



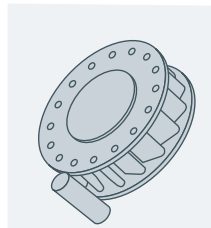
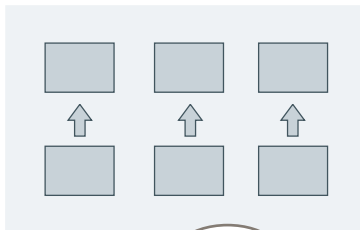
Swedish Civil
Contingencies
Agency

ICS Parables

Part 2

Good intentions

A beautiful Friday morning.



Security patch



LOADING...

- Port 1
- Port 2
- Port 3
- Port 4

These ports don't need to be open. I am sure about that.



Later in another part of the facility.

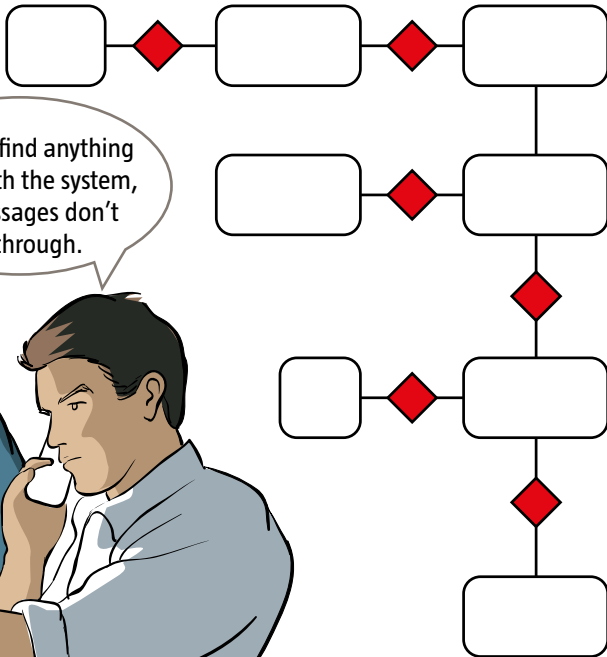
The system doesn't work anymore. I can't monitor the process!



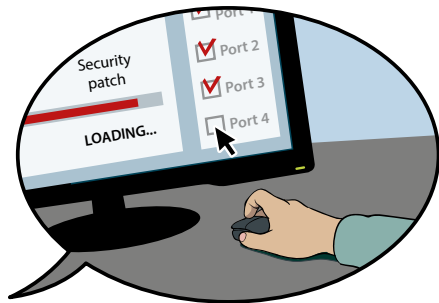
Time passes.



We can't find anything wrong with the system, but messages don't get through.



Next week, Monday coffee break.



- I changed some of the firewall settings last week.
- You didn't talk to us about that? That might be the reason why the process monitoring is not working.
- But you don't monitor the process from the office side of the network, do you?
- Yes we do, but perhaps we forgot to tell you about that.

Recommendations

- Ensure systematic change management in industrial information and control systems.
 - Before and after changes in the industrial information and control systems, ensure that affected parties are always informed of the change.
 - Changes (configurations, “patching”, etc.) are always tested in a separate test environment before being installed in daily operation.
- Harden and upgrade industrial information and control systems in collaboration with system vendors.
 - Ensure that there is clear documentation on how and when system hardening is to be performed or has been performed.
 - Ensure that all upgrades, reconfigurations and “patches” are documented.

Protect vital societal functions.

Protect your organisation.

Protect your industrial control systems.

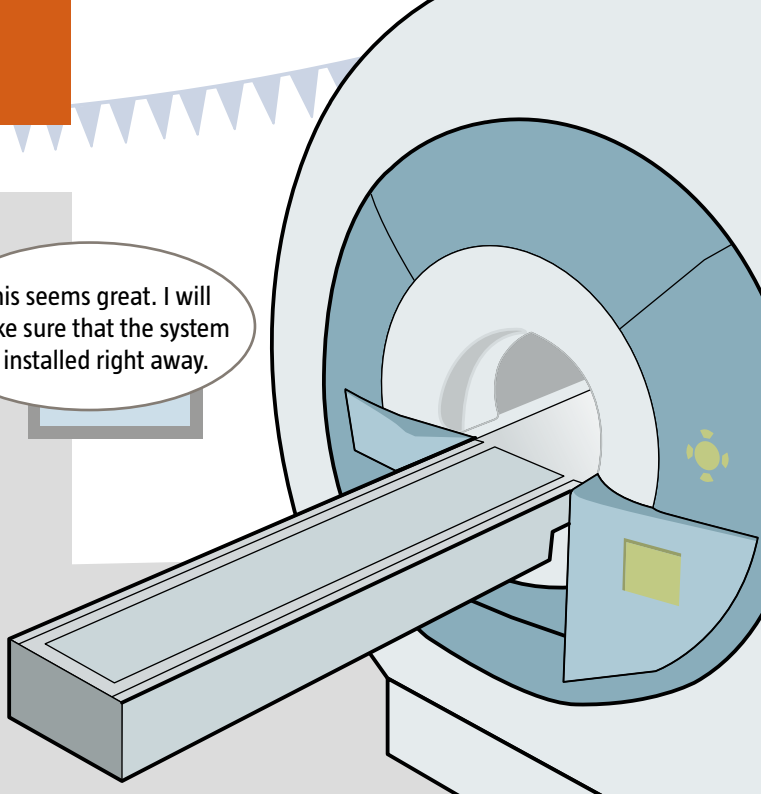


A quick deal

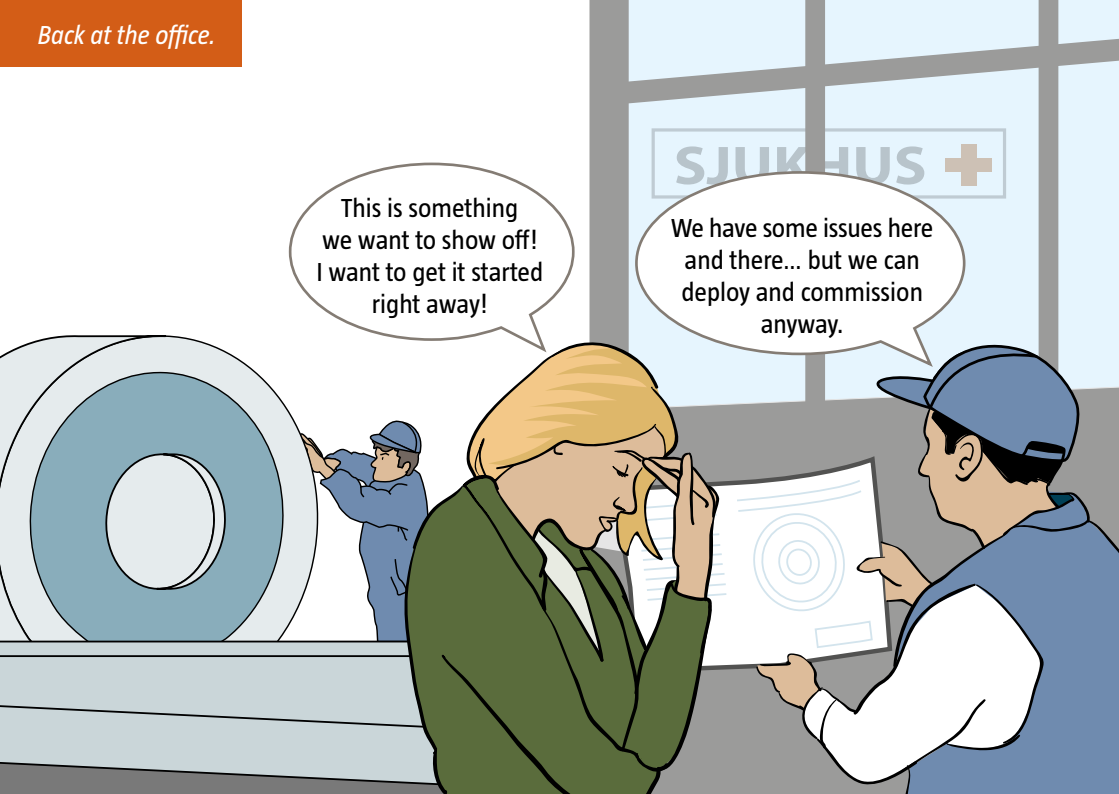
At the conference.



This seems great. I will make sure that the system is installed right away.



Back at the office.



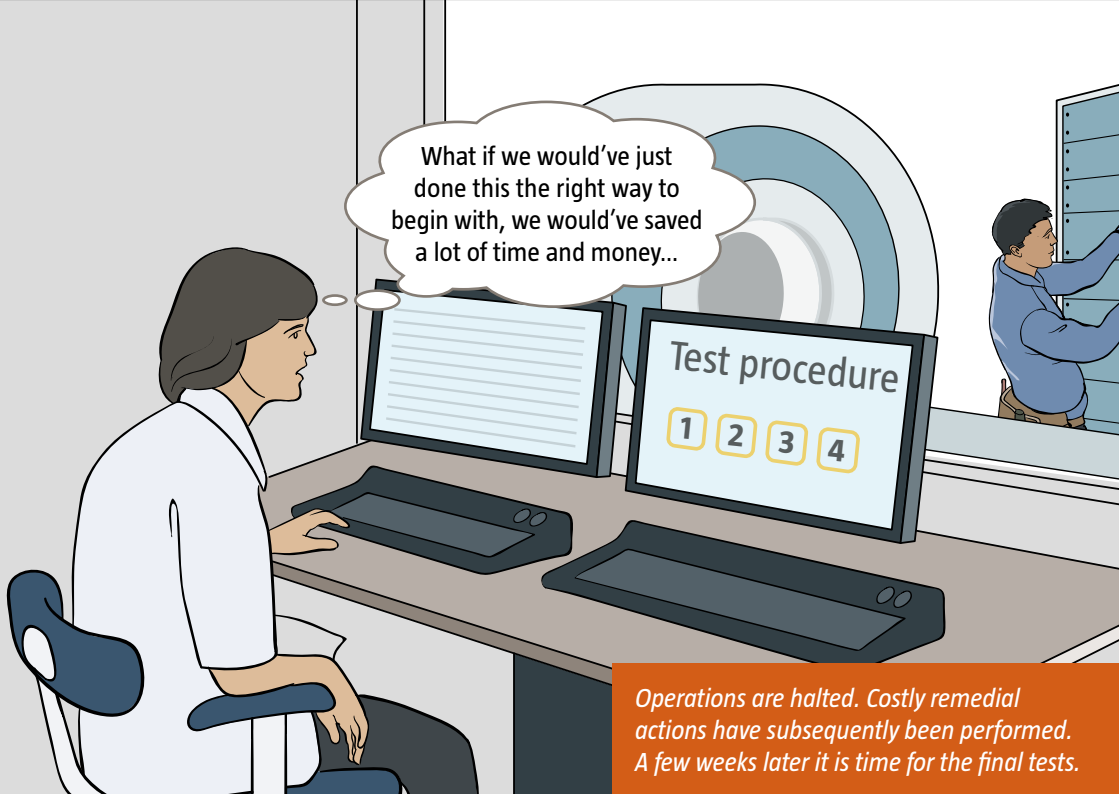
This is something
we want to show off!
I want to get it started
right away!

We have some issues here
and there... but we can
deploy and commission
anyway.

The media has found out about the problems. The PR department is not happy.

Have you seen this? Now they are writing about the problems with the system in the news. We have to do something!





What if we would've just done this the right way to begin with, we would've saved a lot of time and money...

Operations are halted. Costly remedial actions have subsequently been performed. A few weeks later it is time for the final tests.

Recommendations

- Secure management's commitment and responsibility for security in industrial information and control systems.
 - Try to describe what different measures cost – both in investment and in working hours. Relate the cost to the benefit that the measures yield for the business.
- Clarify roles and responsibilities for security in industrial information and control systems.
 - Ensure that there are documented requirements for a system owner, such as expertise, training, security classification, etc.

- Introduce security requirements in industrial information and control systems right from the start in all planning and procurement.
 - Ensure that there are documented procedures for how information security issues shall be handled during all procurement of goods and services.

CONTACT:

scada@msb.se | www.msb.se/ics

Swedish Civil Contingencies Agency (MSB)

SE-651 81 Karlstad Phone +46 (0)771-240 240 www.msb.se/en

Publ.no MSB1278 - September 2018