Sikkerhet av driftskontroll-systemer innen VA.

Hva kan gå galt og hva bør en gjøre for å sikre seg?

VA-dagene Midt-Norge 2013

Martin Gilje Jaatun

Martin.G.Jaatun@sintef.no

Introduksjon

- Litt skremselspropaganda
- Litt edruelig informasjon
- Litt tips om hjelp

Maroochy Shire, Australia

Maroochy Shire Council

http://images.businessweek.com/ss/10/10/1014_cyber_attacks/8.htm

http://www.flickr.com/photos/26085795@N02/5379545920/sizes/l/in/photostream/

Stuxnet

http://en.wikipedia.org/wiki/File:S7300.JPG

http://www.flickr.com/photos/travisgoodspeed/5975075137/sizes/l/in/photostream/

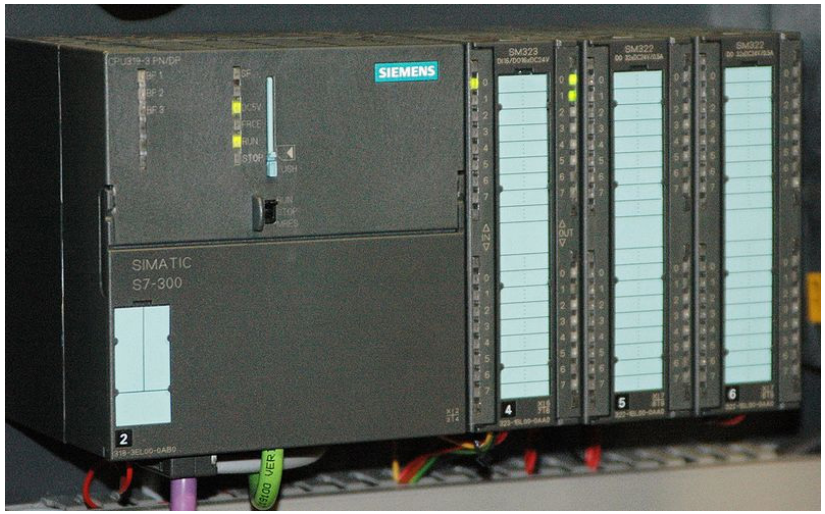
DUQU?

http://warincontext.org/2010/09/26/iran-confirms-stuxnet-found-at-bushehr-nuclear-power-plant/

Flame?

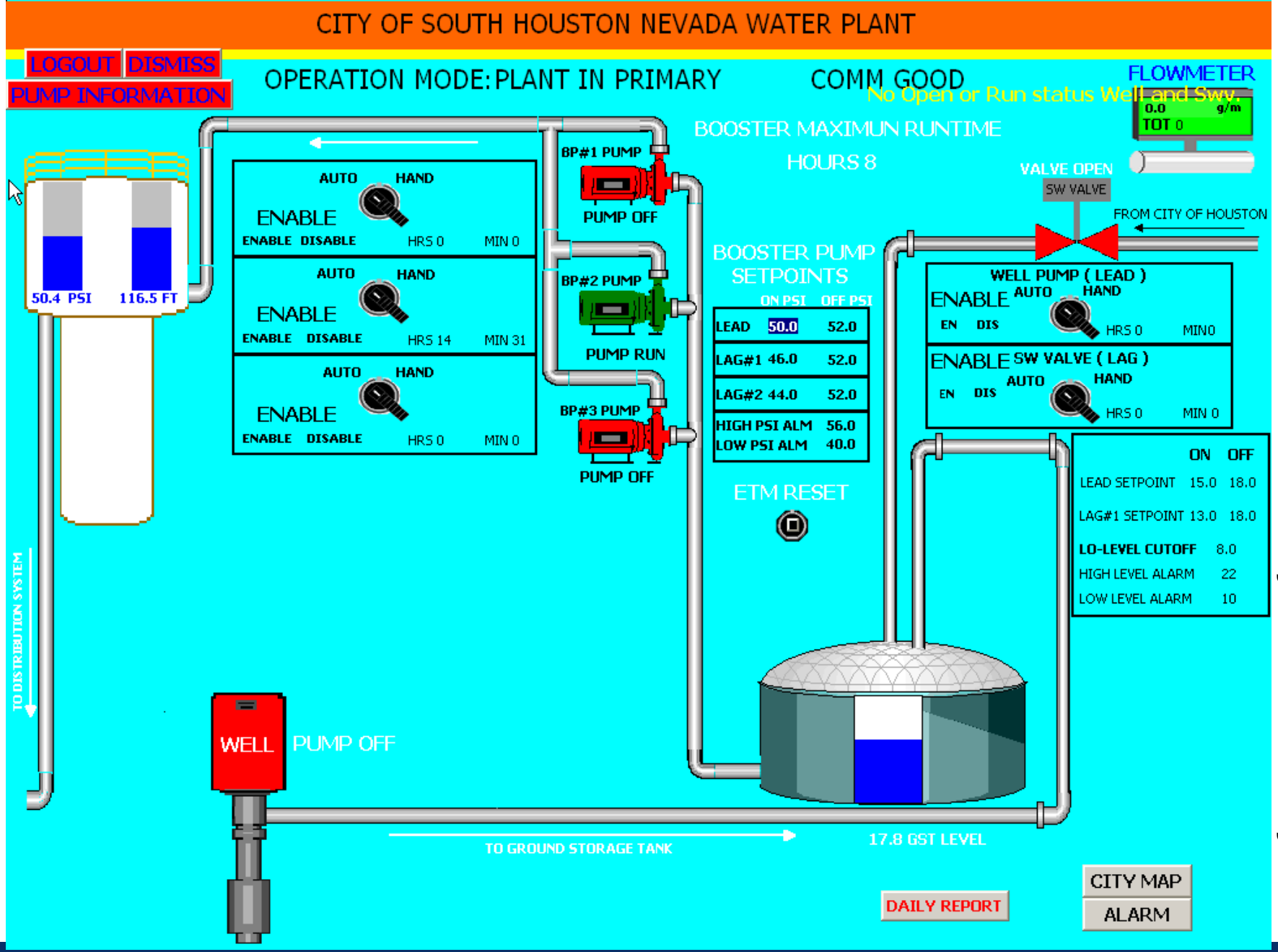
South Houston

- Siemens Simatic MMI tilgjengelig fra internett
- Passord på 3 bokstaver er like ille som "0000"…



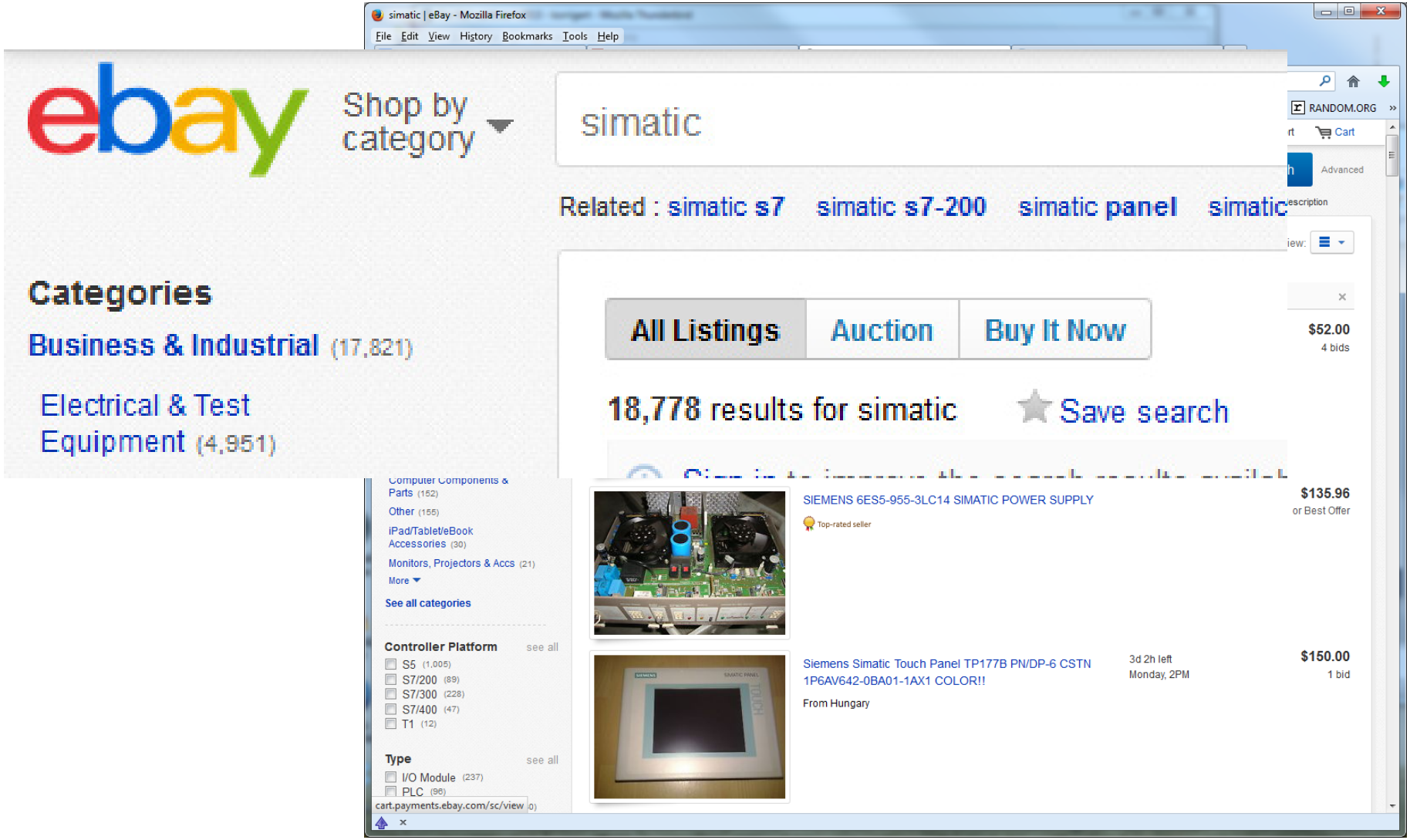
http://en.wikipedia.org/wiki/File:S7300.JPG

the default password for Siemens SIMATIC is "100". There are three different services that are exposed when Siemens SIMATIC is installed; Web, VNC, and Telnet. The default creds for the Web interface is *"Administrator:100"* and the VNC service only requires the user enter the password of *"100" – B.K. Rios*



http://i41.tinypic.com/ip0aa0.png

Mye moro å finne på eBay

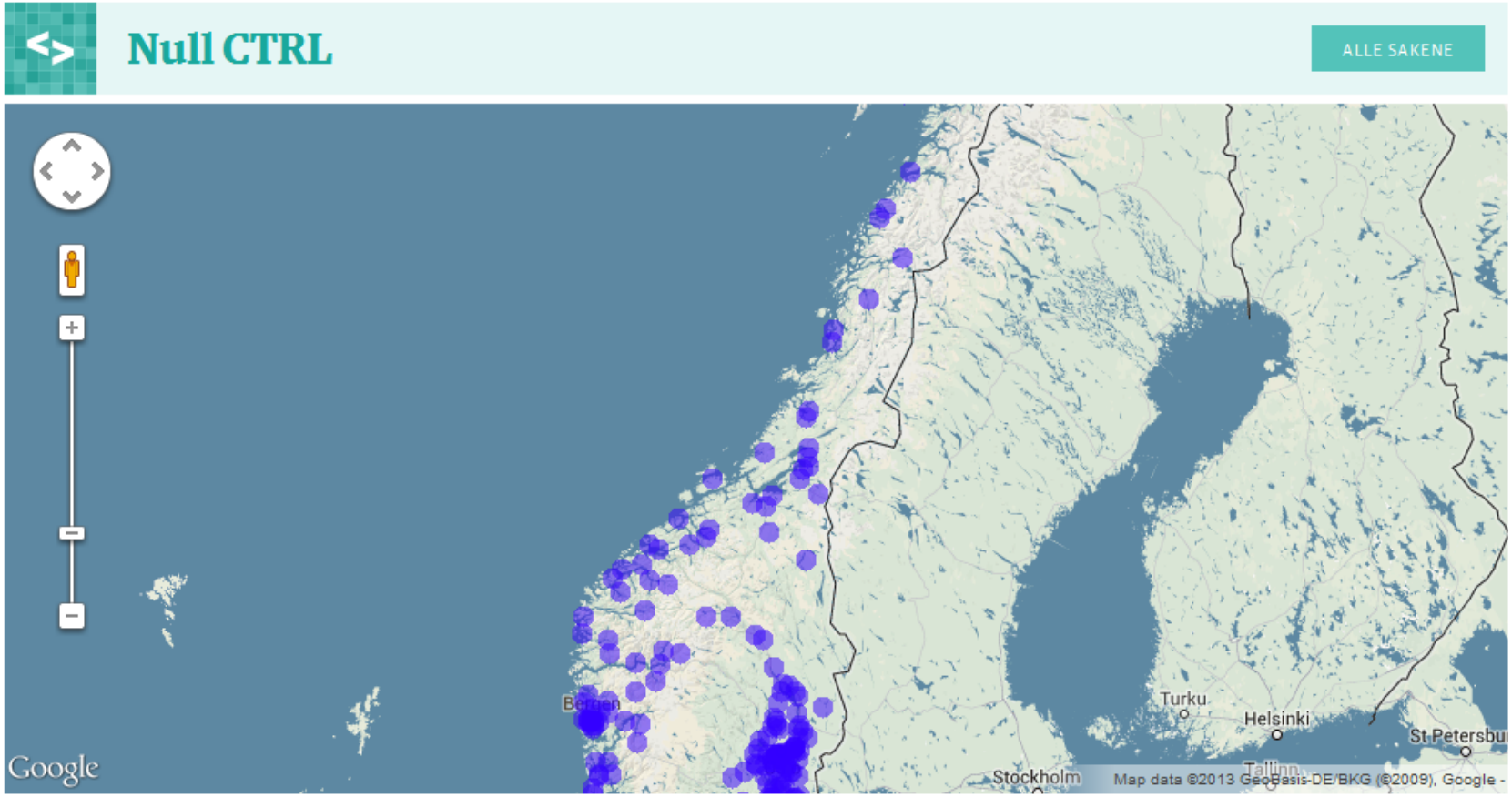


Søk, og I skal finne!

1 million DKS på nett?

Allied Telesis
Alcea
ABB
ADCON
APC
Allen-Bradley
AKCP
Barik
Caterpillar Inc.
Cimetrics
CIMON
Control4
CODESYS
Clorius Controls
Datawatt
Delta Controls
Digi
Ecessa
Ericsson
Emerson
EIG
EnergyICT
Falcon
Force10
Funkwerk
GE
Genohm
Hirschmann
Honeywell
Liebherr
LOGPAC
Itron, Inc.
Koyo
KMC
Komatsu
Lennox
Leica
Lancom
Lantronix
Moxa
LonWorks
LG
Mitsubitshi
Motorola
Niagara
National Instr.
OMRON
openSCADA
Ouman
Phoenix Contact
Phillips
mGuard
Schneider El.
Siemens
RUGGEDCOM
Rockwell Aut.
Powertech
STULZ
SoftPLC
Telemecanique
VxWorks
WAGO
WindWeb
Wonderware

https://www.tofinosecurity.com/blog/project-shine-1000000-internet-connected-scada-and-ics-systems-and-counting



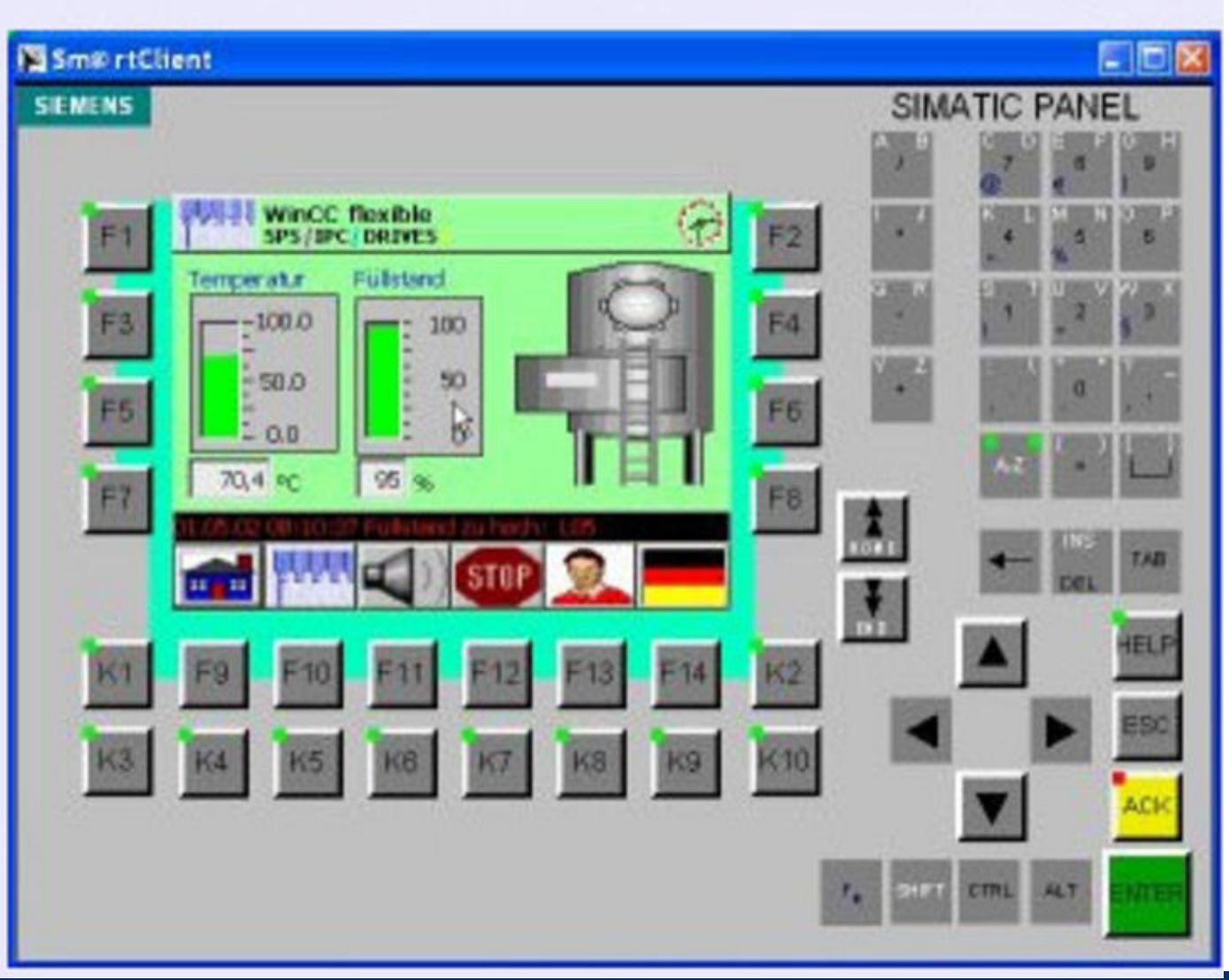
NORSKE SYSTEMER PÅ NETT: I dette kartet er styringssystemene Dagbladet har funnet, plottet geografisk etter IP-adresse. Den geografiske plasseringen kan avvike i større eller mindre grad fra det faktiske. Grafikk: Ola Strømman

«I verste tilfelle kan liv gå tapt»

Dagbladet fant over 2500 norske styringssystemer på nett. Disse brukes blant annet i forsvar, helse, oljebransjen og kollektivtransport.

http://www.dagbladet.no/2013/10/17/nyheter/innenr iks/datasikkerhet/nullctrl/28572676/

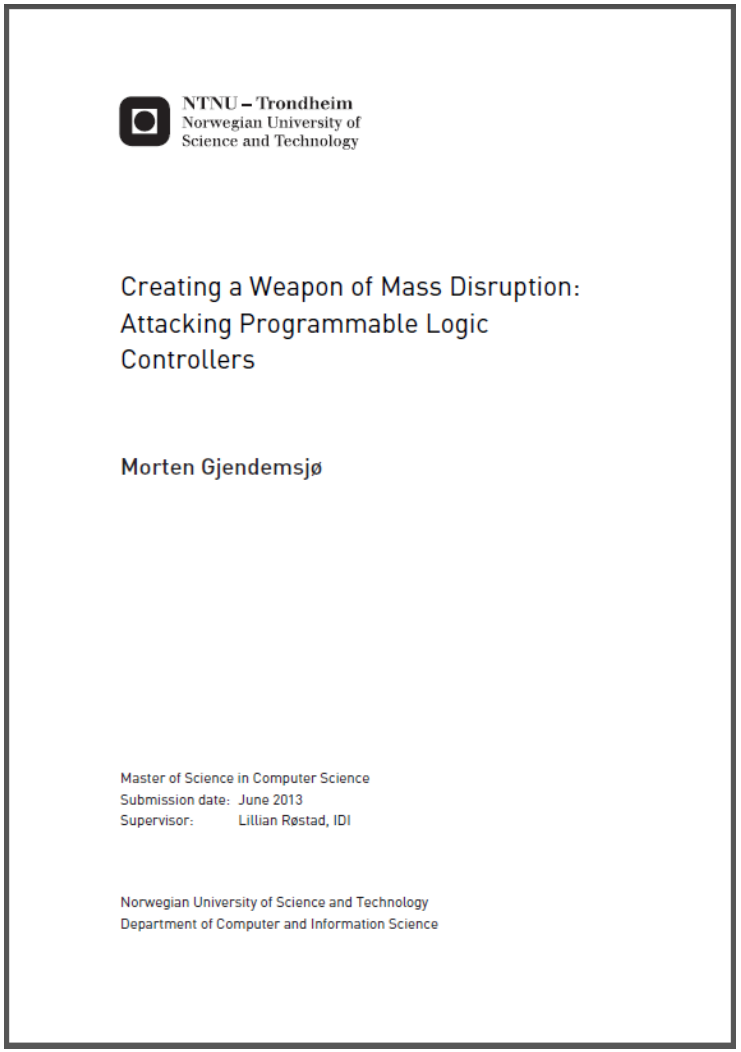
En helt vanlig dag på biobrenselanlegget



http://www.dagbladet.no/2013/10/17/nyheter/innenr
iks/datasikkerhet/nullctrl/28572676/

Er ikke sikkerheten i DKS blitt mye bedre i det siste?

- En rykende fersk masteroppgave fra NTNU tyder på noe annet!



NTNU – Trondheim
Norwegian University of
Science and Technology

Creating a Weapon of Mass Disruption:
Attacking Programmable Logic
Controllers

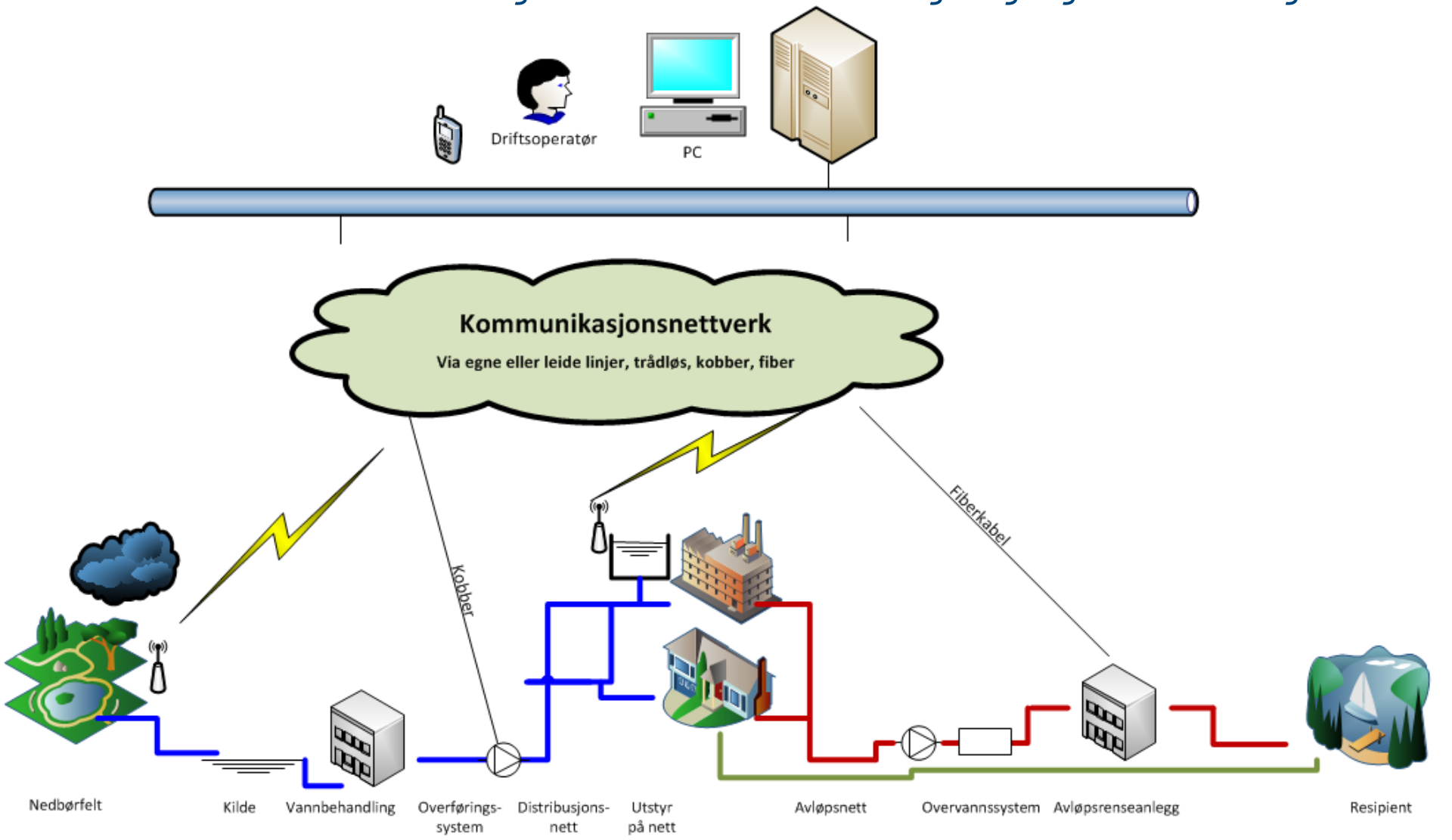
Morten Gjendemsjø

Master of Science in Computer Science
Submission date: June 2013
Supervisor: Lillian Røstad, IDI

Norwegian University of Science and Technology
Department of Computer and Information Science

Hva hender dersom DKS faller ut? Kommer det fortsatt rent vann?

Bruk av driftskontrollsystem innen VA for styring og overvåking

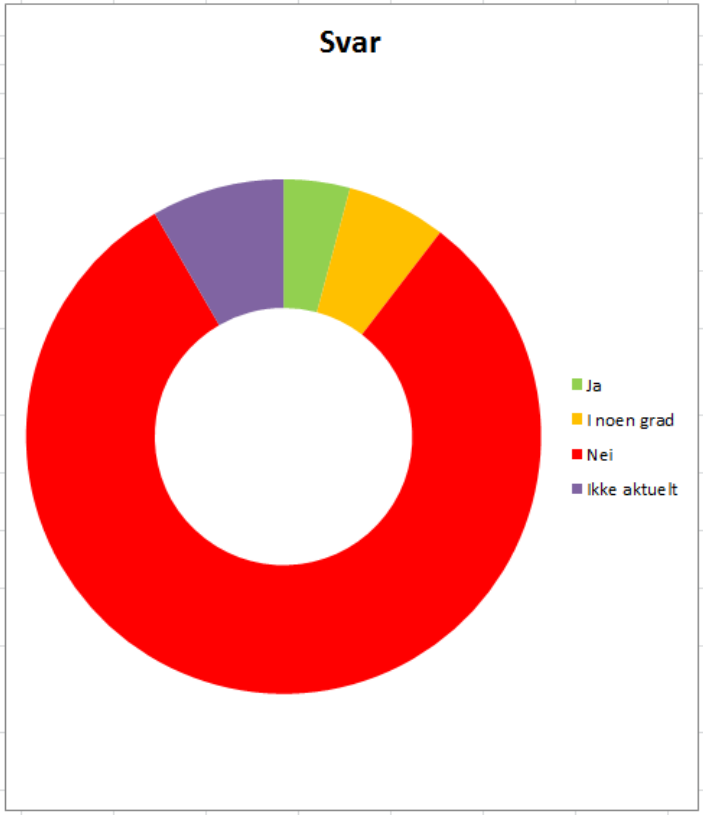


HJELP!?

- Norsk Vann Rapport 195: Veiledning om sikkerhet og sårbahet i driftskontroll-systemer for VA- anlegg
- Tema:
  - Informasjonssikkerhet
  - Sårbarheter
  - Tiltak
  - Sjekkliste

Sjekkliste

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
		Sjekkliste for sikrere driftskontrollsystem for VA														
		Spørsmål	**Ja**	**I noen grad**	**Nei**	**Ikke aktuelt**	**Begrunnelse**									
	1	Er informasjonssikkerhet i driftskontrollsystemer godt nok forankret hos ledelsen i VA-verket?	x													
	2	Er det bevissthet rundt informasjonssikkerhet i hele organisasjonen?		x												
	3	Har alle personlig brukernavn og passord ved pålogging av DKS?		x												
	4	Kreves det 2-faktor autentisering ved ekstern tilgang til DKS (VPN, terminalserver)?		x												
	5	Har virksomheten kontroll med hvem som har tilgang til DKS (tilgangsstyring), hvilke funksjoner de har lov til å utføre og når de har vært pålogget?	x													
	6	Er det spesifisert ulike nivåer på tilgangsrettigheter (innsyn, endring)?				x										
	7	Gjennomgås tilgangsrettigheter årlig for å sikre at alle tilgangsrettigheter er korrekte og på riktig nivå?				x										
	8	Er det gjennomført en ROS-analyse som dekker hjemmevaktordning?				x										
	9	Er det egne PC, nettbrett etc som bare brukes til drift og vakt?				x										
	10	Er det gjennomført tekniske tiltak for å sikre dette (restriksjoner på programutvalg, ikke tilgang til internett for annet enn DKS)?			x											
	11	Er det vurdert skille eventuelt sikkerhetsbarrierer mellom administrative og DKS nett?			x											
		Er det vurdert skille eventuelt sikkerhetsbarrierer mellom														



Jo flere vi er sammen

http://www.flickr.com/photos/frenkieb/

Ditt sikkerhets-team

http://www.flickr.com/photos/ctbto/

Hva om alle VA-verk kunne samarbeide?

Når uhellet er ute

- Kan neppe beskytte mot alle mulige angrep
- Planlegg hendelseshåndtering!
- Samarbeid på tvers av organisasjoner
- Informasjonsdeling!

norskhelsenett HelseCSIRT

UNINETT The Norwegian research network

UNINETT CERT

FinansCERT

VA-CERT?

NSM NorCERT

Under arbeid…

- Jobber med anbefalinger for hendelseshåndtering i VA-bransjen
  - Basert på erfaringer i olje & gass
- Veldig interessert i innspill fra bransjen!


SINTEF

Memo

Information Security Incident Response Management in the Water Sector

PERSON RESPONSIBLE / AUTHOR
Martin Gilje Jaatun
(Based on "Incident Response Management in the oil and gas industry", SINTEF Report A4086 by Martin Gilje Jaatun, Stig Ole Johnsen, Maria B. Line, Odd Helge Longva, Inger Anne Tøndel, Eirik Albrechtsen and Irene Wærø)

FOR YOUR ATTENTION | COMMENTS ARE INVITED | FOR YOUR INFORMATION | AS AGREED

DISTRIBUTION
Rita Ugarelli
Jon Røstum
Bård Myhre
Stig Petersen

PROJECT NO / FILE CODE
SMS-VAV

DATE
2015-08-22

CLASSIFICATION
Unrestricted

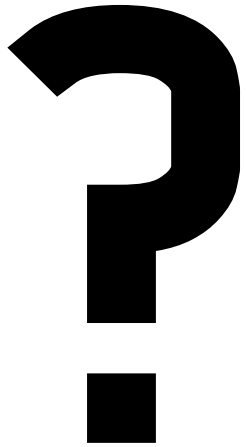
Table of Contents

DRAFT

this memo contains project information and preliminary results as a basis for final report(s). SINTEF accepts no responsibility of this memo and no part of it may be copied.

1 of 12

Spørsmål?



twitter.com/
SINTEF_Infosec

Infosec
Blogg

http://infosec.sintef.no

Martin.G.Jaatun@sintef.no