



# Stuxnet: Dawn of a new era

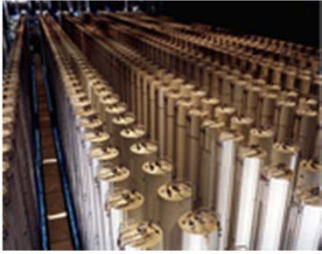
...about the hype & consequences of Stuxnet

**Dr. Stefan Lüders (CERN Computer Security Officer)**

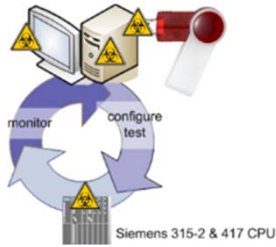
ICALEPCS2011

Grenoble (France), October 11<sup>th</sup> 2011





## 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.

"Stuxnet: Dawn of a new era" — Dr. Stefan Lüders — ICALEPCS2011 — October 11<sup>th</sup> 2011

## Microsoft Investigating Windows Security Zero-Day Targeted by Trojan

 LinkedIn  Twitter 5  Facebook

By: Brian Prince

2010-07-16

Article Rating: ★★★★★ / 3

[There are 0 user comments on this IT Security Review](#)

**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.

"Stuxnet: Dawn of a new era" — Dr. Stefan Lüders — ICALEPCS2011 — October 11<sup>th</sup> 2011

## Microsoft Investigating Windows Security Zero-Day Targeted by Trojan

[LinkedIn](#) [Twitter](#) 5 [Facebook](#)

By: Brian Prince  
2010-07-16

Article Rating: ★★★★★ / 3

[There are 0 user comments on this IT Reviews](#)

Microsoft is investigating reports of a 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 targeting industrial companies.

News

## Siemens: German customer hit by industrial worm

By Robert McMillan

July 20, 2010 07:47 PM ET

1 Comment

[Gefällt mir](#)

+1 0

# COMPUTERWORLD

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.

"Stuxnet: Dawn of a new era" — Dr. Stefan Lüders — ICALEPCS2011 — October 11<sup>th</sup> 2011

## Microsoft Investigating Windows Security Zero-Day Targeted by Trojan

[LinkedIn](#) [Twitter](#) 5 [Facebook](#)

By: Brian Prince  
2010-07-16

Article Rating: ★★★★★ / 3

[There are 0 user comments on this IT Reviews](#)

Microsoft is investigating reports of a 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 targeting industrial companies.

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 been 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.

# COMPUTERWORLD

The Washington Post

# NATIONAL

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.

"Stuxnet: Dawn of a new era" — Dr. Stefan Lüders — ICALEPCS2011 — October 11<sup>th</sup> 2011

## Microsoft Investigating Windows Security Zero-Day Targeted by Trojan

[LinkedIn](#)
[Twitter](#)
5
[Facebook](#)

By: Brian Prince

2010-07-16

Article Rating: ★★★★★ / 3

[There are 0 user comments on this IT:](#)

Mossad's Miracle Weapon

## Stuxnet Virus Opens New Era of Cyber War

By Holger Stark



Photos ▶

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.

## COMPUTERWORLD

## Siemens: German customer hit by industrial worm

By R

**SPIEGEL ONLINE**

:26 AM ET, 09/20/2011

Stuxnet, waiting on Pandora's box

[Ukman](#)

A serious computer worm known as Stuxnet has gained more than notoriety since it was discovered in the summer of 2010. It has caused havoc on Iran's nuclear program. It stirred suspicions that it was unleashed by the Israelis, the Americans or both. And, last but not least, it heightened long-standing concerns about the possibility of 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 vibrate. 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.

It was found at virusBlokada, in Minsk, Belarus.

When the type of SCADA (supervisory control and data acquisition) system targeted by the worm, "told us their reason," Ulasen said in an e-mail







# Natanz, we have a problem.

"Stuxnet: Dawn of a new era" — Dr. Stefan Lüders — ICALEPCS2011 — October 11<sup>th</sup> 2011

## Microsoft Investigating Windows Security Zero-Day Targeted by Trojan

LinkedIn Twitter 5 Facebook

By: Brian Prince  
2010-07-16

Article Rating: ★★★★★ / 3

[There are 0 user comments on this IT.](#)

Mossad's Miracle Weapon

## Stuxnet Virus Opens New Era of Cyber War

By Holger Stark



COMPUTERWORLD

## Siemens: German customer hit by industrial worm

By R **SPIEGEL ONLINE** 10:26 AM ET, 09/20/2011

Stuxnet, waiting on Pandora's box

[Ukman](#)

A serious computer worm known as Stuxnet has gained more than notoriety since it was discovered in the summer of 2010. It has caused havoc on Iran's nuclear program. It stirred suspicions that it was unleashed by the Israelis, the Americans or both. And, last but not least, it heightened long-standing concerns about the possibility of a cyber attack on critical infrastructure in the West.

Use of Iran, Stuxnet worked its way rather insidious means -- it targeted uranium and causing them to stop

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

Facebook Like 274 Twitter Tweet 0

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

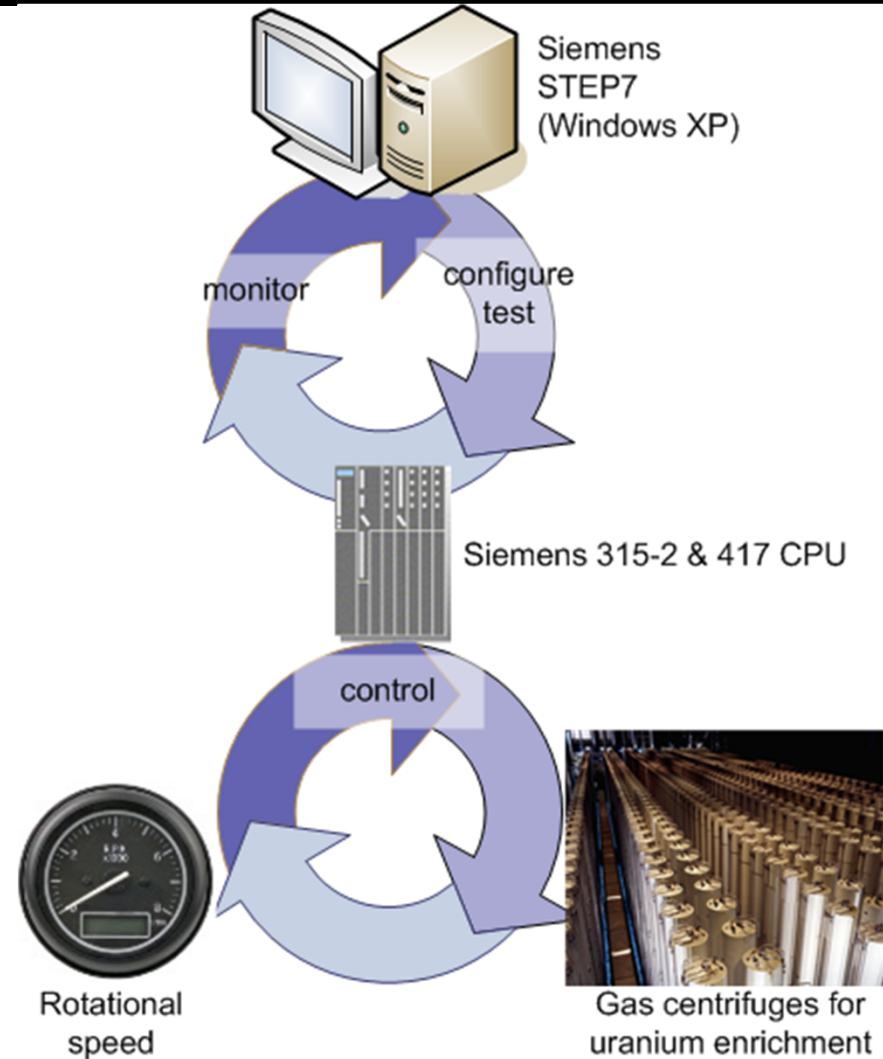
by reason, ... said in an e-mail





# The Workings of Stuxnet (I)

"Stuxnet: Dawn of a new era" — Dr. Stefan Lüders — ICALEPCS2011 — October 11<sup>th</sup> 2011



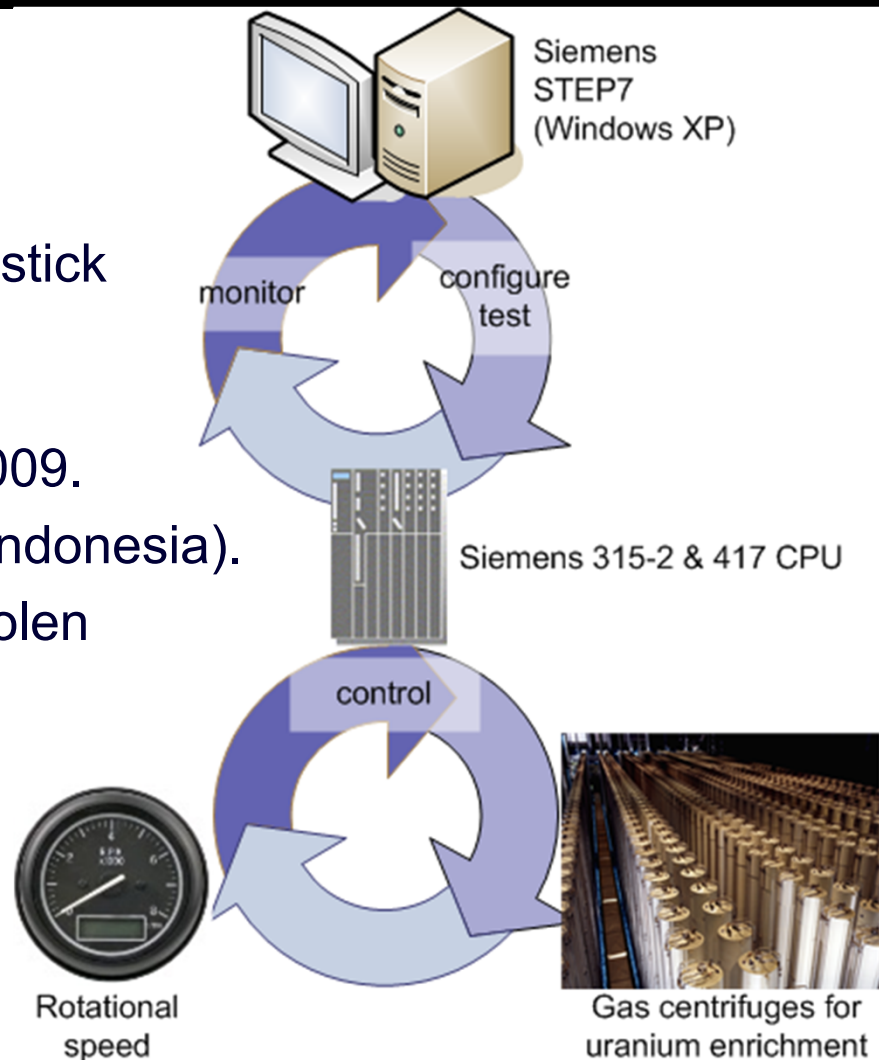




# The Workings of Stuxnet (I)

“Stuxnet: Dawn of a new era” — Dr. Stefan Lüders — ICALEPCS2011 — October 11<sup>th</sup> 2011

- ▶ 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 compromise 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”.



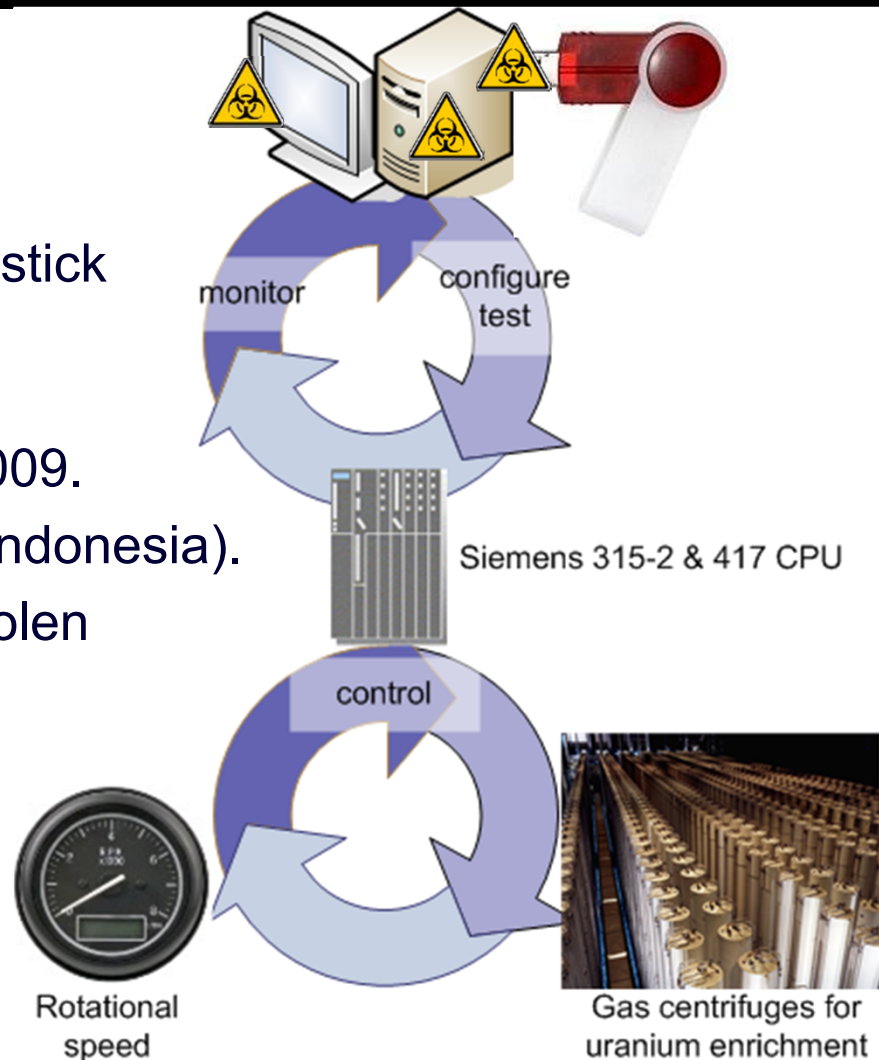


# The Workings of Stuxnet (I)

"Stuxnet: Dawn of a new era" — Dr. Stefan Lüders — ICALEPCS2011 — October 11<sup>th</sup> 2011

- ▶ 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 compromise 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!**





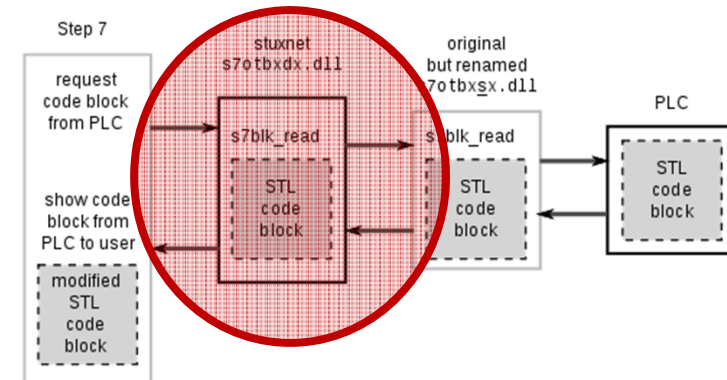
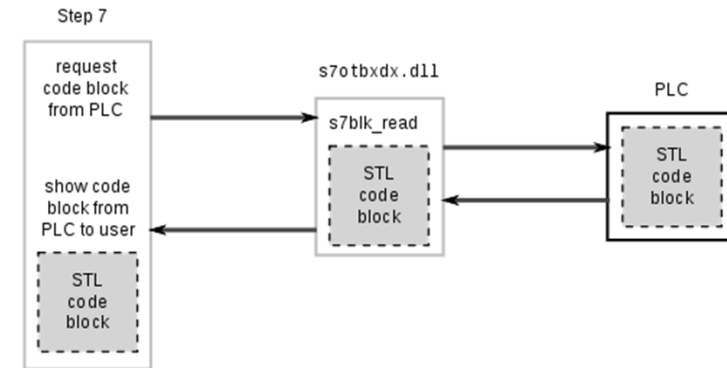


# The Workings of Stuxnet (II)

“Stuxnet: Dawn of a new era” — Dr. Stefan Lüders — ICALEPCS2011 — October 11<sup>th</sup> 2011

- ▶ 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.**



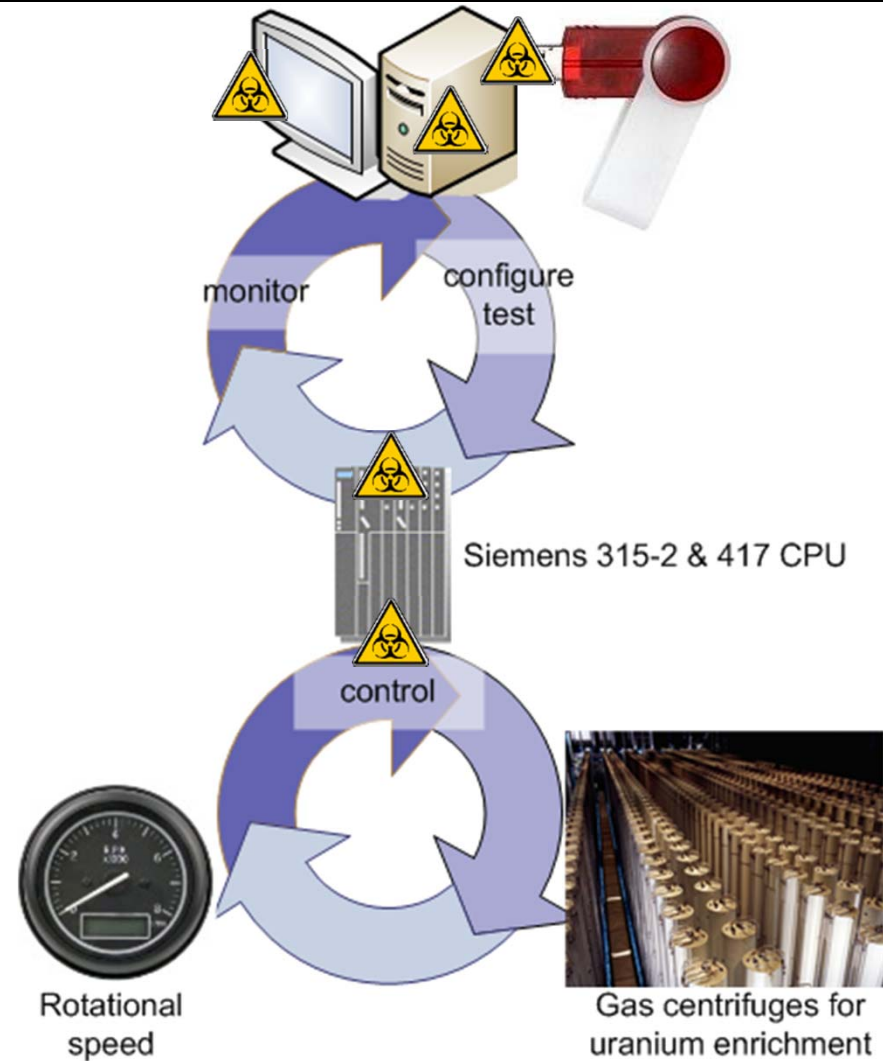
- ▶ If not, Stuxnet got idle and would expire on 2012/06/24.



# The Workings of Stuxnet (III)

“Stuxnet: Dawn of a new era” — Dr. Stefan Lüders — ICALEPCS2011 — October 11<sup>th</sup> 2011

- ▶ Next, Stuxnet was “fingerprinting” connected PLCs.
- ▶ If right PLC configuration, it downloaded/replaced code between 17 and 32 FBs & DBs.







# The Workings of Stuxnet (III)

“Stuxnet: Dawn of a new era” — Dr. Stefan Lüders — ICALEPCS2011 — October 11<sup>th</sup> 2011

- ▶ Next, Stuxnet was “fingerprinting” connected PLCs.
- ▶ If right PLC configuration, it downloaded/replaced code between 17 and 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...**

SIMATIC Manager - [ITCO V1-0 050113 -- \cern.ch\dfs\... \Front End\STEP7 Projects\ITCO\_V\_1]

File Edit Insert PLC View Options Window Help

< No Filter >

Object name	Symbolic name	Created...	Size...	Type	Comment
DB300	DSUstatus	DB	552	Data Blo...	Copyright 2003: Dr. S. Lüders
DB400	PROCstatus	DB	52	Data Blo...	Copyright 2003: Dr. S. Lüders
DB420	DIN	DB	33580	Data Blo...	Copyright 2003: Dr. S. Lüders
DB430	AIN	DB	29100	Data Blo...	Copyright 2003: Dr. S. Lüders
DB440	COMP	DB	10536	Data Blo...	Copyright 2003: Dr. S. Lüders
DB460	MOON	DB	45608	Data Blo...	Copyright 2003: Dr. S. Lüders
DB470	ALM	DB	62248	Data Blo...	Copyright 2003: Dr. S. Lüders
DB480	A2A	DB	50216	Data Blo...	Copyright 2003: Dr. S. Lüders
DB490	ACT	DB	25132	Data Blo...	Copyright 2003: Dr. S. Lüders
DB500	DSSstatus	DB	56	Data Blo...	Copyright 2003: Dr. S. Lüders
DB510	DSS	DB	50	Data Blo...	Copyright 2003: Dr. S. Lüders
DB520	StatusLogBook	DB	14044	Data Blo...	Copyright 2003: Dr. S. Lüders
DB530	AlarmLogBook	DB	12044	Data Blo...	Copyright 2003: Dr. S. Lüders
FC27	MIN	STL	412	Function	Minimum
FC200	QueryPLCstatus	SCL	13920	Function	QueryPLCstatus: State of PLC
FC210	QueryCPU_LEDs	SCL	1802	Function	QueryCPU_LEDs: State of CPU
FC211	QueryModuleStatus	SCL	7610	Function	QueryModuleStatus: State of Module
FC220	QueryCommunicationStatus	SCL	1334	Function	QueryCommunicationStatus: State of Communication
FC240	OBcode	SCL	618	Function	OBcode: program related
FC241	OBmoduleError	SCL	1288	Function	OBmoduleError: (re)sets
FC300	QueryDSUstatus	SCL	17582	Function	QueryDSUstatus: State of DSU
FC400	QueryPROCstatus	SCL	496	Function	QueryPROCstatus: State of PROC
FC420	DINread	SCL	5122	Function	DINread: Read the digital input
FC430	AINread	SCL	7804	Function	AINread: Read the analog input
FC440	FCTcompare	SCL	2850	Function	FCTcompare: Compare the digital input
FC460	FCTmoon	SCL	3264	Function	FCTmoon: M-Out-Of-N function
FC470	ALMtrigger	SCL	5046	Function	ALMtrigger: Trigger alarm
FC480	A2Arelate	SCL	4538	Function	A2Arelate: Relates ALM to A2A
FC490	ACTexecute	SCL	3506	Function	ACTexecute: Set the digital output
FC500	QueryDSSstatus	SCL	510	Function	QueryDSSstatus: State of DSS
FC520	LogStatus	SCL	900	Function	LogStatus: Logs information
FC530	LogAlarm	SCL	784	Function	LogAlarm: Logs gone-off
OB1	OB1	SCL	352	Organiza...	OB1: Main Cycle
OB10	OB10	SCL	120	Organiza...	OB10: Time-Of-Day Interrupt
OB11	OB11	SCL	120	Organiza...	OB11: Time-Of-Day Interrupt
OB12	OB12	SCL	118	Organiza...	OB12: TIME-OF-Day Interrupt
OB32	OB32	SCL	144	Organiza...	OB32: Cyclic Interrupt (e.g. for PLC)



# The Workings of Stuxnet (III)

"Stuxnet: Dawn of a new era" — Dr. Stefan Lüders — ICALEPCS2011 — October 11<sup>th</sup> 2011

- ▶ Next, Stuxnet was "fingerprinting" connected PLCs.
- ▶ If right PLC configuration, it downloaded/replaced code between 17 and 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...

Object name	Symbolic name	Created...	Size...	Type	Comment
DB300	DSUstatus	DB	552	Data Blo...	Copyright 2003: Dr. S. Lüders
DB400	PROCstatus	DB	52	Data Blo...	Copyright 2003: Dr. S. Lüders
DB420	DIN	DB	33580	Data Blo...	Copyright 2003: Dr. S. Lüders
DB430	AIN	DB	29100	Data Blo...	Copyright 2003: Dr. S. Lüders
DB440	COMP	DB	10536	Data Blo...	Copyright 2003: Dr. S. Lüders
DB460	MOON	DB	45608	Data Blo...	Copyright 2003: Dr. S. Lüders
DB470	ALM	DB	62248	Data Blo...	Copyright 2003: Dr. S. Lüders
DB480	A2A	DB	50216	Data Blo...	Copyright 2003: Dr. S. Lüders

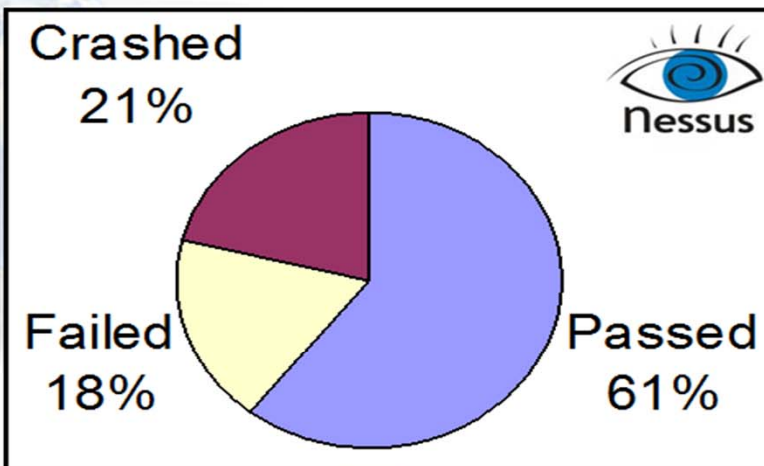
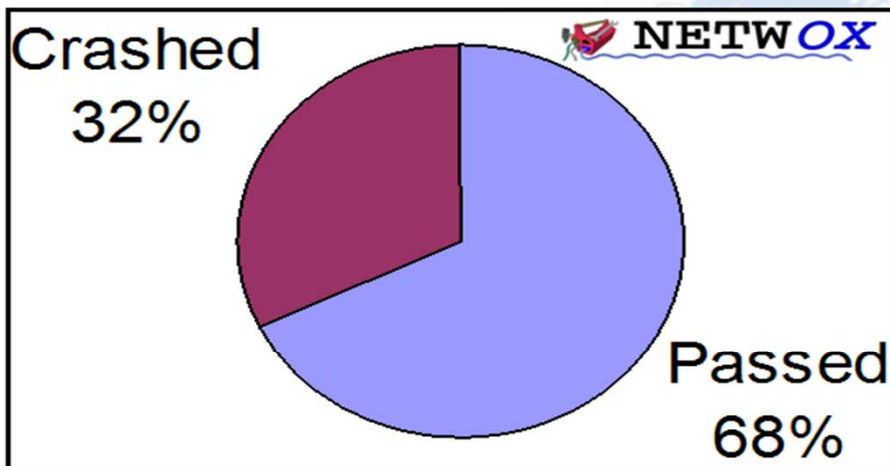
  

Object name	Symbolic name	Created...	Size...	Type	Comment
FC500	QueryDSSstatus	SCL	510	Function	QueryDSSstatus: State of...
FC520	LogStatus	SCL	900	Function	LogStatus: Logs informa...
FC530	LogAlarm	SCL	784	Function	LogAlarm: Logs gone-off...
OB1		SCL	352	Organiza...	OB1: Main Cycle
OB10		SCL	120	Organiza...	OB10: Time-Of-Day Inter...
OB11		SCL	120	Organiza...	OB11: Time-Of-Day Inter...
OB12		SCL	118	Organiza...	OB12: TIME-OF-Day Int...
OB32		SCL	144	Organiza...	OB32: Cyclic Interrupt (e...



## Controls under Attack !

- ▶ 20 devices from 6 different manufacturers (35 tests in total)
- ▶ All devices fully configured but running idle



***...PLCs under load seem to fail even more frequently !!!***  
***...results improve with more recent firmware versions ☺***



# ...but we had this before!

"Stuxnet: Dawn of a new era" — Dr. Stefan Lüders — ICALEPCS2011 — October 11<sup>th</sup> 2011

## CIA slipped bugs to Soviets

### Memoir recounts Cold War technological sabotage

By David E. Hoffman

[washingtonpost.com](http://www.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







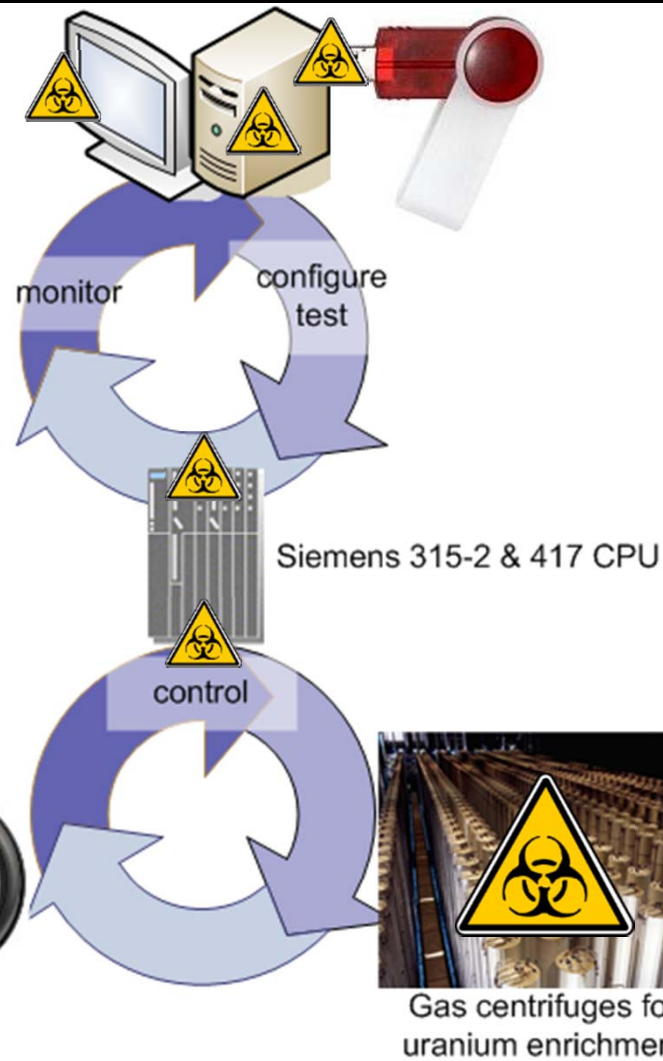
# Protective Measures (I)

"Stuxnet: Dawn of a new era" — Dr. Stefan Lüders — ICALEPCS2011 — October 11<sup>th</sup> 2011

- ▶ 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 ☹)





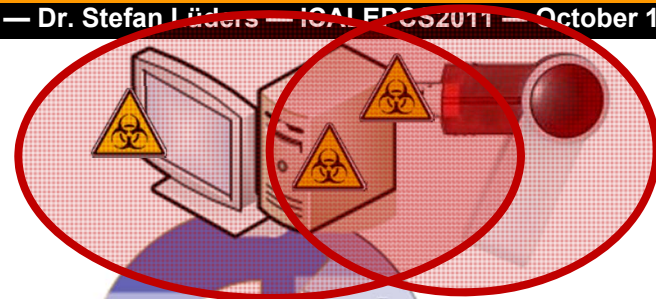
# Protective Measures (I)

"Stuxnet: Dawn of a new era" — Dr. Stefan Lüdgers — ICAI EDCS2011 — October 11<sup>th</sup> 2011

- ▶ 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 ☹)



monitor

configure  
test

Siemens 315-2 & 417 CPU

control



Rotational  
speed



Gas centrifuges for  
uranium enrichment

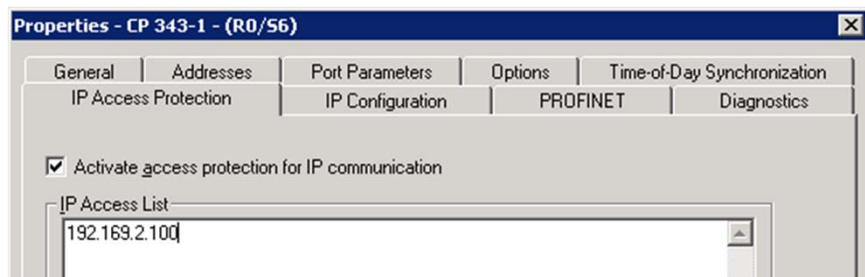
**Apply Defense-in-Depth!!!  
...and follow a standard.**



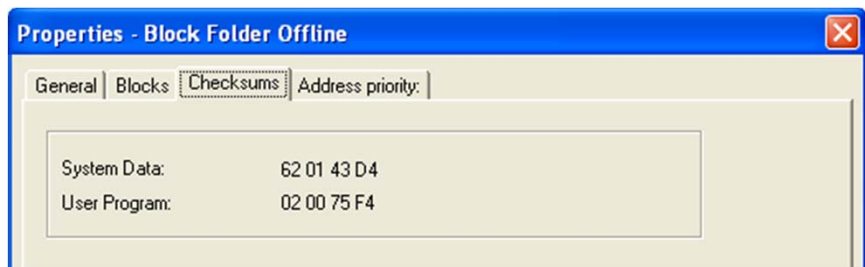
# Protective Measures (II)

“Stuxnet: Dawn of a new era” — Dr. Stefan Lüders — ICALEPCS2011 — October 11<sup>th</sup> 2011

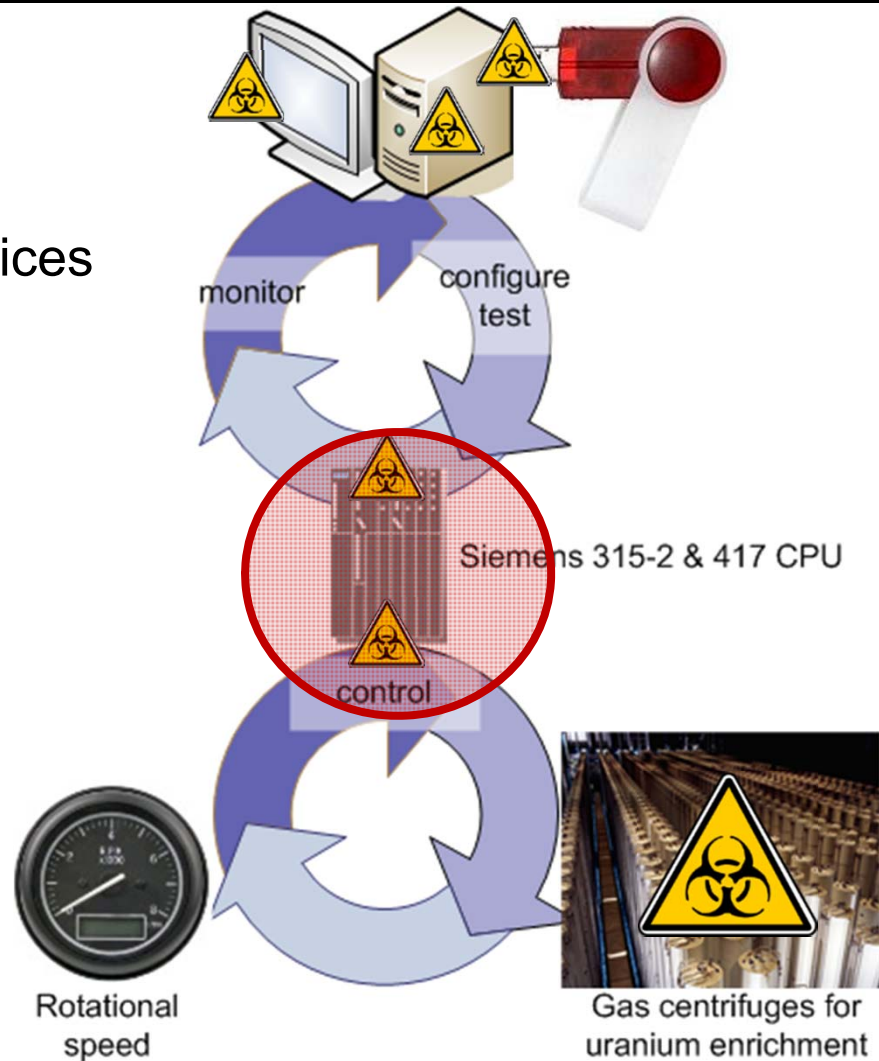
- ▶ **Scan you PLCs** on vulnerabilities & robustness
- ▶ **Lock down the PLC configuration:**  
Enable firewall, disable unneeded services



- ▶ **Enable PLC intrusion detection**



**Talk to your vendor!**  
**Accept the residual risk.**







# (My personal) Conclusions

"Stuxnet: Dawn of a new era" — Dr. Stefan Lüders — ICALEPCS2011 — October 11<sup>th</sup> 2011

## 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!!!

"Stuxnet: Dawn of a new era" — Dr. Stefan Lüders — ICALEPCS2011 — October 11<sup>th</sup> 2011



Courtesy of Microsoft.com



Courtesy Bartek Lynch Nida University

 **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!

