

Stuxnet: Dawn of a new era

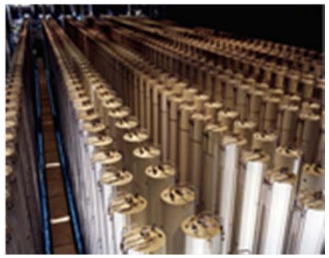
…about the hype & consequences of Stuxnet

Dr. Stefan Lüders (CERN Computer Security Officer)

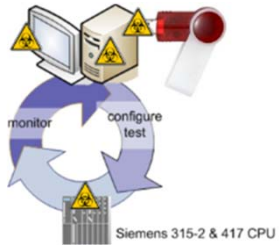
ICALEPCS2011

Grenoble (France), October 11th 2011


Overview



Pandora's Box has been opened!



The Workings

Protective Measures

Disclaimer:

This presentation is based on info from (trusted) third parties.
Nobody who was involved ever commented on this.

Natanz, we have a problem.

Microsoft Investigating Windows Security Zero-Day Targeted by Trojan

LinkedIn Twitter 5 Facebook

By: Brian Prince
2010-07-16
Article Rating: ★★★★★ / 3
There are 0user comments on this IT S
Reviews s

eWEEK.COM

Microsoft is investigating reports of a vulnerability being exploited by a Trojan spreading through USB devices. According to security pros, the malware appears to be targeting the utility industry.

Microsoft is investigating reports of a Windows security vulnerability being exploited by a Trojan some say is targeting industrial companies.

Rate This Article:

Poor ○ ○ ○ ○ ● Best

Rate

Natanz, we have a problem.

Microsoft Investigating Windows Security Zero-Day Targeted by Trojan

LinkedIn Twitter 5 Facebook

By: Brian Prince
2010-07-16
Article Rating: ★★★★★ / 3
There are 0user comments on this IT
Reviews

Microsoft is investigating reports of a v Trojan spreading through USB devices. malware appears to be targeting the ut

Microsoft is investigating reports of a Windows security vulnerability being exploited by a Trojan some say is targeti industrial companies.

COMPUTERWORLD

News

Siemens: German customer hit by industrial worm

By Robert McMillan
July 20, 2010 07:47 PM ET

1 Comment Gefällt mir +1 0

IDG News Service - Siemens confirmed Tuesday that one of its customers has been hit by a new worm designed to steal secrets from industrial control systems.

To date, the company has been notified of one attack, on a German manufacturer that Siemens declined to identify. "We were informed by one of our system integrators, who developed a project for a customer in process industries," said Siemens Industry spokesman Wieland Simon in an e-mail message. The company is trying to determine whether the attack caused damage, he said.

The worm, called Stuxnet, was first spotted last month, when it infected systems at an unidentified Iranian organization, according to Sergey Ulasen, the head of the antivirus kernel department at VirusBlokAda, in Minsk, Belarus. The unidentified victim, which does not own the type of SCADA (supervisory control and data acquisition) systems targeted by the worm, "told us their workstations serially rebooted without any reason," Ulasen said in an e-mail message Tuesday.

Natanz, we have a problem.

Microsoft Investigating Windows Security Zero-Day Targeted by Trojan

LinkedIn Twitter 5 Facebook

By: Brian Prince
2010-07-16
Article Rating: ★★★★★ / 3
There are 0user comments on this IT Reviews

Microsoft is investigating reports of a v Trojan spreading through USB devices. malware appears to be targeting the ut

Microsoft is investigating reports of a Windows security vulnerability being exploited by a Trojan some say is targeti industrial companies.

COMPUTERWORLD

News

Siemens: German customer hit by industrial worm

By Robert McMillan
July 20, 2010 07:47 PM ET

IDG News Service - Siemens has been hit by a new worm de systems.

To date, the company has bee manufacturer that Siemens de our system integrators, who de industries," said Siemens Indu message. The company is tryi damage, he said.

The worm, called Stuxnet, was systems at an unidentified Iran the head of the antivirus kernel department at VirusBlokAda, in Minsk, Belarus.

The unidentified victim, which does not own the type of SCADA (supervisory control and data acquisition) systems targeted by the worm, "told us their workstations serially rebooted without any reason," Ulasen said in an e-mail message Tuesday.

The Washington Post
NATIONA

Posted at 09:26 AM ET, 09/20/2011

After Stuxnet, waiting on Pandora's box

By Jason Ukman

The mysterious computer worm known as Stuxnet has gained more than a little notoriety since it was discovered in the summer of 2010. It wreaked havoc on Iran's nuclear program. It stirred suspicions that it had been unleashed by the Israelis, the Americans or both. And, last but hardly least, it heightened long-standing concerns about the potential for a cyber attack on critical infrastructure in the West.

In the case of Iran, Stuxnet worked its way into an industrial control system by rather insidious means -- identifying the centrifuges used to enrich uranium and causing them to spin so rapidly that they began to break. But experts have said that the worm could just as easily serve as a blueprint to sabotage machines that are critical to power plants, electrical grids and other utilities in the United States and elsewhere.

Natanz, we have a problem.

Microsoft Investigating Windows Security Zero-Day Targeted by Trojan

LinkedIn Twitter 5 Facebook

By: Brian Prince
2010-07-16
Article Rating: ★★★★★ / 3
There are 0user comments on this IT

COMPUTERWORLD

News

Siemens: German customer hit by industrial worm

By

SPIEGEL ONLINE

The Washington Post
NATIONA

:26 AM ET, 09/20/2011

tuxnet, waiting on Pandora's box

Ukman

erious computer worm known as Stuxnet has gained more than
toriety since it was discovered in the summer of 2010. It
havoc on Iran's nuclear program. It stirred suspicions that it
unleashed by the Israelis, the Americans or both. And, last
y least, it heightened long-standing concerns about the
for a cyber attack on critical infrastructure in the West.

se of Iran, Stuxnet worked its way into an industrial control
y rather insidious means -- identifying the centrifuges used to
anium and causing them to spin so rapidly that they began to
ıt experts have said that the worm could just as easily serve as
nt to sabotage machines that are critical to power plants,
grids and other utilities in the United States and elsewhere.

nt at VirusBlokAda, in Minsk, Belarus.
wn the type of SCADA (supervisory
geted by the worm, "told us their
y reason," Ulasen said in an e-mail

Mossad's Miracle Weapon

Stuxnet Virus Opens New Era of Cyber War

By Holger Stark

dpa

The Mossad, Israel's foreign intelligence agency, attacked the Iranian nuclear program with a highly sophisticated computer virus called Stuxnet. The first digital weapon of geopolitical importance, it could change the way wars are fought -- and it will not be the last attack of its kind.

Natanz, we have a problem.

Microsoft Investigating Windows Security Zero-Day Targeted by Trojan

LinkedIn Twitter 5 Facebook

By: Brian Prince
2010-07-16
Article Rating: ★★★★★ / 3
There are 0user comments on this IT

COMPUTERWORLD

News

Siemens: German customer hit by industrial worm

By R

SPIEGEL ONLINE

The Washington Post
NATIONA

:26 AM ET, 09/20/2011

tuxnet, waiting on Pandora's box

Ukman

erious computer worm known as Stuxnet has gained more than
toriety since it was discovered in the summer of 2010. It
havoc on Iran's nuclear program. It stirred suspicions that it
unleashed by the Israelis, the Americans or both. And, last
y least, it heightened long-standing concerns about the
for a cyber attack on critical infrastructure in the West.

Mossad's Miracle Weapon

Stuxnet Virus Opens New Era of Cyber War

By Holger Stark

The Mossad, Israel's foreign intelligence ag
program with a highly sophisticated comput
digital weapon of geopolitical importance, it could change the way wars are fought -- and it will not be the last attack of its kind.

se of Iran, Stuxnet worked its
y rather insidious means -- i
anium and causing them to s

The Economist

Cyberwar

The meaning of Stuxnet

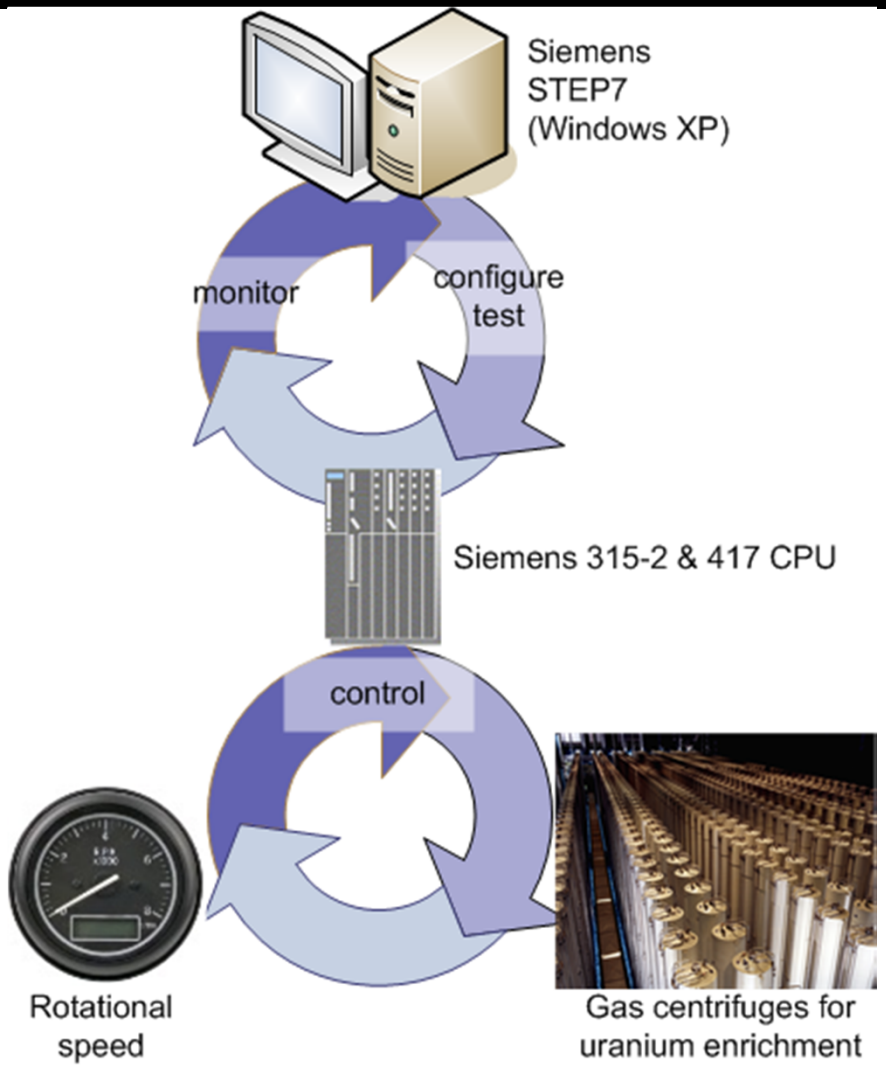
A sophisticated "cyber-missile" highlights the potential—and limitations—of cyberwar

Sep 30th 2010 | from the print edition

Like 274 Tweet 0

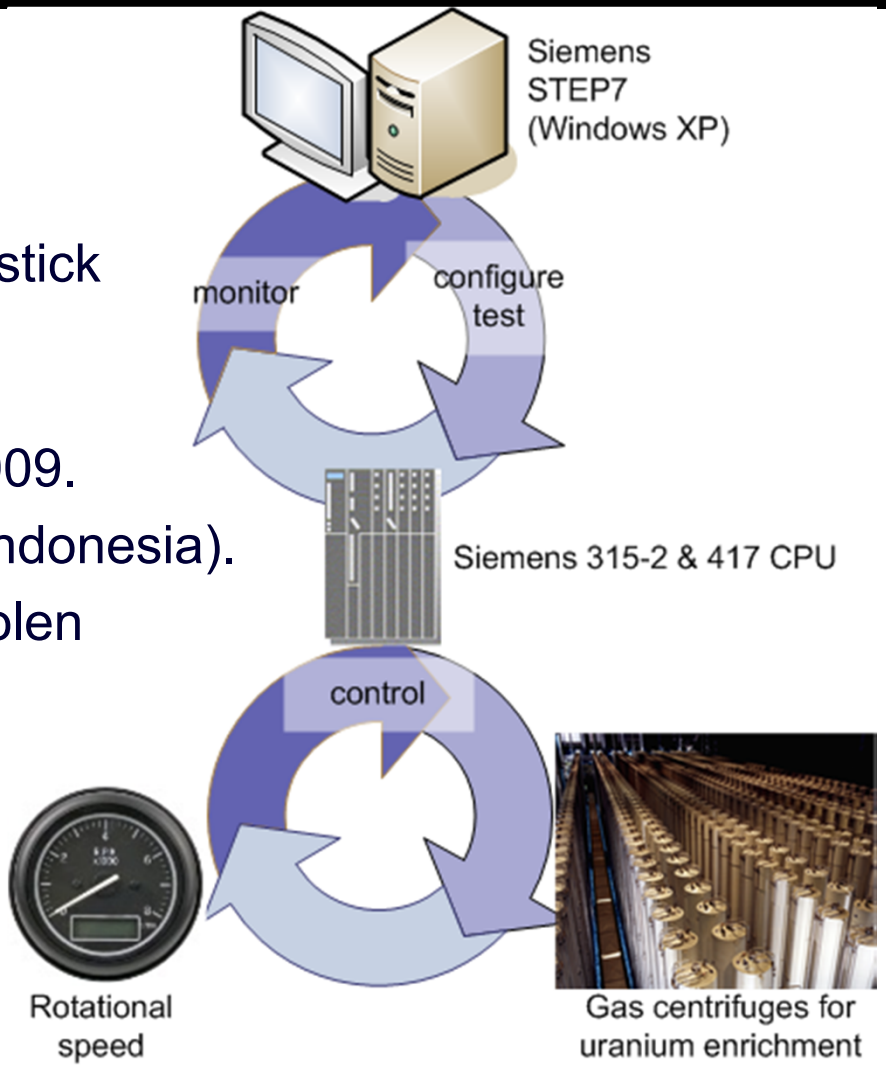
y reason," Olasch said in an e-mail

The Workings of Stuxnet (I)




The Workings of Stuxnet (I)

- An infected USB stick was infiltrated into the plant either by malicious act or through social engineering.
- Once inserted into a Windows PC, the stick tried to compromize the O/S with up to 4(!) zero-day exploits (worth >$100k).
- There were 4-5 evolutions starting 6/2009.
- Infected 100.000 PCs (60% Iran,10% Indonesia).
- Using "rootkit" technologies and two stolen certificates, it hid from being detected.
- It tried to infect other hosts and establish a P2P connection "home".

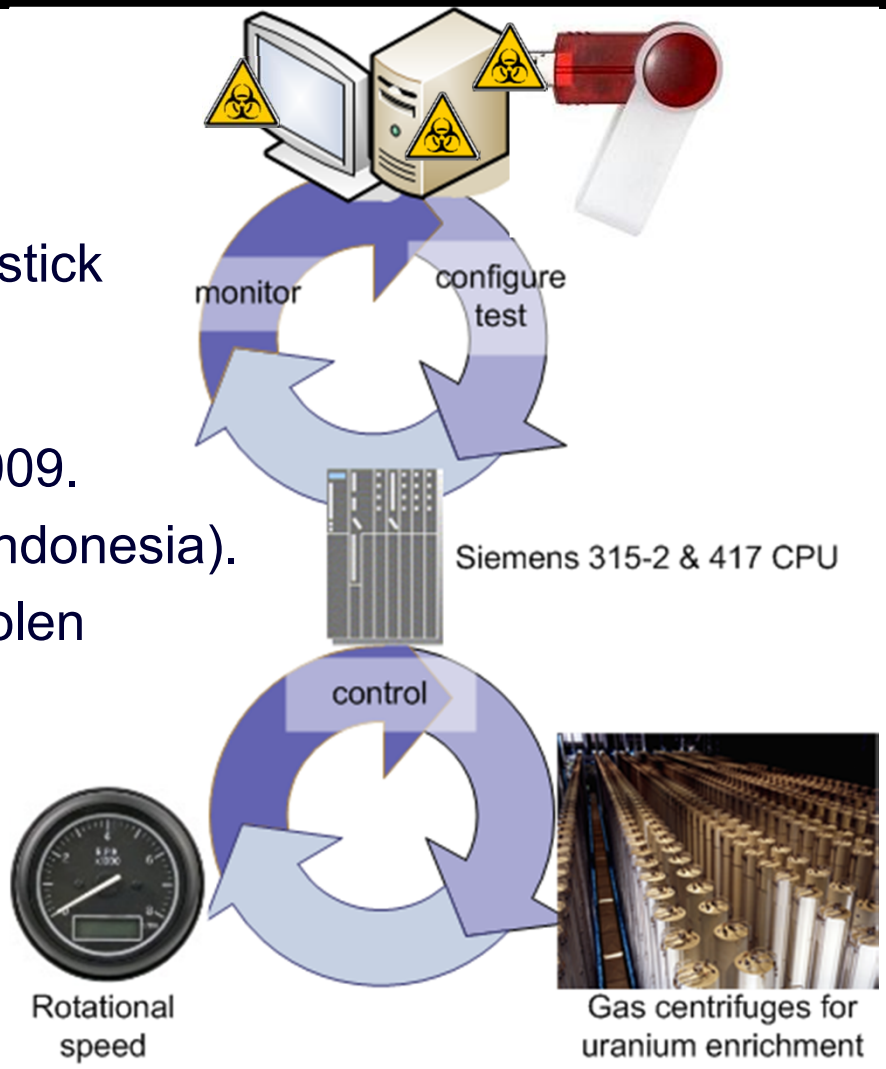



The Workings of Stuxnet (I)

- An infected USB stick was infiltrated into the plant either by malicious act or through social engineering.
- Once inserted into a Windows PC, the stick tried to compromize the O/S with up to 4(!) zero-day exploits (worth >$100k).
- There were 4-5 evolutions starting 6/2009.
- Infected 100.000 PCs (60% Iran,10% Indonesia).
- Using "rootkit" technologies and two stolen certificates, it hid from being detected.
- It tried to infect other hosts and establish a P2P connection "home".

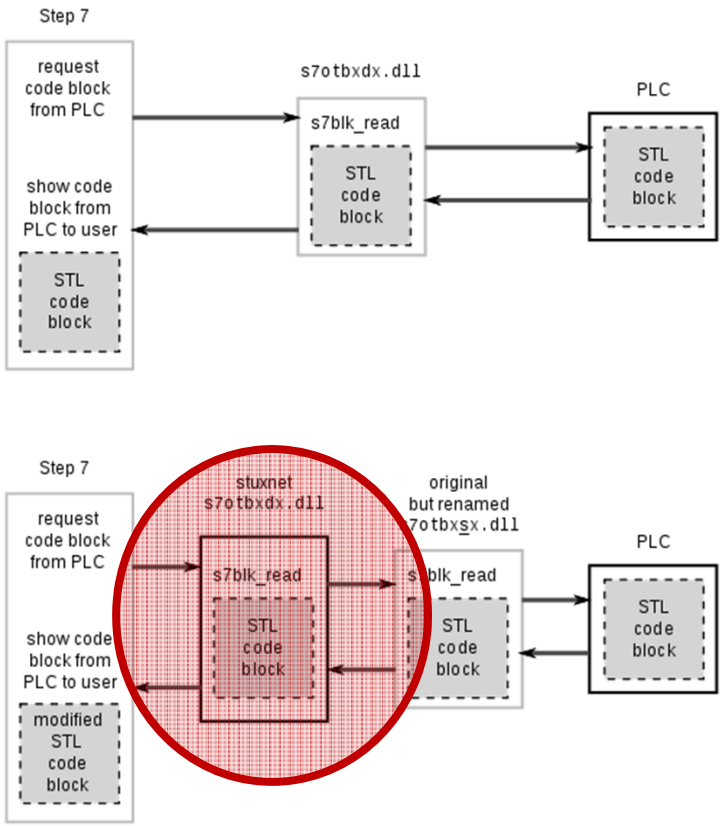
So far, nothing new:

A standard,
but expensive virus!



The Workings of Stuxnet (II)

- Stuxnet then checked the local configuration looking for the presence of Siemens PCS7/STEP7/WINCC SCADA software.
- If so, it copied itself into the local STEP7 project folder (to propagate further).
- It replaced the S7 communication libraries (DLLs) used for exchanging data with a PLC.
- Stuxnet can now manipulate values to be send to the PLC or displayed by the SCADA.

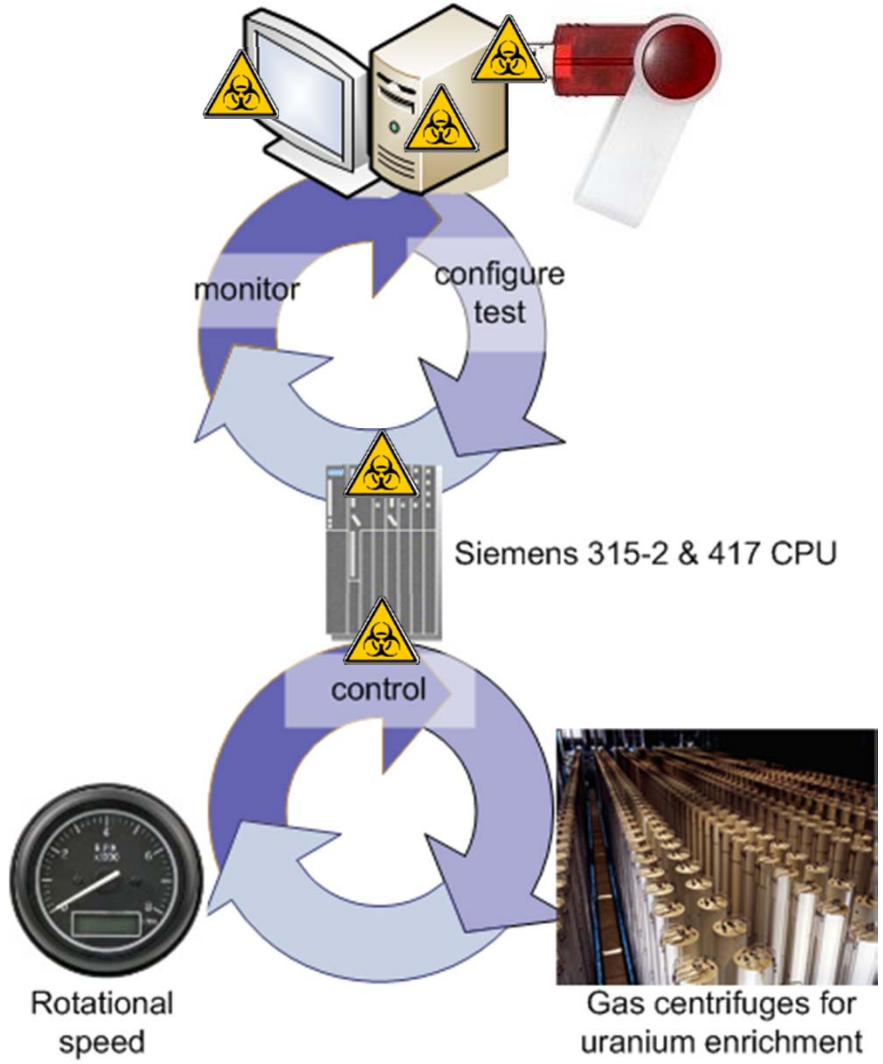


Stuxnet is now the "Man in the Middle" controlling the communication between SCADA & PLC.

- If not, Stuxnet got idle and would expire on 2012/06/24.

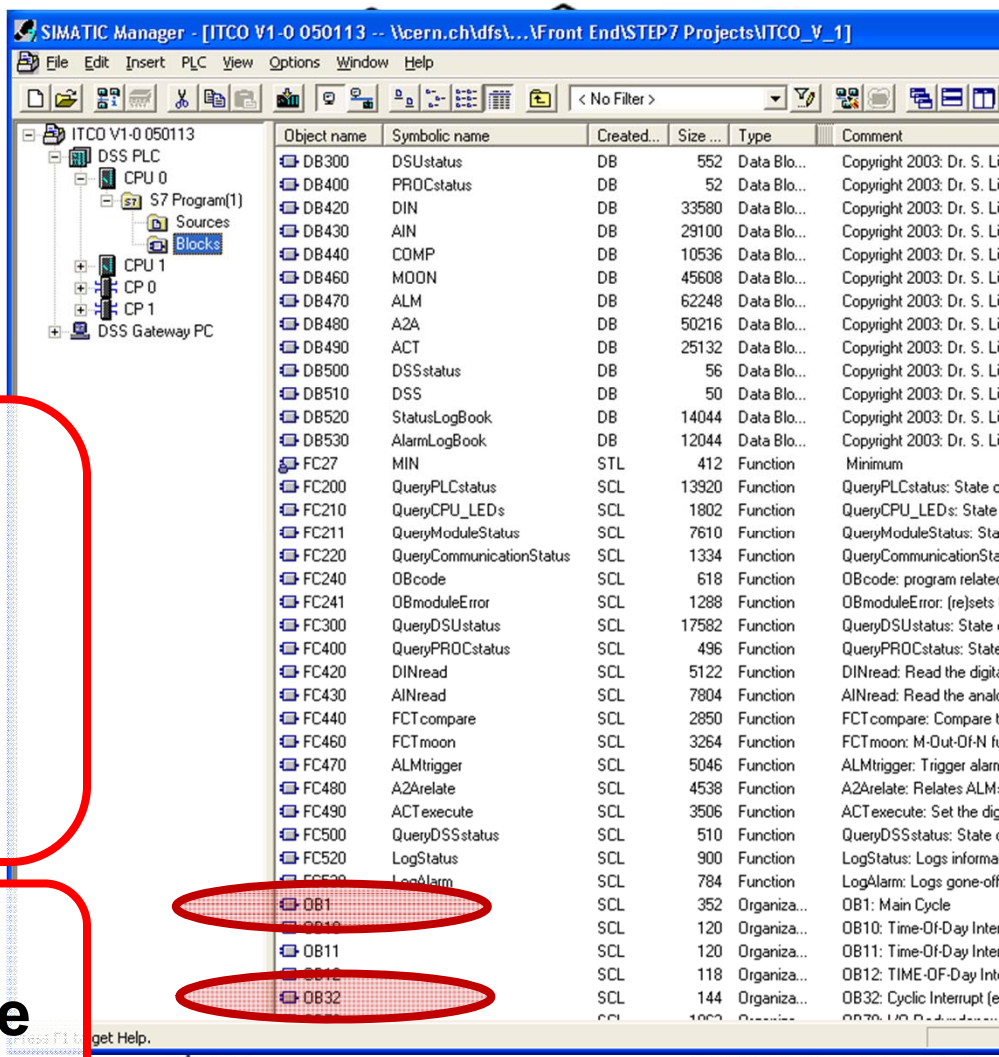
The Workings of Stuxnet (III)

- Next, Stuxnet was "fingerprinting" connected PLCs.
- If right PLC configuration, it downloaded/replaced code between17and 32 FBs & DBs.



The Workings of Stuxnet (III)

- Next, Stuxnet was "fingerprinting" connected PLCs.
- If right PLC configuration, it downloaded/replaced code between17and 32 FBs & DBs.



This code varied the rotational speed of the centrifuges over months wearing them out and inhibiting uranium enrichment.

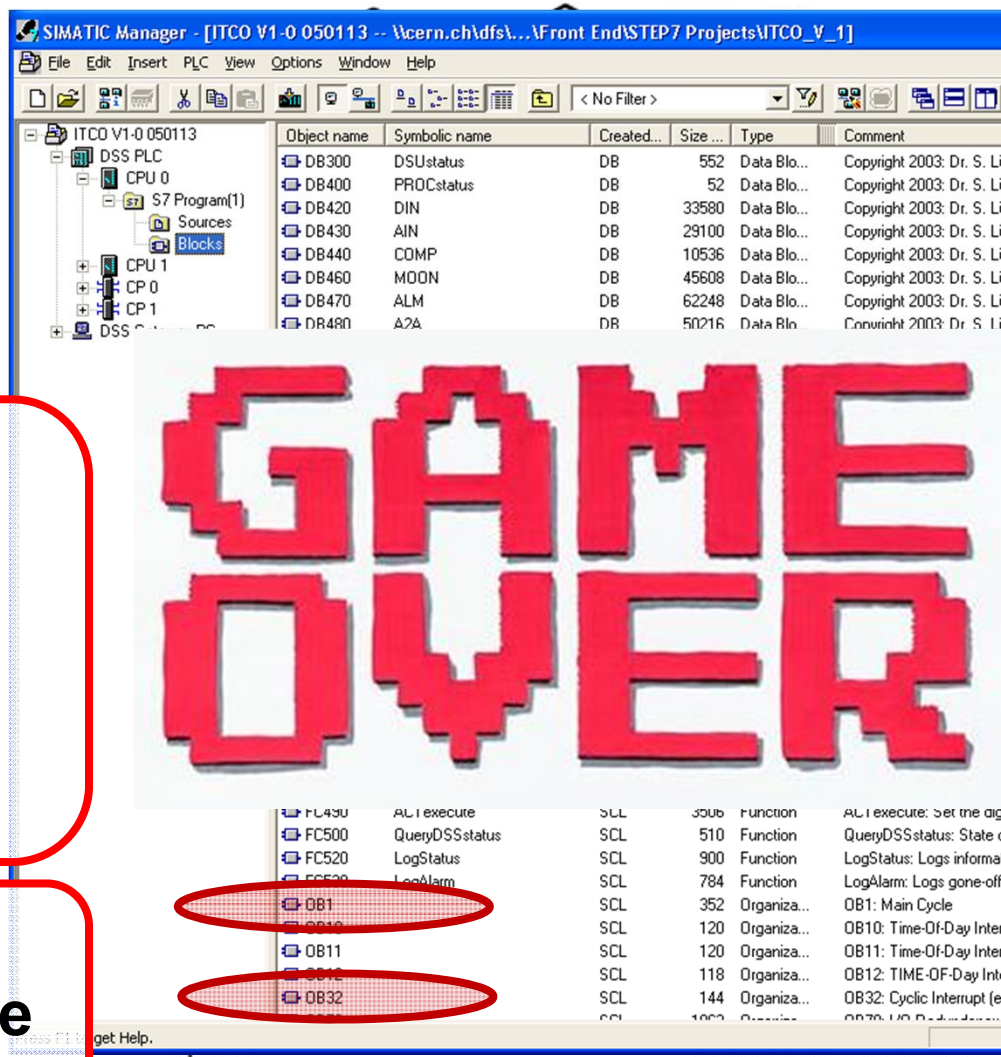
The "Man in the Middle" made everything looked fine at the SCADA level…

The Workings of Stuxnet (III)

- Next, Stuxnet was "fingerprinting" connected PLCs.
- If right PLC configuration, it downloaded/replaced code between17and 32 FBs & DBs.

This code varied the rotational speed of the centrifuges over months wearing them out and inhibiting uranium enrichment.

The "Man in the Middle" made everything looked fine at the SCADA level…

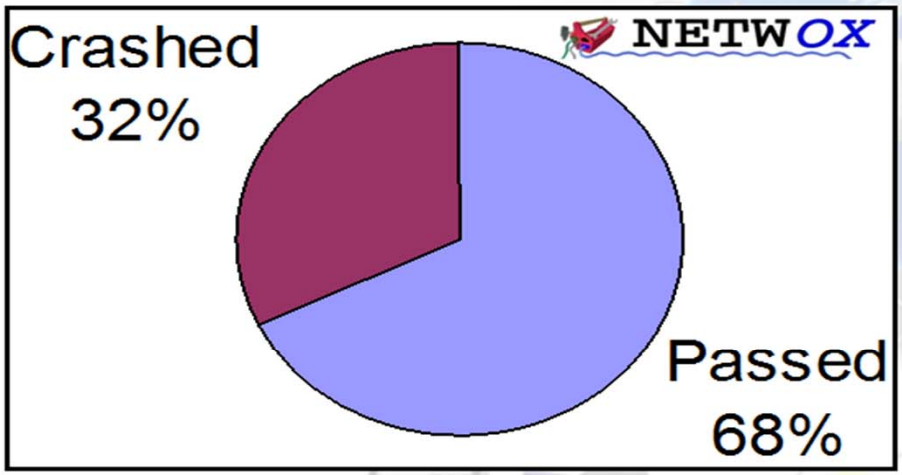


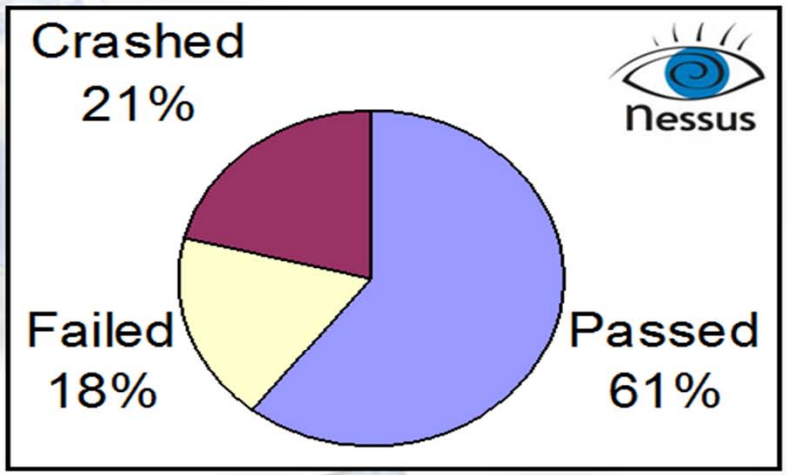
GAME OVER

Déjà vu?

Controls under Attack !

- 20 devices from 6 different manufacturers (35 tests in total)
- All devices fully configured <u>but running idle</u>





...PLCs <u>under load</u> seem to fail even more frequently !!!

...results improve with more recent firmware versions ☺

…but we had this before!

CIA slipped bugs to Soviets

Memoir recounts Cold War technological sabotage

By David E. Hoffman

washingtonpost.com

updated 12:13 a.m. ET Feb. 27, 2004

In January 1982, President Ronald Reagan approved a CIA plan to sabotage the economy of the Soviet Union through covert transfers of technology that contained hidden malfunctions, including software that later triggered a huge explosion in a Siberian natural gas pipeline, according to a new memoir by a Reagan White House official.

The Washi

Obama to ta
policy

Toyota face
warn of def

Corrections

Obama to m
church lead

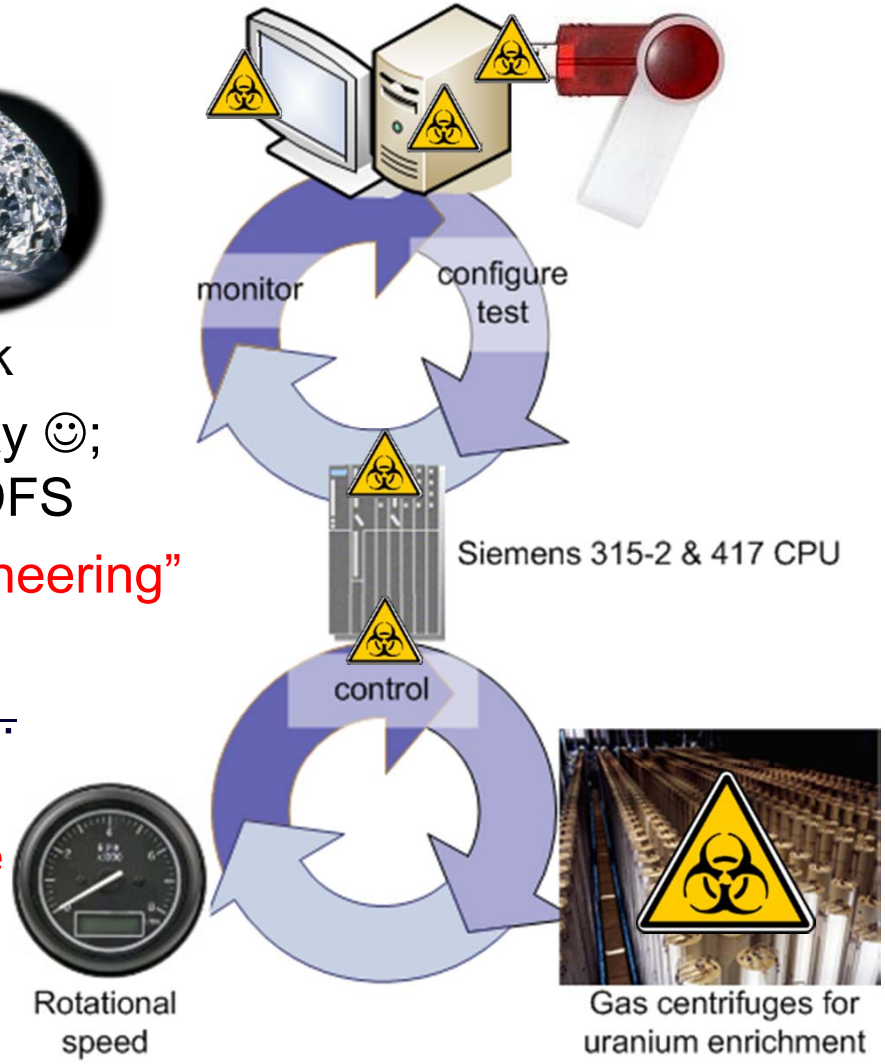
Easter quak
downtown

Protective Measures (I)

- Deploy a Defense-in-Depth protection




- Establish security cells on your network
- Forbid usage of USB keys or use Epoxy ☺; restrict usage of CDs, open shares & DFS
- Teach your experts about "Social Engineering"
- ~~Screen your experts: alcohol/drugs, financial, psychological/social/family, …~~
- Patch, patch, patch…
  …and run up-to-date antivirus software
  (wouldn't have helped here ☹)

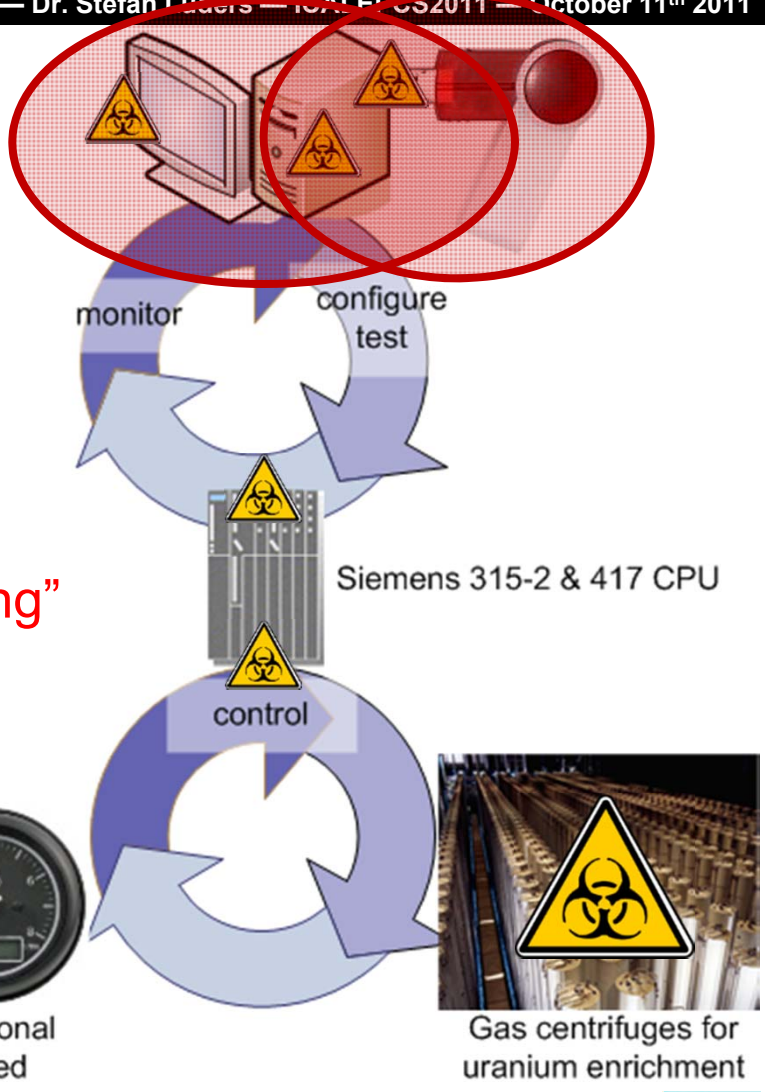


Protective Measures (I)

- Deploy a Defense-in-Depth protection



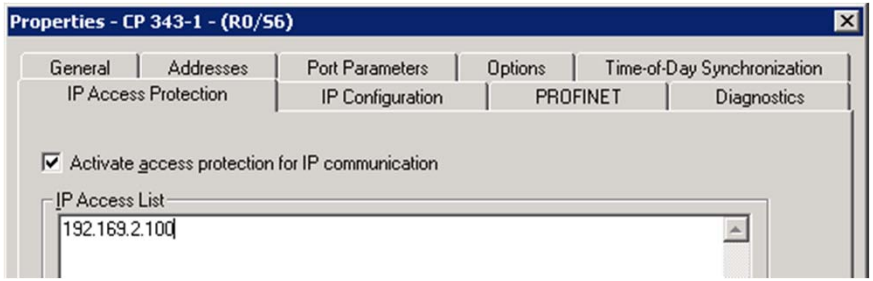

- Establish security cells on your network
- Forbid usage of USB keys or use Epoxy ☺; restrict usage of CDs, open shares & DFS
- Teach your experts about "Social Engineering"
- ~~Screen your experts: alcohol/drugs, financial, psychological/social/family, …~~
- Patch, patch, patch…
  …and run up-to-date antivirus software
  (wouldn't have helped here ☹)



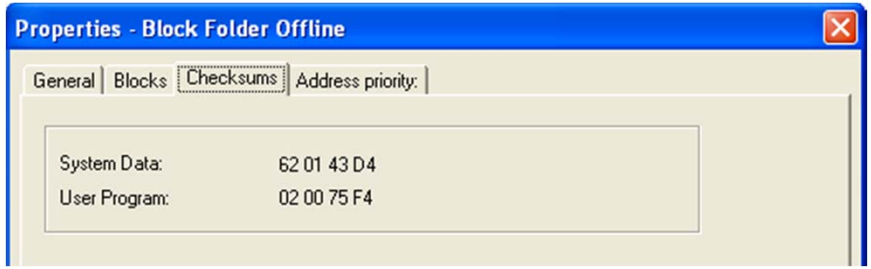
Apply Defense-in-Depth!!!
…and follow a standard.

Protective Measures (II)

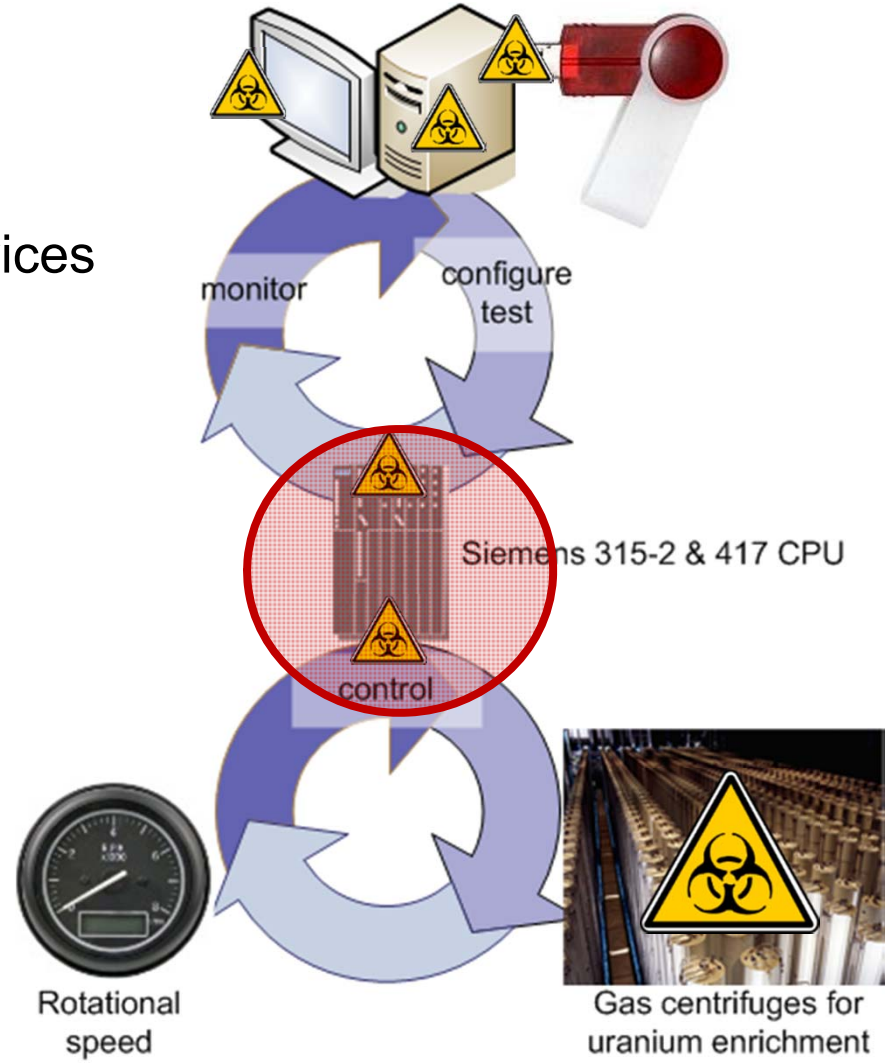
- Scan you PLCs on vulnerabilities & robustness
- Lock down the PLC configuration:
  Enable firewall, disable unneeded services



- Enable PLC intrusion detection



Talk to your vendor!
Accept the residual risk.




(My personal) Conclusions

Stuxnet was the wake-up call... but for whom ☹?

- Attackers and researchers are now poking around control system security
- The media is creating a hype and call out the "Era of Cyber-War"
- Security companies enter in the belief knowing control systems well

Vendors are now open to act and users to demand ☺

- Note: this was not against Siemens, they just happened to be involved

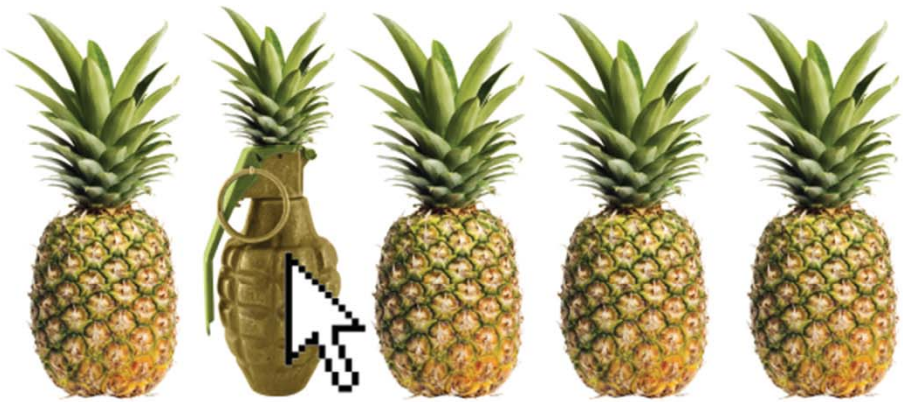
Control System Cyber-Security
is now / must now be taken seriously.
Defense-in-Depth is the key!!!

Choose a standard and follow it.
Get all stakeholders involved:
controls experts, IT/security experts, vendors.

Merci beaucoup!!!

Protect your computers

Any unprotected computer connected to the Internet is likely to be infected within minutes!



Be careful with e-mail & Web

Cybercriminals are trying to trick you!