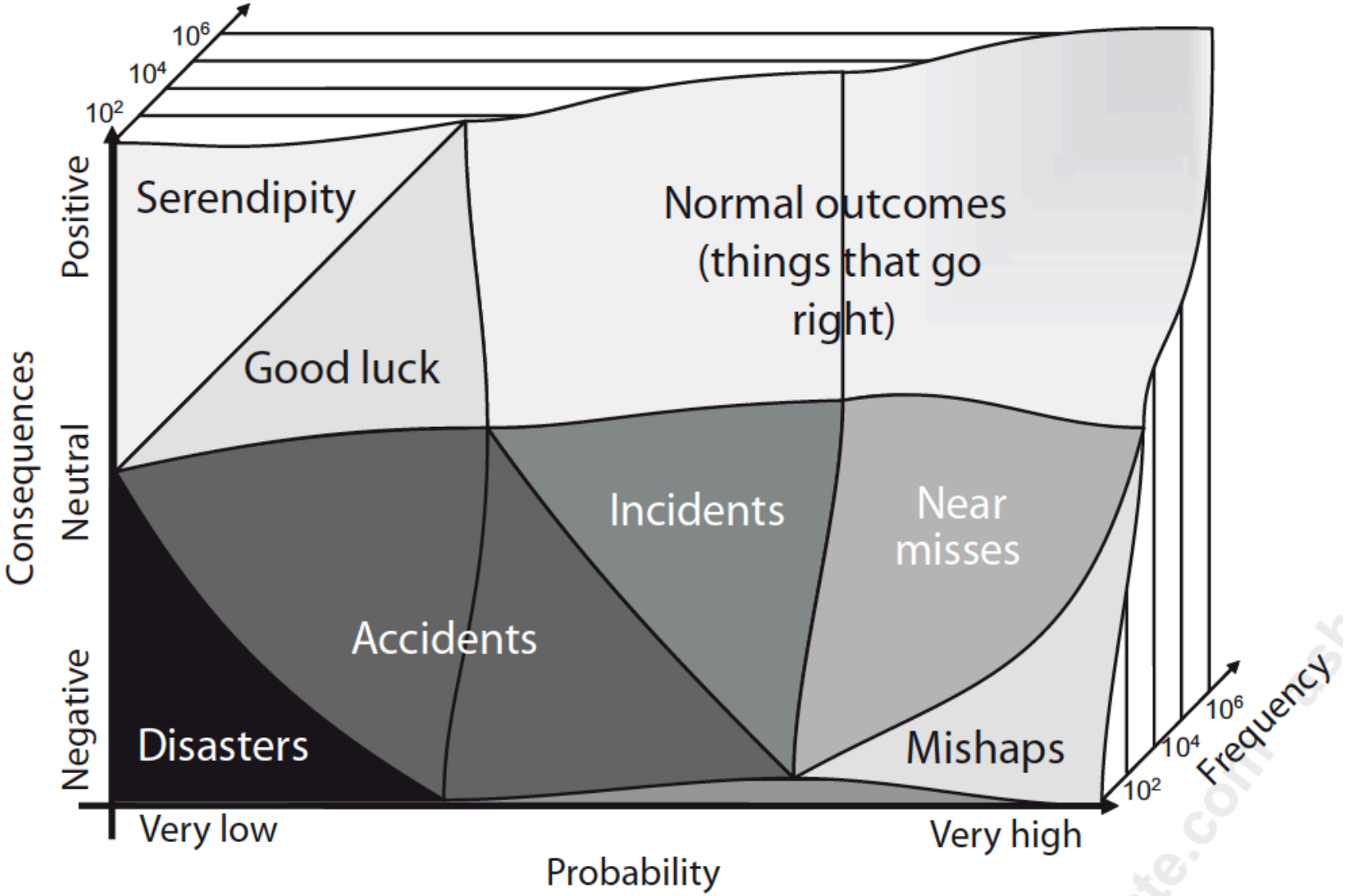
The four basic abilities of resilience engineering



By Erik Hollnagel

SINTEF | NTNU Det skapende universitet

By Erik Hollnagel et al. – Resilience Engineering in Practice, A Guidebook – Ashgate



SINTEF | NTNU Det skapende universitet

The irony of resilience

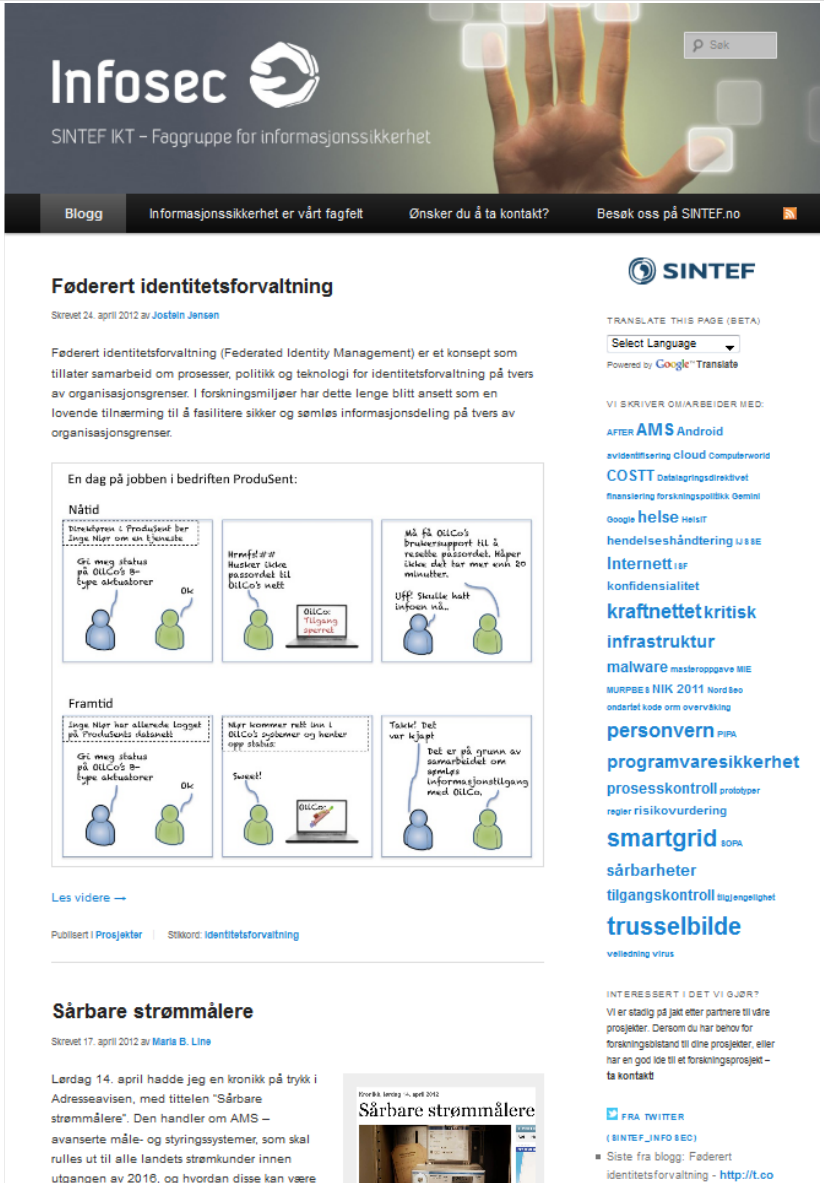
- The competence that is needed for responding to unexpected incidents, is also the competence that might be reduced through many attempts to anticipate incidents and prepare for them.

- Resilience is about being prepared – and being prepared to be unprepared.

(In the near) future work

- MSc project: Measuring information security – currently writing paper
- MSc thesis: Study how recent major ICT security incidents have been responded to
- Experts in Teams: Privacy issues, recommendations for the DSOs
- Study differences between large and smaller DSOs
  - New series of interviews: small DSOs (~20 employees)
- Retrospectives: after an incident
- Observations: Visit a DSO, walk and talk, observe meetings and interactions
  - "Don't underestimate the coffee machine”
- Study documentation, compare to interview findings

- PhD project – Maria B. Line
  www.item.ntnu.no/people/personalpages/phd/maria.b.line/start
- Infosec blog (in Norwegian)
  http://infosec.sintef.no
- The Norwegian Smartgrid Centre
  www.smartgrids.no
- Film: What is Smart Grids (Smartgrid-senteret; in Norwegian)
  http://youtu.be/VkFBE-Gy31Y
- Film: E.ON Smart Grids – a cute and informative film about SG
  http://www.youtube.com/watch?v=36e33i8wzKE
- NVE: Risk assessment of AMI – by SINTEF (in Norwegian):
  www.nve.no//no/Nyhetsarkiv-/Nyheter/God-sikkerhet-grunnleggende-for-vellykket-AMS-utrulling/
- Security Threats in Demo Steinkjer – by SINTEF:
  www.sintef.no/Publikasjoner-SINTEF/Publikasjon/?pubid=SINTEF+A23351
- The Data Inspectorate: Guide to processing personal data in AMI
  www.datatilsynet.no/Global/english/Automatiske_maalesystemer_ENG.pdf
- Erik Hollnagel: An introduction to Resilience Engineering
  www.gowerpublishing.com/pdf/SamplePages/Resilience_Engineering_in_Practice_Prol.pdf



@mariabline

Visit our blog:

infosec.sintef.no

SINTEF | NTNU Det skapende universitet