Why (Control System) Cyber-Security sucks…

Summary of the 6th Control System Cyber-Security Workshop

Dr. Stefan Lüders
CERN

with contributions from
Stephen Page (CERN), Alain Buteau & Philippe Pierrot (SOLEIL), Dirk Zimoch (PSI), Denis Paulic (ESS), Sergi Blanch & Sergio Vicente (ALBA), Pascal Oser (CERN), Kevin Brown (BNL), Andrei Sukanov (BNL), Anton Joubert (SKA), Luis Rodriguez Fernandez (CERN), and Karen White (ORNL)

ICALEPCS2017
Barcelona · Spain, October 8-13 · Palau de Congressos de Catalunya

16th International Conference on Accelerator and Large Experimental Physics Control Systems


Ooops, your files have been encrypted!
English
Payment will be raised on
5/15/2017 16:50:06
Time Left
02:23:34:22
Your files will be lost on
5/19/2017 16:50:06
Time Left
06:23:34:22
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
About bitcoin
How to buy bitcoins?
Contact Us
Check Payment
Decrypt

The Why

Karen White (ORNL)

Consequences

- Unauthorized access or actions can be malicious or unintentional
- In either case, the impact can be far reaching
  - Damage to equipment or facility
  - Loss of data
  - Operational downtime
  - Institutional embarrassment, loss of confidence from funding authority or management
  - Disciplinary actions (will someone be fired for this?)

The Consequences

IT security coordination group

Definition

- The *IT security coordination group* at ALBA is a consultancy Inter-section group in the *Computing Division*

Objectives

- Afford cybersecurity from a multidisciplinary point of view
- Avoid collisions among different section interests.
- Propose the measures to be deployed to the section heads in the *Computing Division*

Sergi Blanch & Sergio Vicente (ALBA)

Assign Responsibility

Governance for Software Security

EUROPEAN SPALLATION SOURCE

Denis Paulic (ESS)

- **IEC 61511 : 2016**
  - **Part 1, Clause 8.2.4.**
    - A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS. It shall result in:
      - A description of devices covered by this assessment (SIS, BPCS, any device connected to SIS)
      - A description of identified threats that could exploit vulnerabilities and result in security events
      - A description of potential consequences resulting from security events and likelihood of these events occurring.
      - Consideration of various phases, such as design, implementation, commissioning, operation, and maintenance
      - The determination of requirements for additional risk reduction
      - A description of, or references to information on, the measures taken to reduce the… threats.
- **IEC 61508 : 2010**
  - **Part 1, Clause 7.4.2.3**
    - If the hazard analysis identifies the malevolent or unauthorised action, constituting a security threat,…, then a security threats analysis should be carried out
- **IEC 62443 - Security for Industrial Automation and Control Systems**
- **NIST Special publication 800-82: Guide to Industrial Control Systems (ICS) Security**

NIST = National Institute of Standards and Technology
SIS = Safety Instrumented System

Follow a Standard

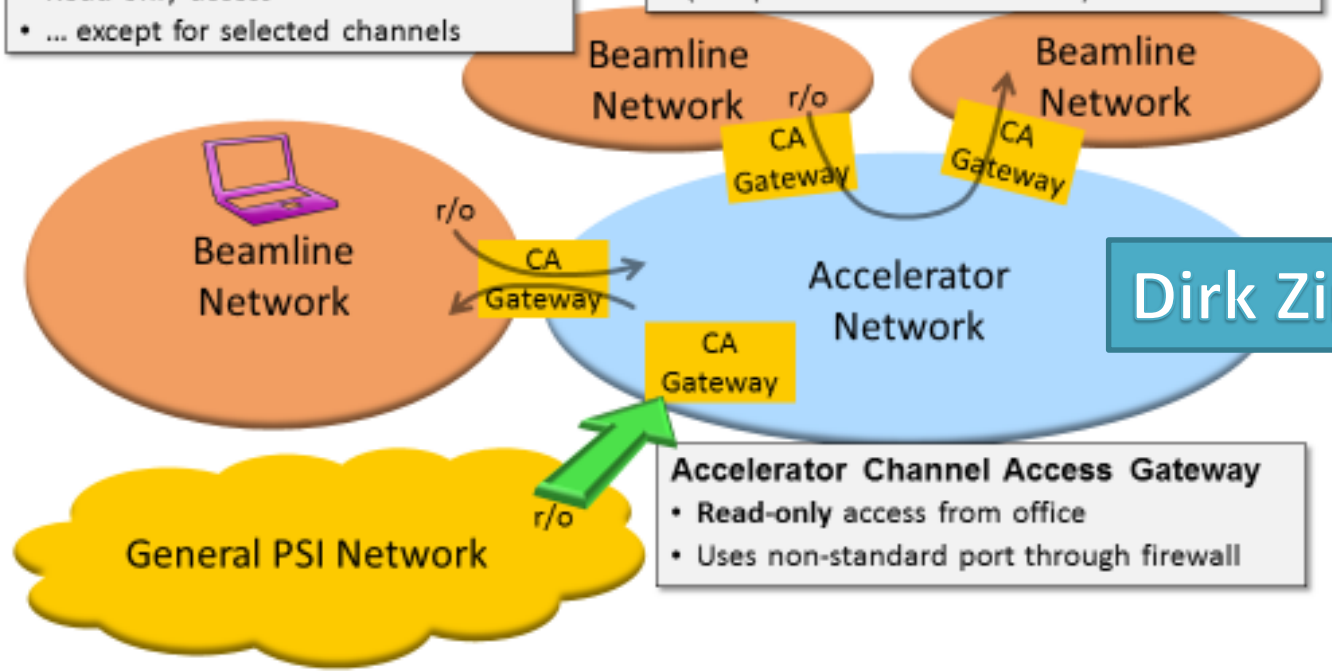
EPICS access

Goals

- Allow **safe** channel Access between beamlines and from office
- Read-only access
- ... except for selected channels

Beamline Channel Access Gateways

- Connect beamlines with accelerator
- Dual network interfaces
- Beamline **writable** from accelerator
- Accelerator **not writable** from beamline (except for selected channels)



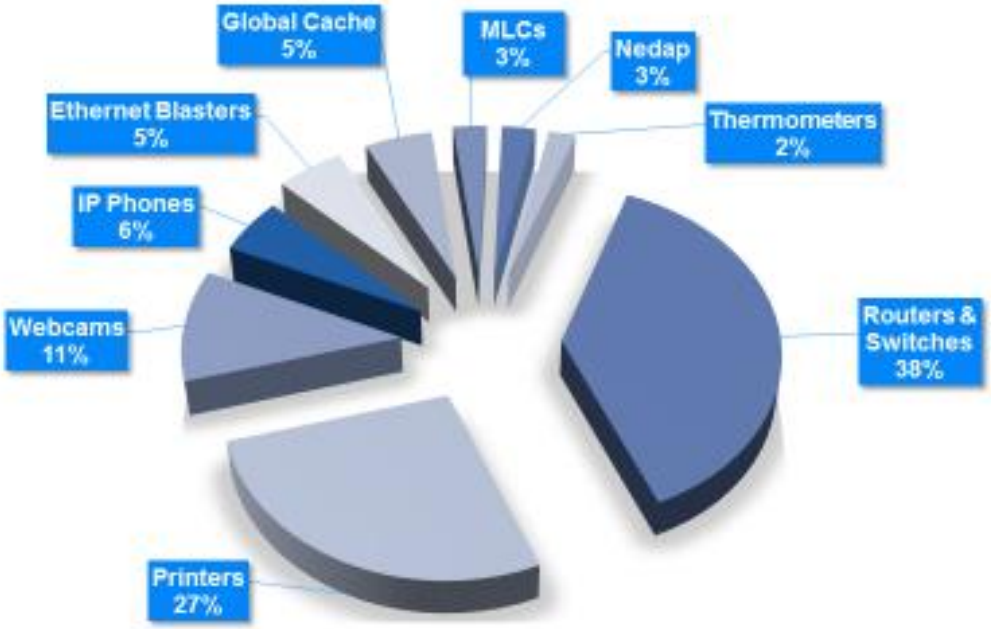
Accelerator Channel Access Gateway

- **Read-only** access from office
- Uses non-standard port through firewall

Dirk Zimoch (PSI)

Control the Network

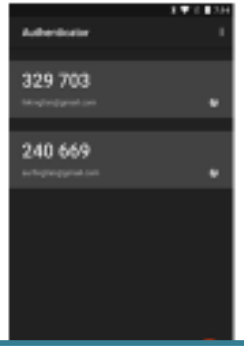
Distribution of IoT at CERN



Pascal Oser (CERN)

Two-factor authentication

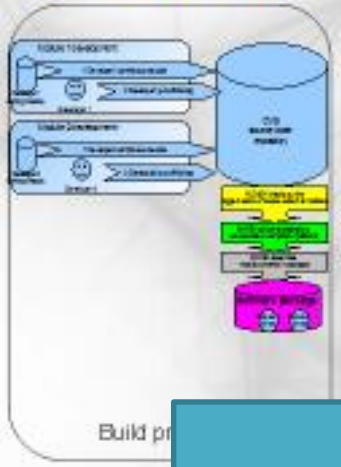
- Both the user's password and a physical second factor would be needed for access.
- The second factor can be a USB key, smartphone application (e.g. Google Authenticator) or SMS with a one-time password.
- Prevents access if a password is compromised.
- To be integrated into central account management and applied to SSH, web (Single Sign-On) and Windows remote desktop.
- Should be applied on the bastion hosts and required when passing over the perimeter of the accelerator network.



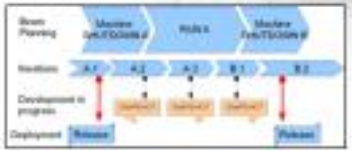
Stephen Page (CERN)

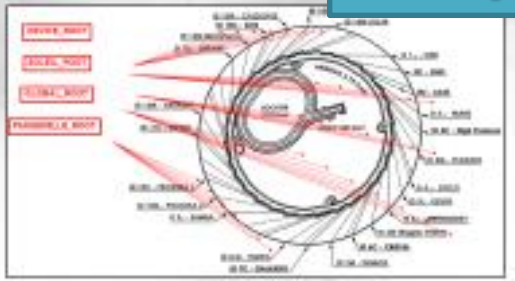
Software Development Cycle for Controls

- **Continuous Integration orchestrates binaries production**
  - "All binaries must be constructed from source code independently of the development environment"
  - Source code is stored in various repositories : CVS, SVN, GIT
  - Some repos are outside SOLEIL (GitHUB, SourceForge)
  - Other are inside SOLEIL (SVN,CVS)
- **Software applications are regrouped in so called "packages"**
  - Each package regroups a coherent set of software components delivering a "high level service"



- **"Continuous delivery" is done during "SOLEIL shutdowns"**
  - Official releases of all software packages are installed on the accelerators and all the beamlines **without any exceptions**





Alain Buteau &
Philippe Pierrot (SOLEIL)

Control Deployment

A big "GRÀCIES & GRACIAS" to the presenters, the participants and the conference program committee & staff!

09:00	**Logistics of the 6th Control System Cyber-Security Workshop** *Palau de Congressos de Catalunya*	*Dr. Stefan Lueders* 09:00 - 09:05
	Why Control System Cyber-Security Sucks *Palau de Congressos de Catalunya*	*Dr. Stefan Lueders* 09:05 - 09:20
	The Trickle Down Effect: Protecting SCADA systems at the high energy physics lab, SLAC, by minimizing human error through phishing training policy and best practices	*Ashley Tolbert*
	Control system network security issues and recommendations *Palau de Congressos de Catalunya*	*Stephen Page* 09:45 - 10:10
10:00	**Control-system cyber security practices at SOLEIL**	*Alain Buteau* 10:10 - 10:35
	Palau de Congressos de Catalunya	10:35 - 11:00
	Accelerator network safety at PSI *Palau de Congressos de Catalunya*	*Dirk Timoch* 11:00 - 11:20
	Secure PSS software development *Palau de Congressos de Catalunya*	*Denis Kolic* 11:20 - 11:45
	Building Institution Security Appliances	*Sergi Blanch-Torné et al.*
	Palau de Congressos de Catalunya	11:45 - 12:00
	Internet of Things: Control Networks *Palau de Congressos de Catalunya*	*Pascal Oser* 12:10 - 12:35
	Secure and/or cyber espionage	*Kevin Brown*
	Palau de Congressos de Catalunya	
	Lunch Break	
	Access Security of Control System *Palau de Congressos de Catalunya*	*Andrei Sukhanov* 14:00 - 14:30
	Secrets management in a control system environment using Vault *Palau de Congressos de Catalunya*	*Anton Joubert.* 14:30 - 15:00
15:00	**1000 things you always want to know about SSO but you never dared to ask!** *Palau de Congressos de Catalunya*	*Luis Rodriguez Fernandez* 15:00 - 15:30
	Coffee Break *Palau de Congressos de Catalunya*	15:30 - 16:00
16:00	**Discussion on AuthN & AuthZ** *Palau de Congressos de Catalunya*	*Karen White* 16:00 - 16:45
	General Discussion *Palau de Congressos de Catalunya*	*Dr. Stefan Lueders* 16:45 - 17:30
17:00		

https://indico.cern.ch/event/616635/

50+ participants (new record!!)

Ten in-depth presentations & three awesome panel discussion session