



DIY.DESPAIR.COM

Why (Control System) Cyber-Security sucks...



Why (Control System) Cyber-Security sucks...
Dr. Stefan.Lueders@cern.ch
CS2HEP, October 8th 2017, Barcelona (E)



**New kids on the block:
How to patch IoTs
(RasPI, Arduino, ...)?**

How to involve/force vendors?

...and how to counter their fantasy pricing?

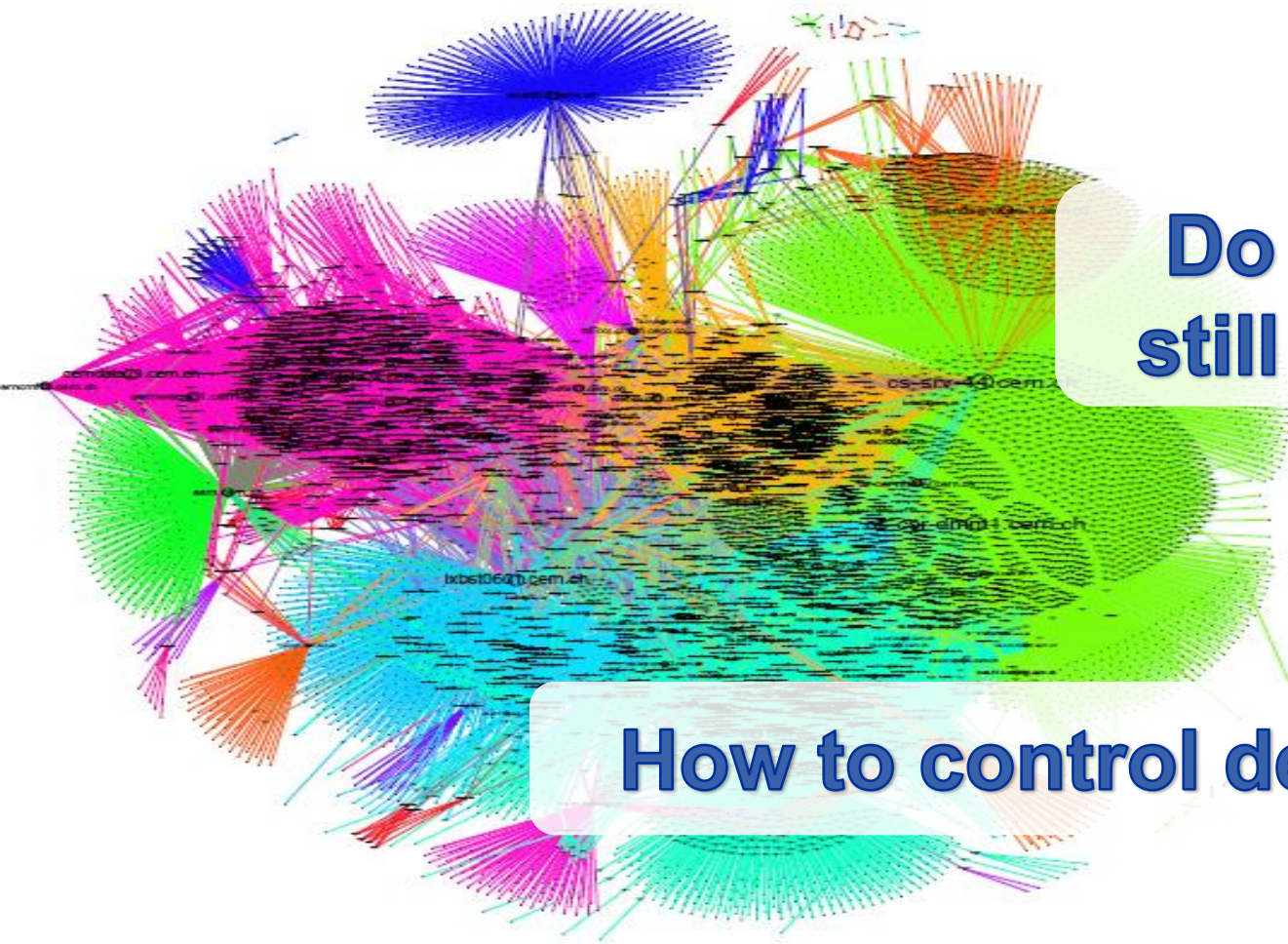


**Dealing with USB ports is
already problematic...**



**... but embedded WLAN
is becoming a pain!**





**Do network cells
still make sense?**

How to control dependencies?





Where/How to manage common services: SSO, AD/LDAP, versioning, storage, DB, ...?

A new axis of complexity: virtualization & containers, IPMI/BMC, HV, VM, image provisioning...



Why (Control System) Cyber-Security sucks...

Dr. Stefan.Lueders@cern.ch

CS2HEP, October 8th 2017, Barcelona (E)

Computer Centre Segregation



How to split development & initial testing, final testing & roll-out, and operations?



What if we're forced to use Cloud Services (e.g. Github, Office 365)?



How to import external software libraries (e.g. PyPi)?







CERN Single Sign-On

Multi-Factor Authentication requested

Sign in with second factor verification

Reminder: you have agreed to comply with the [CERN computing rules](#)

Select your Multi Factor system

-  **SMS**
Two factor authentication asking your CERN credentials, and a verification code will be sent by SMS to your CERN mobile phone.
-  **Google Authenticator**
Two factor authentication asking your CERN credentials, and a verification code using Google Authenticator Smartphone application.
-  **Yubikey**
Two factor authentication asking your CERN credentials, and a verification code using your USB YubiKey device.
-  **Smartcards**
Two factor authentication using your CERN Access Card Smartcard chip.

Remember my choice and skip this screen next time

Next

Where (What!) is an
2FA (open source) solution
for Win, SSO/web & LX?



Why (Control System) Cyber-Security sucks...

Dr. Stefan.Lueders@cern.ch

CS2HEP, October 8th 2017, Barcelona (E)

AuthN & AuthZ



**Why do BSc/MSc students,
computing engineers,
control system engineers,
come w/o security knowledge?**



**Exposure
Threats**

**Complexity
Vulnerabilities**

**Dependencies
Consequences**



**Why (Control System)
Cyber-Security sucks...**



09:00	Logistics of the 6th Control System Cyber-Security Workshop <i>Palau de Congressos de Catalunya</i>	<i>Dr. Stefan Lueders</i> 09:00 - 09:05	
	Why Control System Cyber-Security Sucks <i>Palau de Congressos de Catalunya</i>	<i>Dr. Stefan Lueders</i> 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	<i>Ashley Tolbert</i>	
10:00	Control system network security issues and recommendations <i>Palau de Congressos de Catalunya</i>	14:00	
	Control-system cyber-security operational practices at SOLEIL <i>Palau de Congressos de Catalunya</i>		
	Coffee Break <i>Palau de Congressos de Catalunya</i>	15:00	
11:00	Accelerator network safety at PSI <i>Palau de Congressos de Catalunya</i>		
	Security measures for ESS PSS software development <i>Palau de Congressos de Catalunya</i>		
12:00	Rethinking Institution Security Approach <i>Palau de Congressos de Catalunya</i>	16:00	
	Internet of Things on Accelerator Control Networks <i>Palau de Congressos de Catalunya</i>		
	Dealing with insecure and/or cyber espionage enabled COTS devices <i>Palau de Congressos de Catalunya</i>	17:00	
13:00	Lunch Break		
		Access Security of RHIC Control System <i>Palau de Congressos de Catalunya</i>	<i>Andrei Sukhanov</i> 14:00 - 14:30
		Secrets management in a control system environment using Vault <i>Palau de Congressos de Catalunya</i>	<i>Anton Joubert.</i> 14:30 - 15:00
		1000 things you always want to know about SSO but you never dared to ask! <i>Palau de Congressos de Catalunya</i>	<i>Luis Rodriguez Fernandez</i> 15:00 - 15:30
		Coffee Break <i>Palau de Congressos de Catalunya</i>	15:30 - 16:00
		Discussion on AuthN & AuthZ <i>Palau de Congressos de Catalunya</i>	<i>Karen White</i> 16:00 - 16:45
		General Discussion <i>Palau de Congressos de Catalunya</i>	<i>Dr. Stefan Lueders</i> 16:45 - 17:30



Bye, Bill. Welcome RasPI & Arduino

Core-ICS apart, interconnections will grow

ICS and IoT will merge in some way

Wireless is already on the plant-floor

Internet & cloud access will become normal

Incentives for secure ICS lacks business case

