

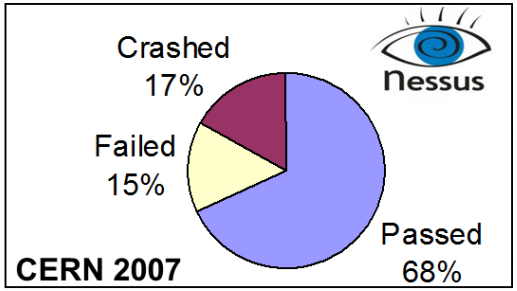
3rd Control System Cyber-Security Workshop

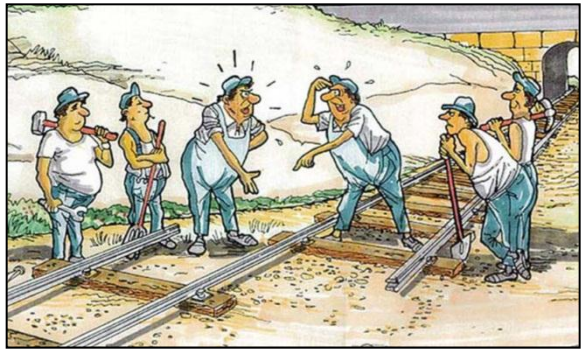
A Summary of this year's meeting

Dr. Stefan Lüders (CERN Computer Security Officer)
with contributions from
E. Bonaccorsi (LHCb), P. Charrue (CERN), P. Chochula (ALICE),
S. Hartman (ORNL), T. Hakulinen (CERN), T. McGuckin (JLab),
T. Sugimoto (Spring8), F. Tilaro (CERN), V. Vuppala (NSCL/MSU)

ICALEPCS, Grenoble (France), October 11th 2011


(R)Evolution, w/o security






(CS)² in HEP — The Objectives

Attendance: ~40 people ☺

Scope:

- All security aspects related with HEP control systems
- Control PCs, control software, controls devices, accounts, …

Objectives:

- Raise awareness
- Exchange of good practices, ideas, and implementations
- Discuss what works & what not, pros & cons
- Report on security events, lessons learned & successes
- Update on progresses

	How things go wrong. LUE *Kilimandjaro Nord, WTC Convention Center, Grenoble (France)*
10:00	**Review of a cyber-security event at Jefferson Lab accelerator network** M *Kilimandjaro Nord, WTC Convention Center, Grenoble (France)*
	Coffee Break *Kilimandjaro Nord, WTC Convention Center, Grenoble (France)*
11:00	**Cybersecurity for the Control System Engineer** HA *Kilimandjaro Nord, WTC Convention Center, Grenoble (France)*
	Experiences with ISO/IEC 27001 Implementation at NSCL *Kilimandjaro Nord, WTC Convention Center, Grenoble (France)*
12:00	**Inventory and Risk assessment of the CERN Technical Network** C *Kilimandjaro Nord, WTC Convention Center, Grenoble (France)*
	Can off-the-shelf control systems be compliant with CERN computer security policy? HA
13:00	**Lunch Break** *Kilimandjaro Nord, WTC Convention Center, Grenoble (France)*
	Cyber security from the ALICE user's perspective C *Kilimandjaro Nord, WTC Convention Center, Grenoble (France)*
14:00	**IT security for the LHCb Experiment** BONA *Kilimandjaro Nord, WTC Convention Center, Grenoble (France)*
	Application and Virus Detecting Firewall on the SPring-8 Experimental User Network SUG
15:00	**Industrial Devices Robustness Assessment and Testing against Cyber Security Attacks**
	Coffee Break *Kilimandjaro Nord, WTC Convention Center, Grenoble (France)*
16:00	**Discussion** I *Kilimandjaro Nord, WTC Convention Center, Grenoble (France)*

Attacks are FACT!

September 2009

Detectors: LAr

Terminal — ssh — ttys000 — 80×2

ssh

26/11/09

ZeuL's Connect B

Dumping Ar

Connec

3200K .....

3250K .....

3300K .....

3350K .....

3400K .....

April 2011

securitynews DAILY

Alerts! | Cybercrime | Home & Auto | Identity Theft | Internet Scams | Malware/Viru

Cyberattack Hits Oak Ridge National

ory

By Matt Liebowitz, SecurityNewsDaily Staff Writer

Summer 2011

Twitter / @reversemode: Writing a post involving C ... - Windows Internet Explorer

http://twitter.com/#!/reversemode/status/100

Favorites

Twitter / @reversemode: Writing a post involving...

twitter

Search

Don't miss any updates from Rubén Santamarta

Get your account on Twitter today to stay up-to-date with what interests you!

Sign up »

Text follow reversemode to 40404 in the United States

@reversemode

Rubén Santamarta

Writing a post involving CERN, LHC, SCADA, passwords... one of the most curious cases I've found.

9 Aug via TweetDeck

Timeline of Attack

Attack initiated across multiple DOE sites

Two externally facing web-servers compromised

Attackers elevate privileges

2011

Source: Verizon

April

Su	M	Tu	W	Th	F	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

May

Su	M	Tu	W	Th	F	Sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

June

Su	M	Tu	W	Th	F	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

July

Su	M	Tu	W	Th	F	Sa
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

August

Su	M	Tu	W	Th	F	Sa
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

September

Su	M	Tu	W	Th	F	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

Mai 2011


Security is a CHALLENGE…

Off-the-shelf IT security not that easy:
Patching, AV, shared passwords, network scans, …

Can off-the-shelf control systems be compliant with CERN computer security policy?

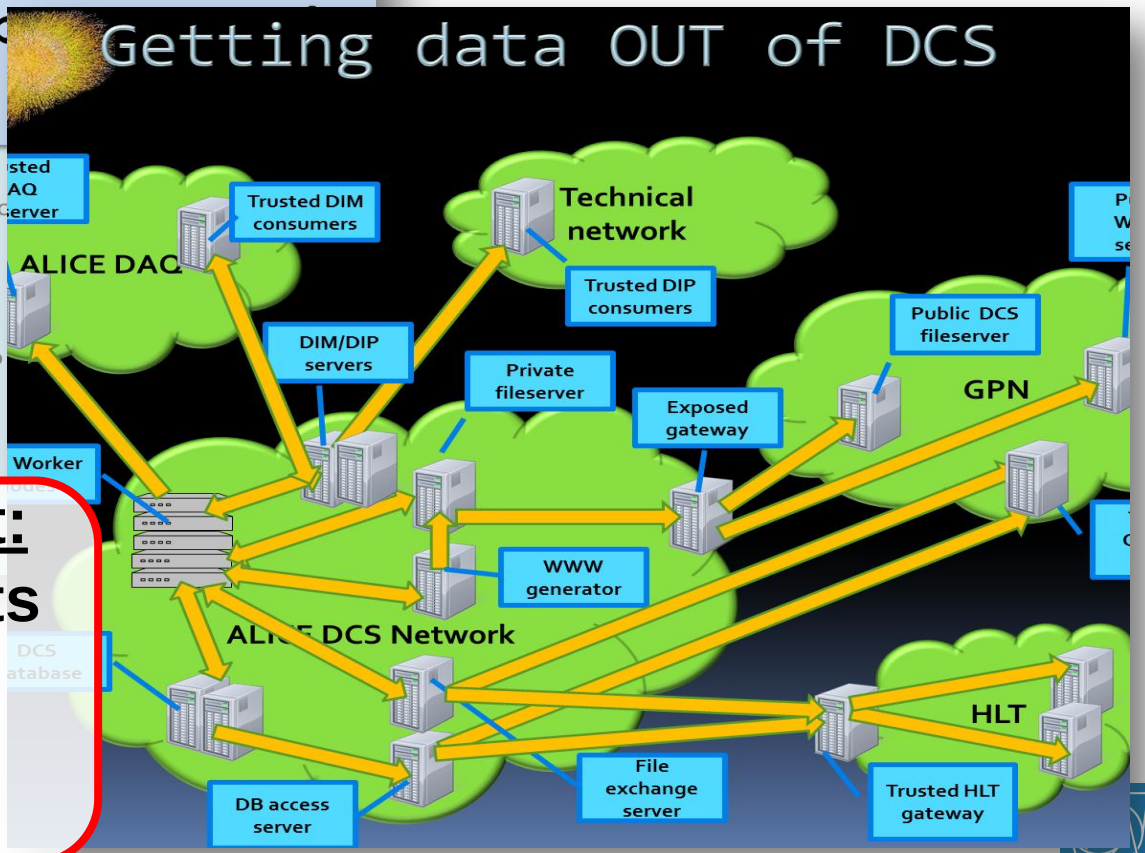
3rd Control System Cyber-Security Workshop, Grenoble

9.10.2011

Timo Hakulinen, Pierre Ninin, Francesco Valsan
GS/ASE, CERN, Geneva

EDMS 1161633

Priorities are different:
Technical requirements + operational needs often collide with security.




…which can be OVERCOME!

Defense-in-Depth:
Network security gives an excellent basis.

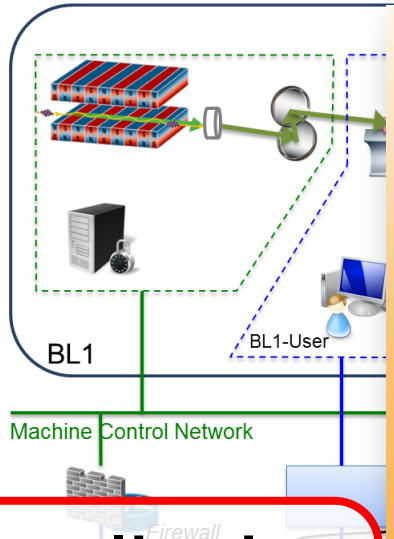
Network Securi

General public and log in services/ Terminal services
- RDP windows remote desktops
- SSH gateways
- NX linux remote desktops
- Web services

Network segmentation and trusted zones
- level of trust based on three tiers the sensitivity of the data being processed

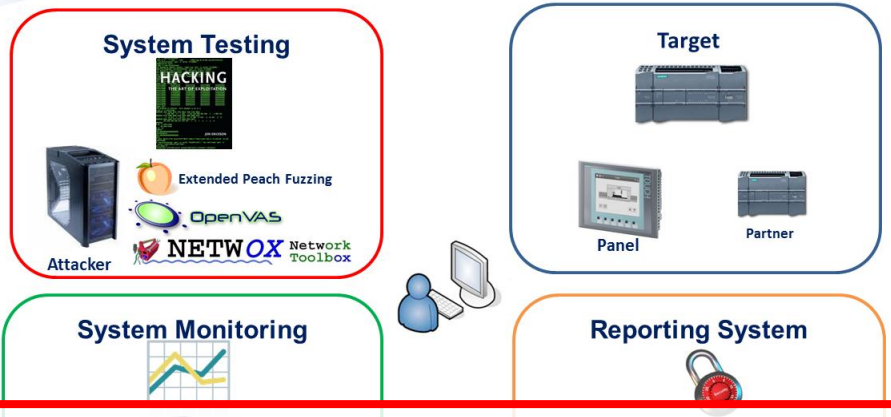
Anomaly & Intrusion detection

Install the Next Generation Firewall (2010 Fall -)



Test-bench diagram

icalepcs 2011



Compartmentalization
of networks reduces cross-infections.

Controls devices are insecure.
Test them, make them fail and send them back to the vendor ☺


Get Started: Two Approaches

Top-Down:

Going for full-blown ISO27000 certification. *Kudos!!*

Argus: Asset and Risk Profiles

#	Risk ID	Threat Scenario	CIA ID	Threat Scenario: Actor	Means	Motive	OC	SR	P
1	RSK-PLC2	Production Safety PLC's logic can be modified by connecting to it over the network	CIA-PSW	Disgruntled	PLC				
2	RSK-PLC1	Production Control System PLC's logic can be modified by connecting to it over the network	CIA-PSW						
3	RSK-DR	Recovering from a disaster almost entirely dependent on external agency with no formal SLA	IAC-FS						
4	RSK-LIC1	Licenses, especially the physical ones, not protected, and can be stolen.	CIA-SWL						
5	RSK-SW1	Documentation for many software not available/complete	CIA-CSD						
6	RSK-IT	Most IT operations are outsourced with no formal SLAs	CIA-COM, IAC						
7	RSK-IP	Some employees have knowledge of SW/HW for which there is no documentation or backup personnel	CIA-IP						
8	RSK-LIC2	Licenses can get destroyed.	CIA-SWL						
9	RSK-PRJ	On-going project data can get destroyed (dependent on external agency with no SLAs)	CIA-PRJ						
10	RSK-DMS	Data can be modified or deleted from DMS	CIA-DMS						
11	RSK-ECV	EPICS PV values can be modified during an experiment	CIA-EC						
12	RSK-PLC4	Some software (PLC, Stepper Motor Controller etc) is not under configuration control	CIA-PSW						
13	RSK-HIC	Solaris server Icarus becomes unusable	CIA-CSW						
14	RSK-STI	Softools IDE is crucial for embedded controllers, and the one-man supplier may go out of business	CIA-CSW						
15	RSK-ECA	Embedded Controllers do not have access	CIA-CSW						
16	RSK-ARC								

Computer Questionnaire

Launch LANDB Window | Display Selected Computer in CCDB Window

TNQ Questionnaire Computer — Cancel | Apply Changes to TNQ Compute

Id	670
Computer Name	cwe-2001-ctfb
LANDB Computers ID	155470
How is the Operating System Loaded?	Over Ethernet
What method is used to patch the Operating System?	SLC Repository – YUM Auto Update, Manual Reboot
Date of Last Installed Operating System Version or Patch	
Select Anti-Virus Software	NONE
How is the anti-virus signature file updated?	Not Applicable
If On-Demand, Enter Date of Last Installed Anti-Virus Signature File	
Is this a Mobile Computer (eg. special unit configured for mobile)?	No
Does this Computer onnect to the network via a Modem?	No
u apply Local Configurations afte Installing the Operating System?	Yes
Are Only the Requi ed Software & Services Installed?	No
Have Vendor efault Passwords been Changed?	Yes
Have Vendor Default Accounts been Changed?	Yes
Do Ex ate Rely Directly n this Computer (eg. not on DIP)?	No
Last Modified By	TLAHEY
Last Modified Date	23-MAR-11

Computer Data from LANDB and Layout/CCDB

Bottom-Up:

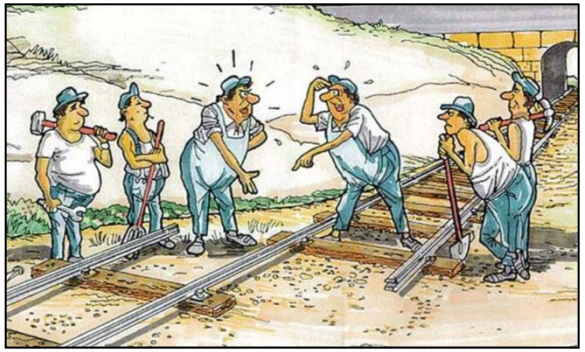
A thorough assessment involving all stakeholders


ONE Take-away

This is a people's problem.

(Still) need for a "Change-of-Mind".

Establish a Security Culture!




Merci beaucoup!!!

Thanks to all participants & esp. to the presenters. Well done, guys!!!

Un merci spécial au comité local d'organisation!