WAVESTONE

DYODE: Do Your Own DiodE

A DIY, low-cost data diode for ICS

BruCon, October 2017
Arnaud Soullié

Who are we?

Arnaud

@arnaudsoullie

/ Pentest & research
/ Interests
  / Windows Active Directory
  / ICS security
  / Wine tasting / Motorbike riding
    (we're not going to talk about it today)
/ Talks & workshops
  / BlackHat Europe 2014
  / Hack In Paris 2015
  / BruCon 0x07
  / BSides Las Vegas 2015 / 2016
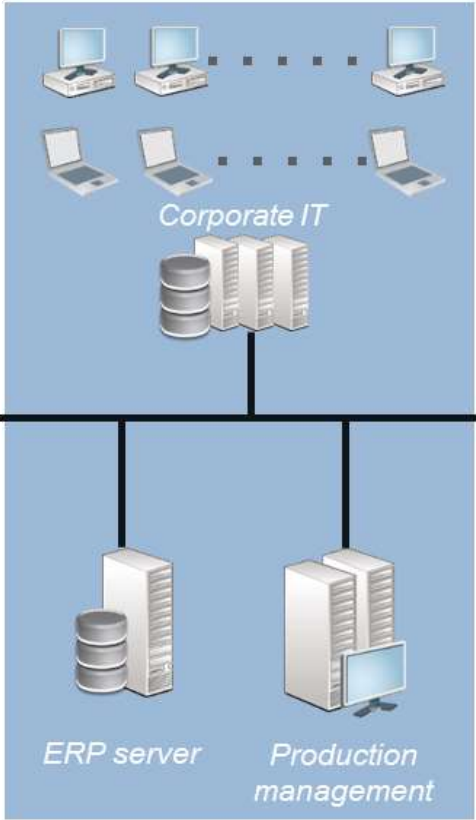 / DEFCON 24 / 25 (ICS VILLAGE)

Manager @ **WAVESTONE**

Ary

/ Advisory & audit (used to do pentests)
/ Interests
  / Windows Security
  / Cryptophony

/ Talks: IEEE ICC 2009, JSSI 2013 and 2014, SSTIC 2016, Bsides Las Vegas 2016

/ Book Information Security, Eyrolles Edition [in French] – written with several authors including Arnaud
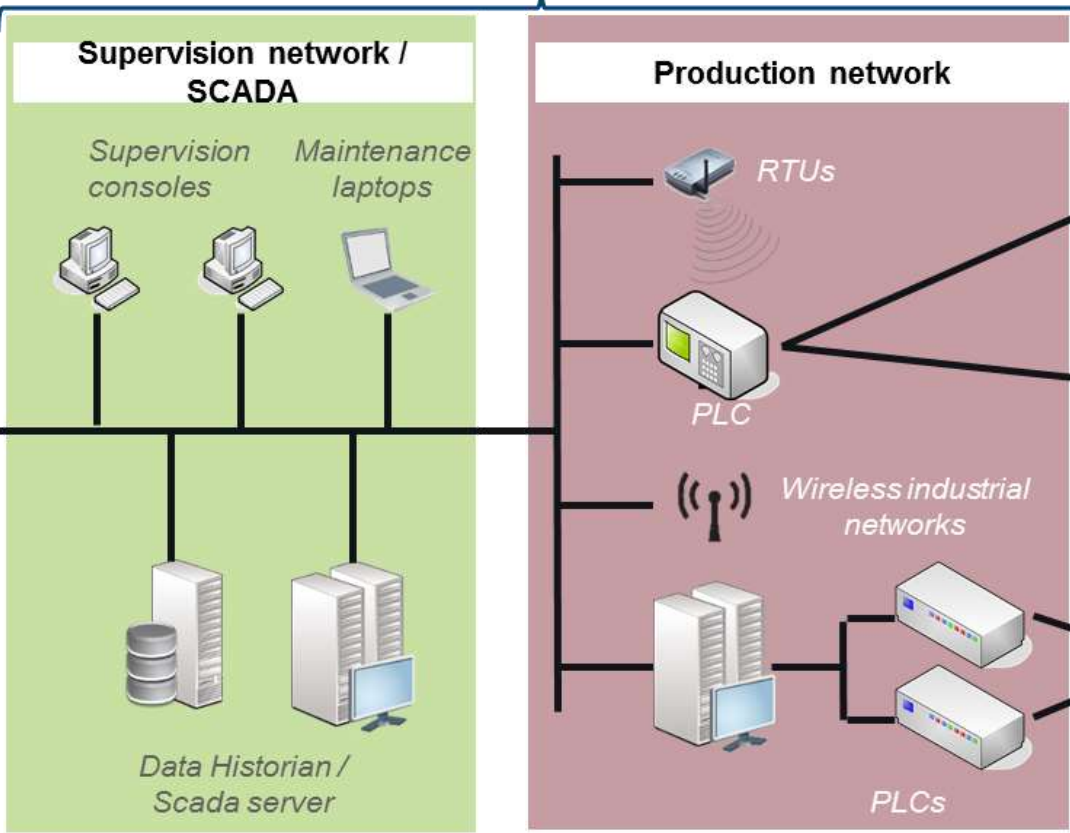
Tax exile @ $Big4 in Switzerland ;)

ICS 101

DATA DIODES 101

/ AKA "one-way gateway"

/ Use of light as the transport medium

/ PN junction prevents electrons from going backwards

➔ Security property is backed by physics. *Hack that.*

COMMERCIAL DATA DIODES

WHY THIS PROJECT ?

/   Feedback from lots of ICS security assignments

➔ *There are lots of needs for exchanging information between CORP and ICS*

/   Commercial data diodes exist, but are quite expensive

➔ *Security / cost trade-off , not easy to sell*

/   Examples

Predictive maintenance : send a 100kb file every 6 hours to a 3rd party

Cooling units : 3rd party needs to access a PLCs output in real-time for efficiency improvement

➔ *Data only needs to be exchanged one-way, but in these examples the high cost of a commercial Data Diode combined with business needs to exchange information, resulted in uncontrolled network connection between two networks*

DYODE PROJECT

/ Based on existing work : Lagadec, Austin Scott, Robert Gabriel

/ Low cost & DIY

Use of standard hardware (COTS) and open-source software

Target cost of 200$ per unit

/ Objectives

Proof of Concept

Transparent, easy to deploy solution

Share the results

DYODE project has no commercial intent, but an implementation by a vendor is authorized
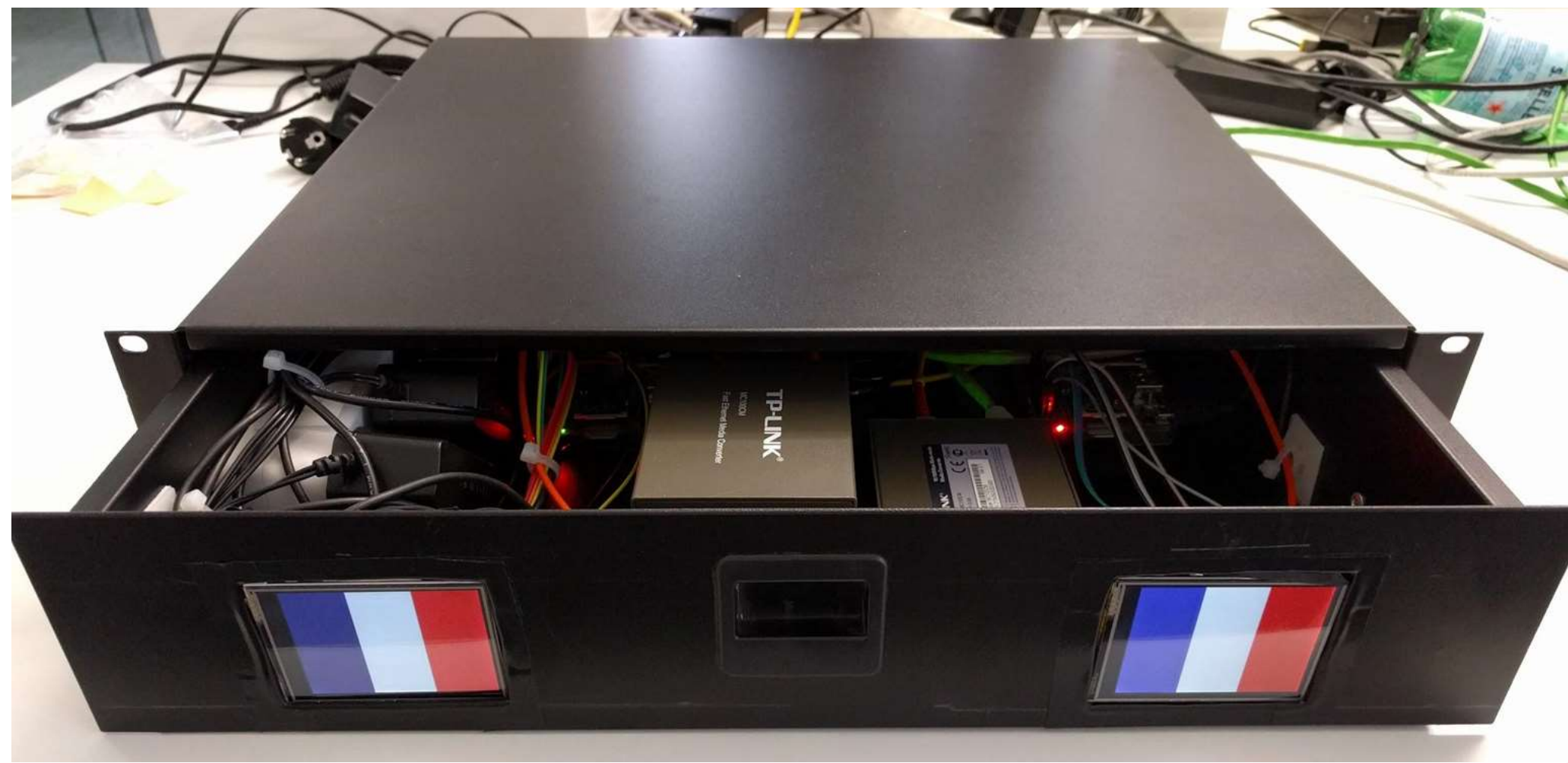
HARDWARE

/ Use of copper-optical converters

/ Use of a 3rd converter to fake a signal on the second (link failure protection)

/ Raspberry Pis used for the "in" and "out" counters

DYODE

ICS

CORP

— **Copper Ethernet**

— **Optical**
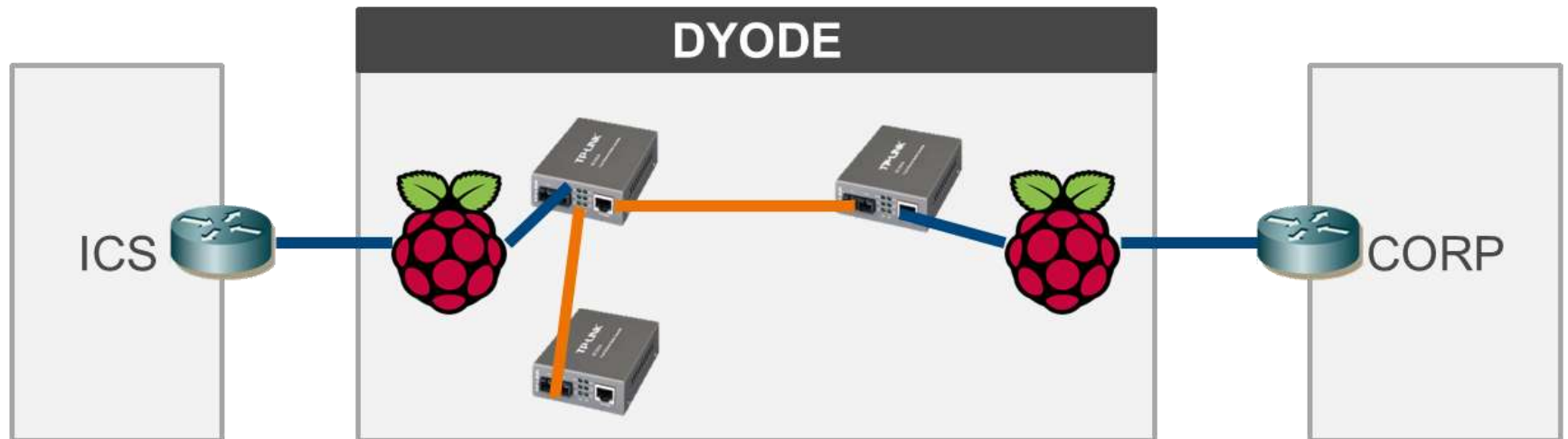
HARDWARE

HARDWARE

SOFTWARE

Improve

Develop

Prototype

Latency improvement
Replace *udpcast* by a custom, naïve Python UDP socket implementation

Develop features
Development of data diode features on top of *udpcast* using Python
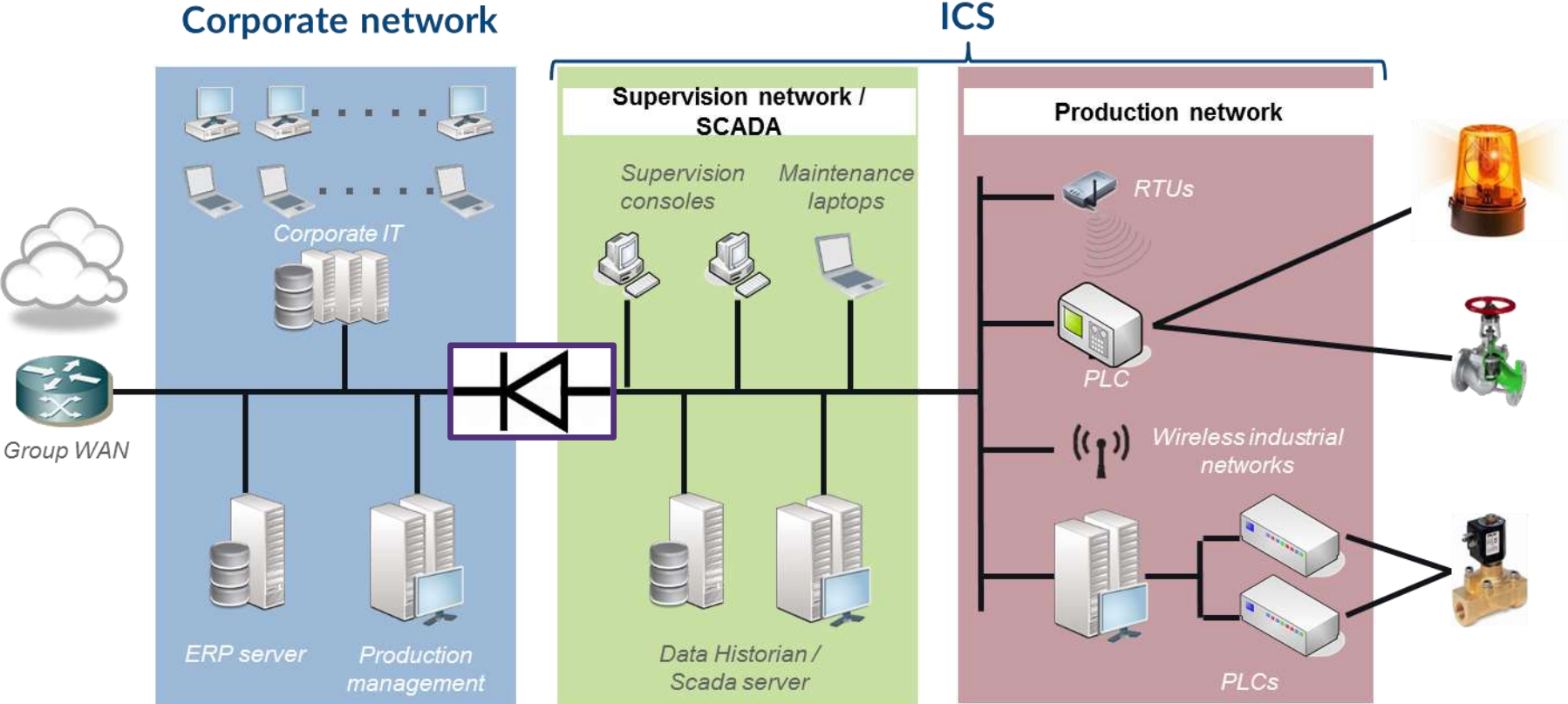
/ File transfer

/ Modbus

/ Screen sharing

Quickly prototype
Use of *udpcast*, an open-source software that allows unidirectional file transfer

DEMO

[VIDEO] DEMO TIME!

DEMO

PC Industriel

PC bureautique

SSTIC - DYODE - IN [En fonction] - Oracle VM VirtualBox

Fichier   Mach...   ...   Entr...   Périph'iques   Aide

Recycle Bin

Rick Astley -
Never Gonna
Give You Up

ModbusPal

screen_share

Host Name: IE10WIN7
IE Version: 10.0.9200.17148
OS Version: Windows 7
Service Pack: Service Pack 1
User Name: IEUser
Password: Passw0rd!

Snapshot/backup:
Create a snapshot (or keep a backup of downloaded archiv
this VM, so that you can reset quickly after the OS t

Licensing notes and evaluation period:
The modern.ie virtual machines use evaluation versions of N
limited. You can find a link to the full license on the

Activation:
For Windows 7, 8, and 8.1 virtual machines, you need to co
trial. In most cases, activation will be done automat
enter "*slmgr /ato*" from an administrative comman
For Windows Vista, you have 30 days after first boot.
For Windows XP, you have 30 days after first boot. You will
minutes after boot stating the days left (in the syste

Re-arm:
In some cases (Windows XP, Vista, and 7), it may be possib
there are rearms left. The following commands can
prompt (**right-click** on **Command Prompt** and sel

FR   6:22 AM
                            5/30/2016

CTRL DROITE

Kali2 Solucom 2016-01 [En fonction] - Oracle VM VirtualBox

Fichier   ...   ...   Écra...   Entrée   Périphériques   Ai...

Appli...ation...:enu...   5:22

out on dyodeout - File Manager

File   Edit   View   Go   Help

smb://dyodeout/out/

Warning, you are using the root account, you may harm your system.

Name   Size

DEVICES

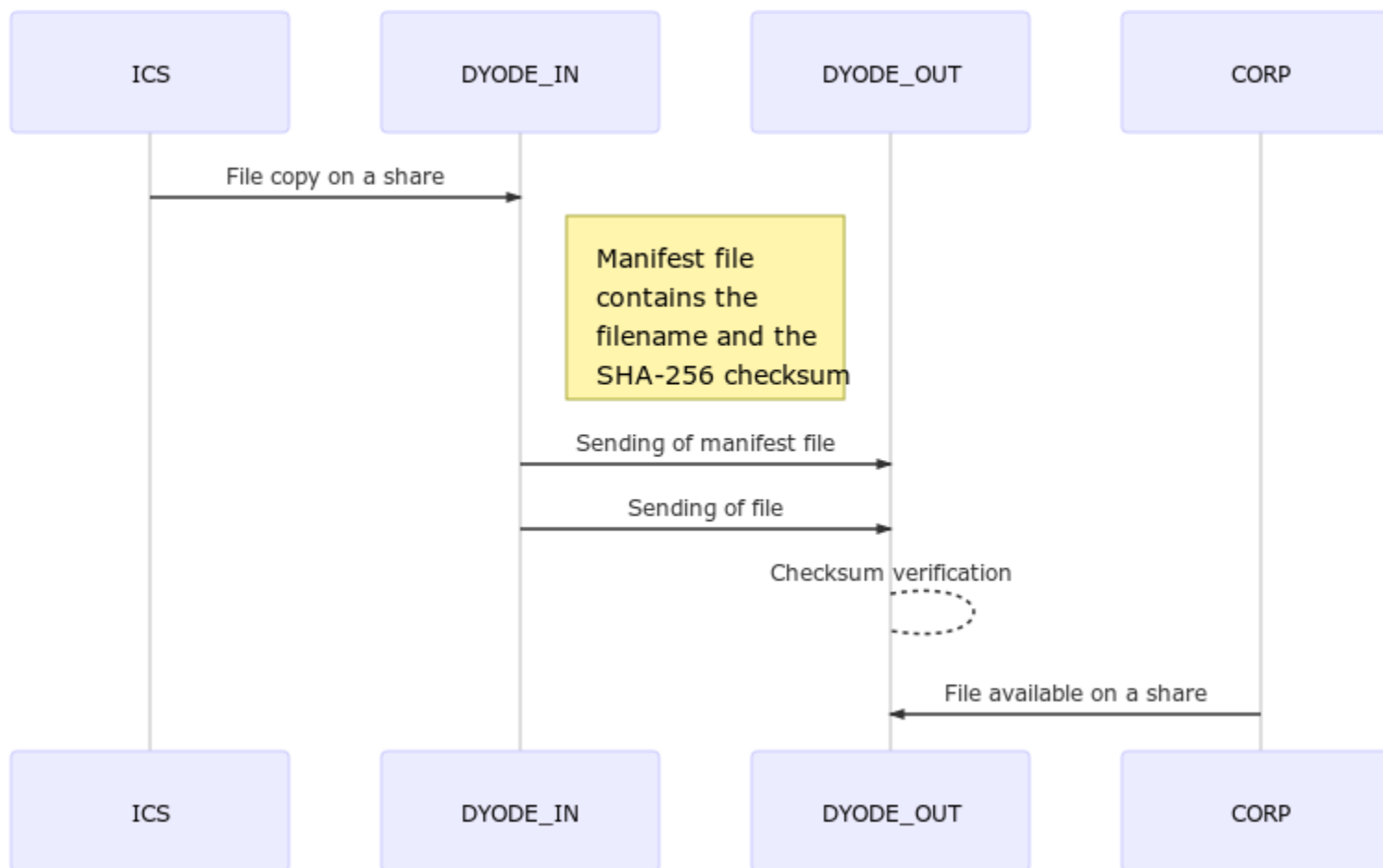File Syst...

PLACES

root

Desktop

Trash

NET   Trash is empty

Browse ...

/out/ ...

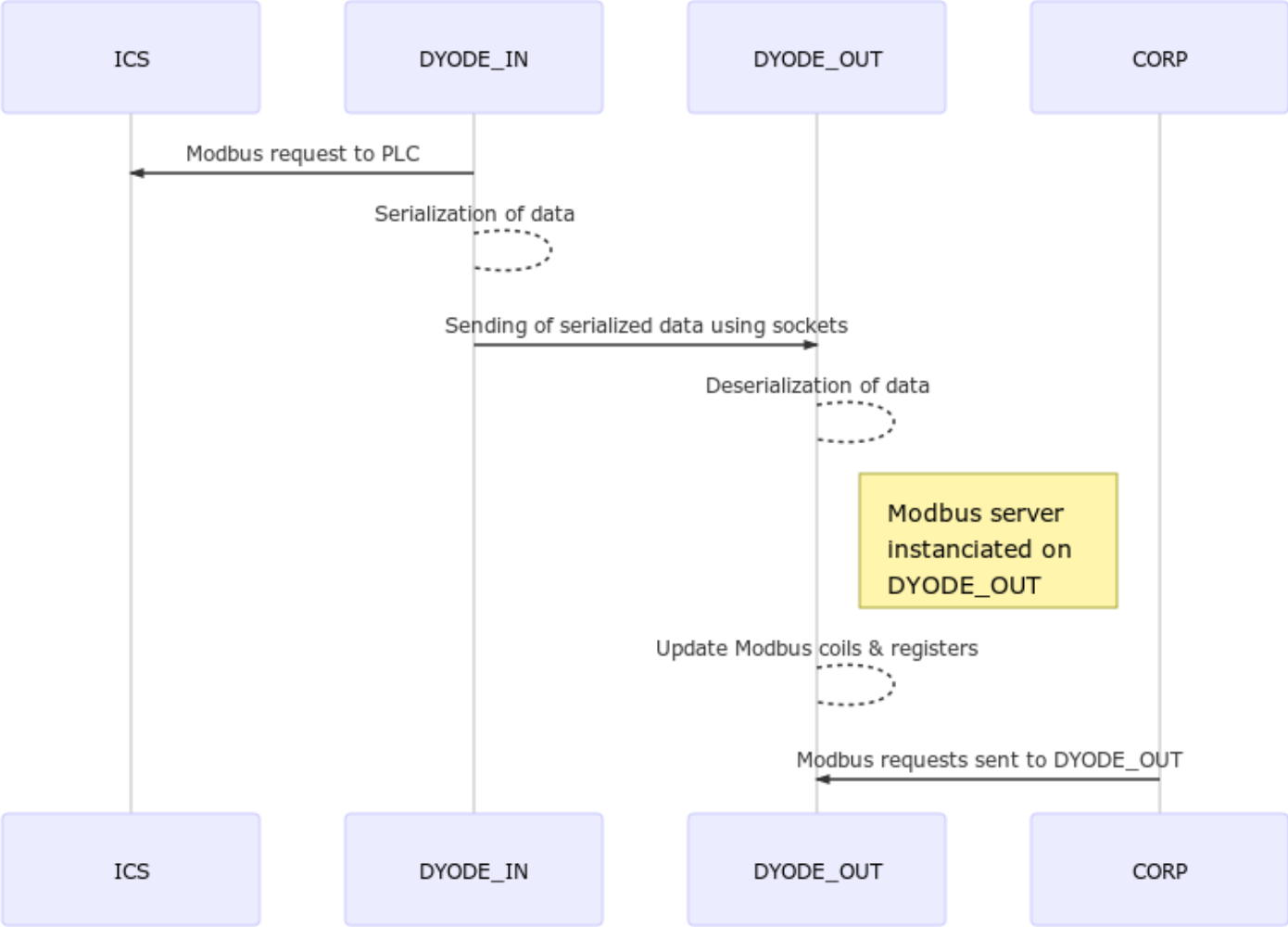0 items, Free space: 11.6 GB

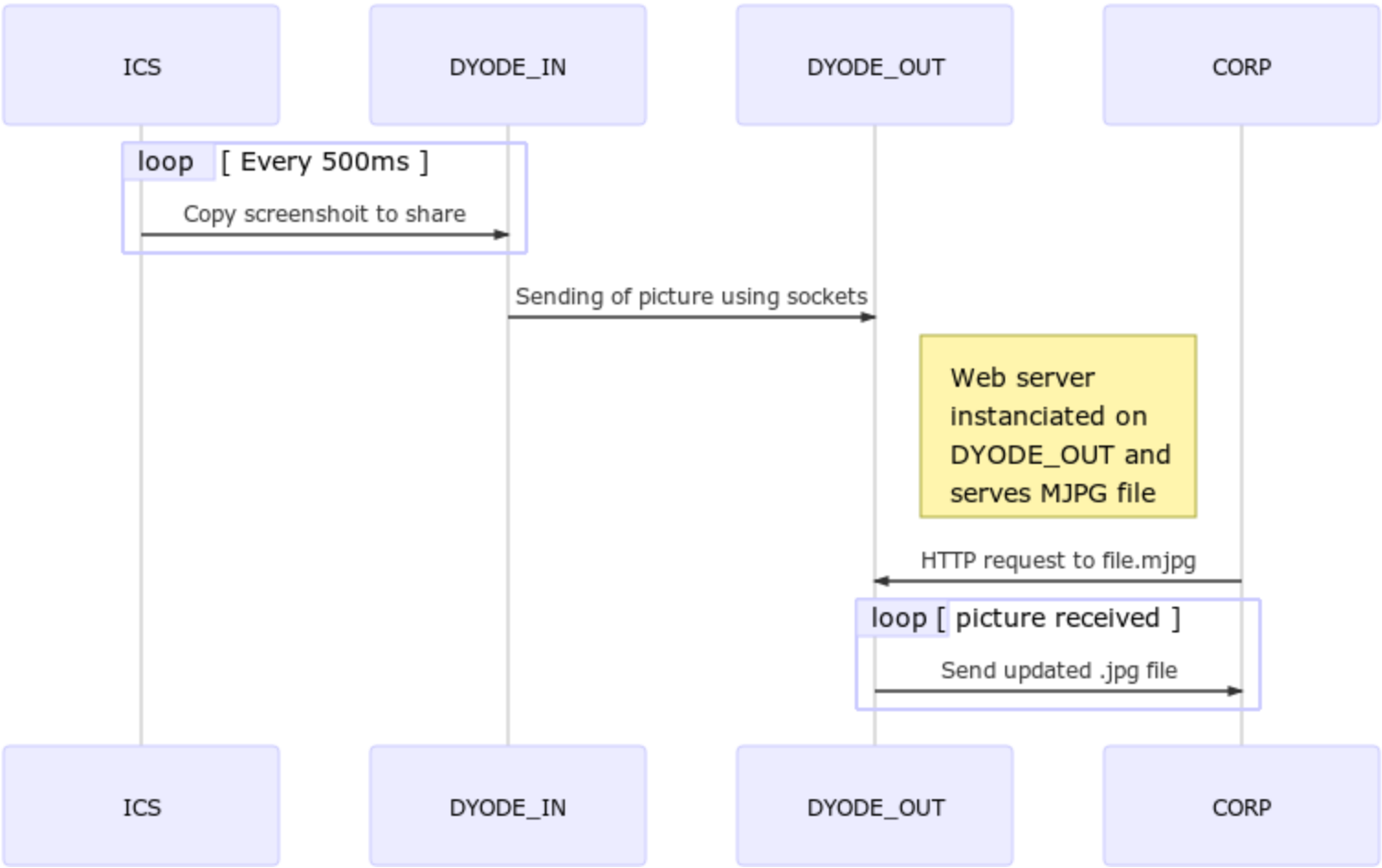CTRL DROITE

FILE TRANSFER WORKFLOW

MODBUS TRANSFER WORKFLOW

SCREEN SHARING WORKFLOW

CONFIGURATION FILE

```
config_name: "Dyode test"
config_version : 1.0
config_date: 2016-05-04

dyode_in:
  ip: 10.0.1.1
  mac: b8:27:eb:89:1e:f3
dyode_out:
  ip: 10.0.1.2
  mac: b8:27:eb:b1:ff:ab

modules:
  "File share 1":
    type: folder
    port: 9600
    in: /home/pi/in
    out: /home/pi/out
```

```
"Modbus PLC":
    type: Modbus
    port: 9400
    ip: 192.168.1.150
    port_out: 502
    registers:
      - 0-100
      - 400-450
    coils:
      - 0-10
      - 100-110
  "Screen_share_1":
    type: screen
    port: 9900
    in: /home/pi/screenz
    out: /home/pi/screenz
```

REAL COST

Component	Quantity	Cost
Raspberry Pi + power supply	2	92€
Copper-Optical converter	3	117€
Optical cable	2	15€
USB-Ethernet adapter	4	16€
Rack 19" 2U	1	59€
Screens	2	70€
Buzzer	1	5€
GRAND TOTAL		**374€**

The more the better
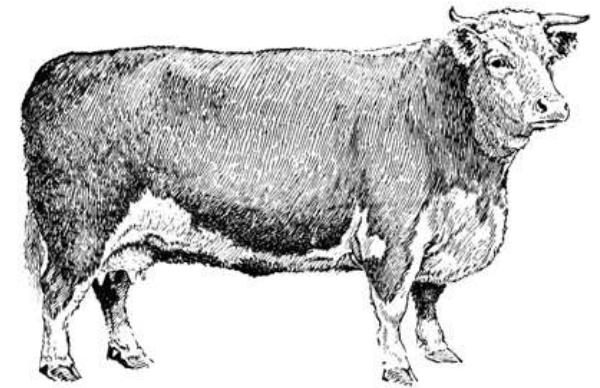
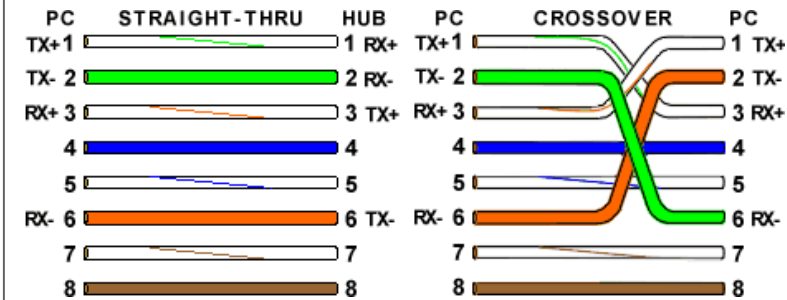Properly stacking security appliances

Just like LEGO blocks

O RLY? A Rich CISO

WHY NOT JUST CUT THE CABLE?

Cutting the cable?

/ Yes, it is possible to have a one-way gateway by using half-duplex mode on network interfaces and cutting the 2 RX of the Ethernet cable

/ Seems simpler than the DYODE implementation

However

/ You'll still need the "in" and "out" counters (Raspi) to use a one-way connection for TCP protocols

/ In theory, advanced attacks may allow to send information the other way around, for example by switching ports "up" and "down"

IMPROVEMENTS > Reducing the cost

Most expensive components : in/out counters & optical converters
➔ *Let's change that !*
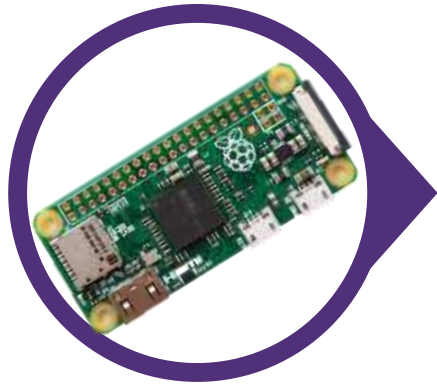
Replace classical RSPi by RSPi 0 (5$)

(When you can find one...)
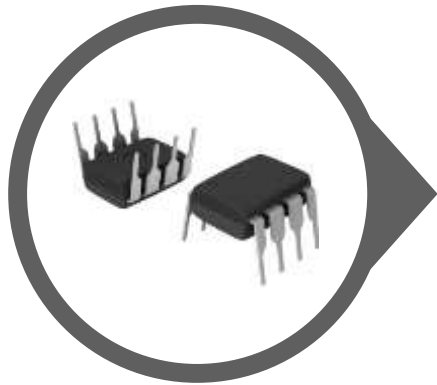
Replace the Ethernet-FO converters by a serial connection with an optocoupler also called photocoupler

/ Diode opto-isolator = LED + photodiode

/ Very low cost solution (2€)

/ Acceptable bandwidth for some usages (20ko/s)

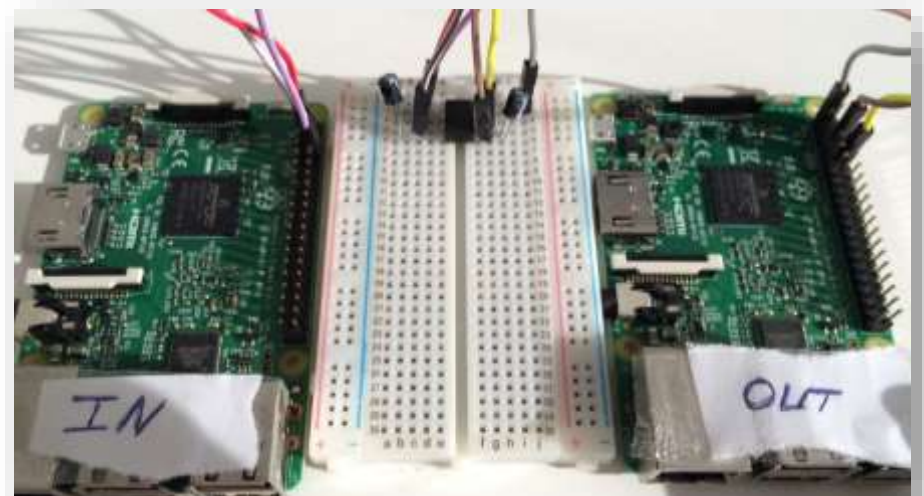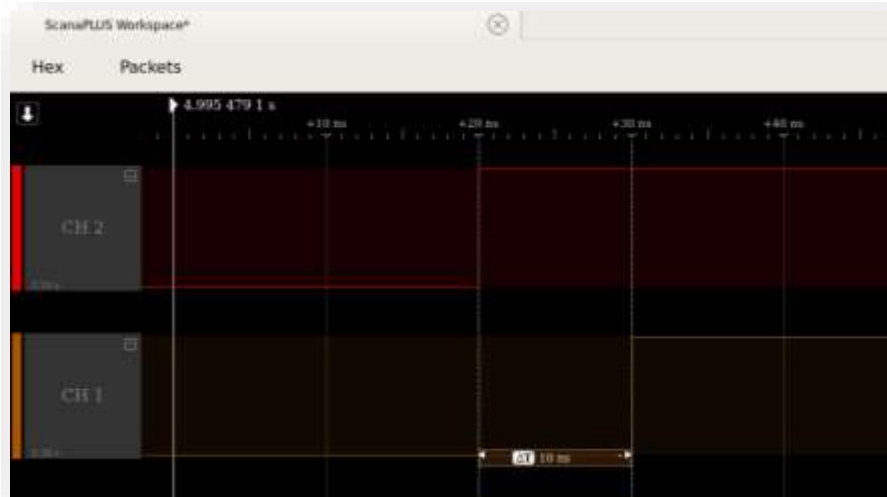/ For very sensitive environments, do your own

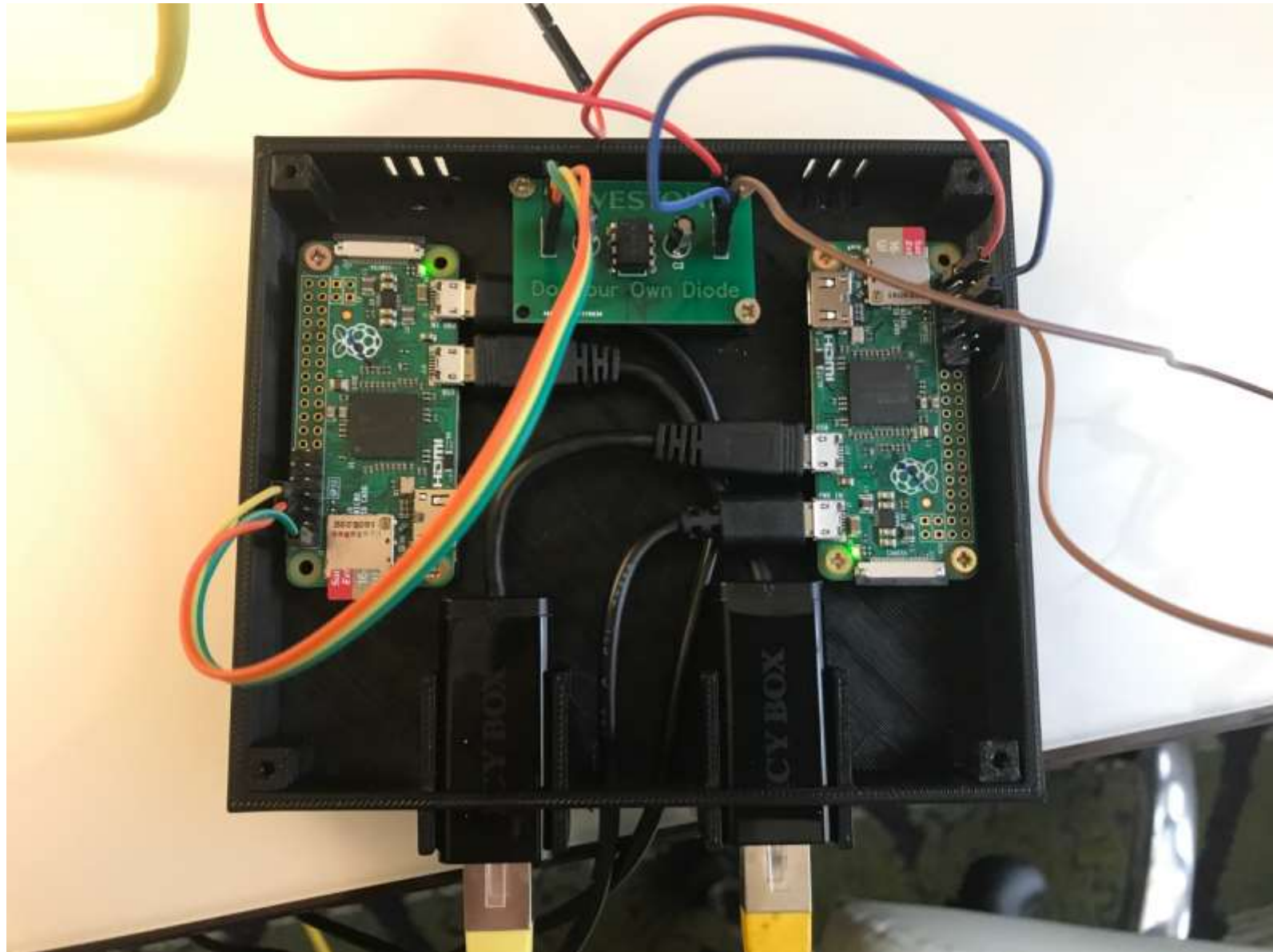(it is harder to backdoor a LED than a black box circuit in epoxy)
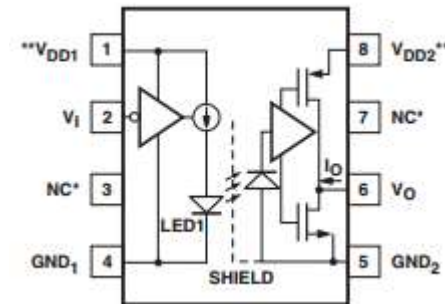
DYODE Ultra-low cost version

Component	Quantity	Cost
Raspberry Pi 0 + power supply + SD Card	2	32€
Optocoupler+capacitor+misc.	1	5€
MicroUSB-Ethernet adapter	2	30€
DIN Rail compatible box	1	12€
GRAND TOTAL		**80€**

DYODE v2 final prototype

Hardware is open source as well !
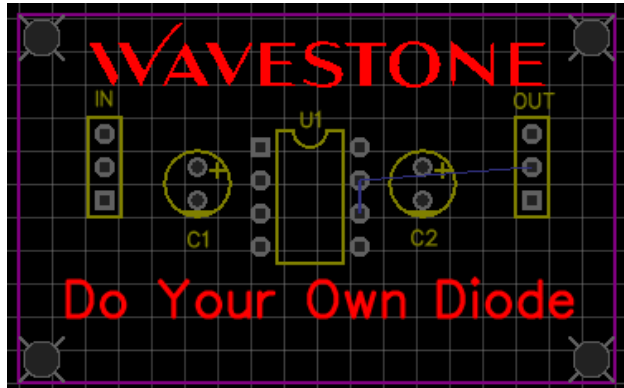

```
*PADS-PCB*
*PART*
U1 DIP--8
IN HDR-3X1/2.54
[…]
C2 CAP-D5.0XF2.0

*NET*
*SIGNAL* U1_2
IN.2 U1.2
[…]
*END*
```
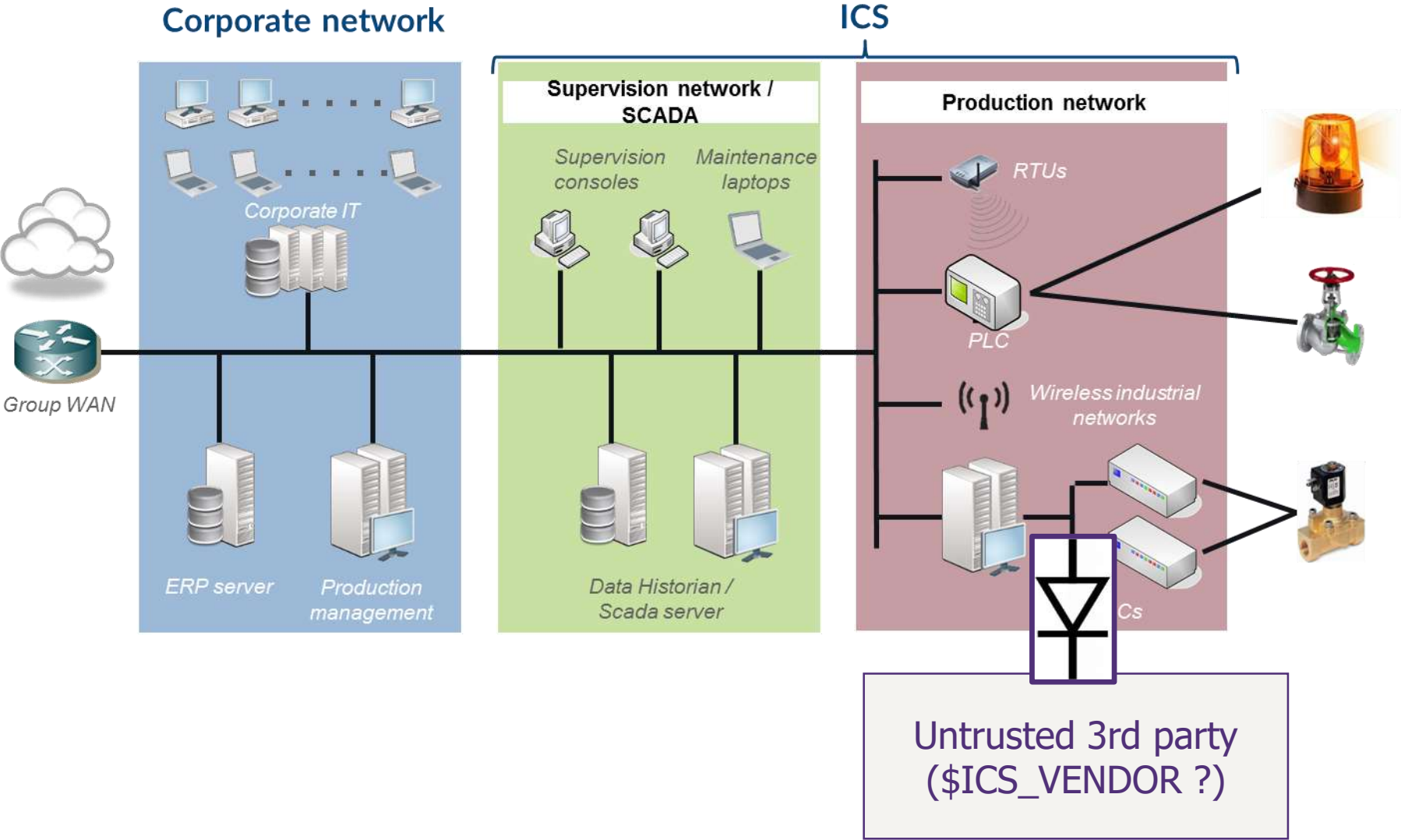
Netlist
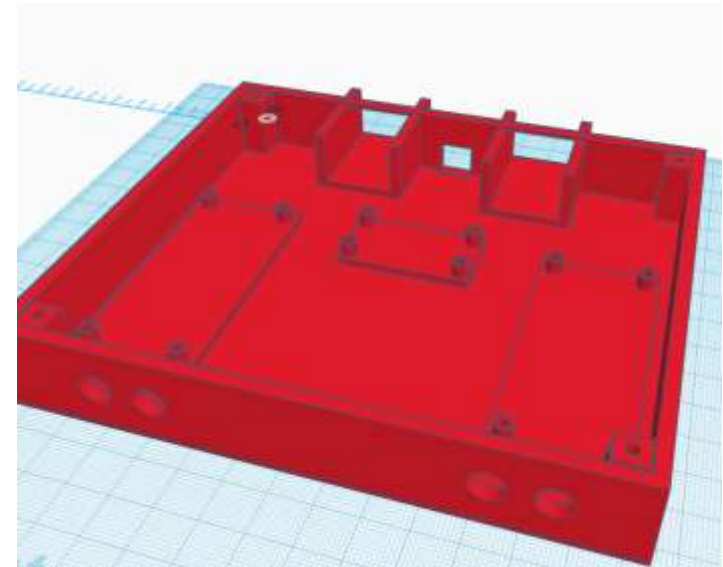

```
solid stl_item0  facet
normal 0 0 1    outer loop
vertex -56.25 23.799 9
vertex -56.5 24.232 9
vertex -56.561 23.561 9
endloop  endfacet  facet
normal 0 0 1    outer loop
vertex -55.112 21.051 9
vertex -54.982 20.568 9
[…]
```

STL file for 3D-printing the case

DEMO

[LIVE] DEMO TIME!

DEMO

Corporate network

ICS

Supervision network / SCADA

Production network

Supervision consoles   Maintenance laptops

Corporate IT

RTUs

PLC

Group WAN

Wireless industrial networks

ERP server   Production management

Data Historian / Scada server

Cs

Untrusted 3rd party ($ICS_VENDOR ?)
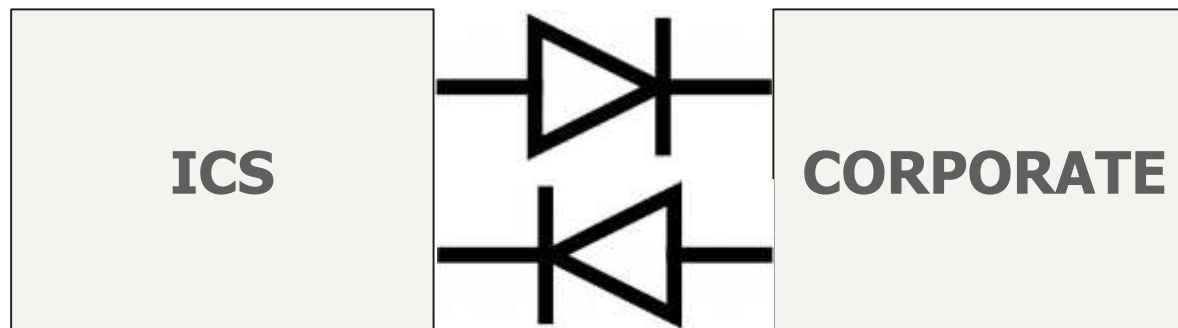
SO, IS IT MAGICAL ?

/ Nope.

/ Most of the time, need to exchange data two ways:

  / CORP -> ICS for updates, docs

  / ICS -> CORP to export production data

/ So you'll end up with two data diodes, one in each direction, which goes a bit against the principle...

THREAT MODELING (SIMPLIFIED)

What does DYODE guarantees?

No data will go from OUT to IN. That's all. Period.

⌄

What attacks are still possible?

The overall security of the solution still relies on logical hardening.

If the "out" corner is not secured, it might be possible for an attacker to

/ Perform a Denial of Service

/ Compromise the Raspi and modify the data

LIMITS

Performances

/ Low speed, a few mbs

/ High latency caused by flat file transfer

➔ *Replaced by a naive, native Python sockets implementation*

Side channels

/ Side channels, especially based on electromagnetic leaks (TEMPEST) were not taken in consideration in the threat model

/ However, EM leaks can be reduced with faraday cages
➔ *Re-use of forensics (relatively low cost) portable faraday cages used when handling phones?*

Gateway hardening

/ In and out gateways are not especially hardened and can be compromised

/ The target it only to prevent information flowing from ICS to CORP

Not compatible with safety-critical environments (yet)

Roadmap

Modbus/S7 integrity control

- Acting as an application firewall in whitelist mode to check the correctness of the parameters

Link status monitoring - Heartbeat

- Ex: Using a cronjob + a SNMP trap on the receiver side

File integrity checking (1/2)

- Level1: perform a file validation by the receiving gateway, either with an AV (basic) or a specific parser/converter such as Lagadec's Exefilter or CIRCLean or against specific hashes for binaries

- Level2: use a dedicated device for file parsing which can be further hardened (the exposition can be limited to the parsing component, the TCP/IP stack and a limited number or entry points)

- Level3: Use Qubes OS throwable VM

Other protocols

- Add support for SNMP, Syslog, CIFS, SMTP, FTP, SFTP, etc

Traceability of the transfers

- Level1: generate hash of the files/values transferred

- Level2: use 2 DYODE and 3 RSPi (in, out and crypto-signer); the RSPi in the middle combined with an OpenPGP card can generate the hashes and add a signature

Current deployments

/ Similar setup, different implementation (.NET) made by one of our clients

/ Used in a summer internship for Virginia Space #ohmygawddyodeintospace
https://github.com/EBUJOLD/data-diode
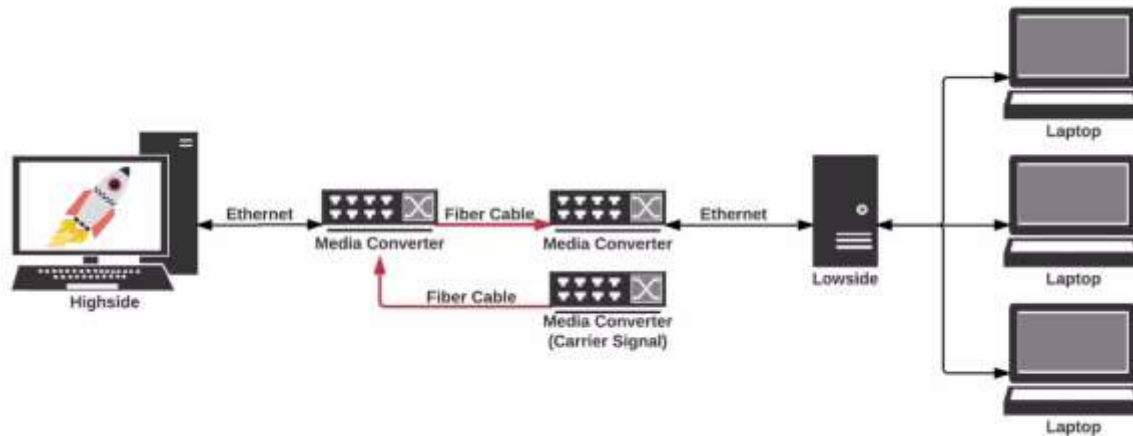
/ Tests in progress at another client to isolate safety PLCs from the DCS

Conclusion

It works.

It's cheap.

Contribute !

As demonstrated
[*if the demo did not fail*]
DYODE answers to safe
data exchange needs

300€ for the v1

80€ for the v2

We need contributions to
make the product more
reliable and add features

https://github.com/wavestone-cdt/dyode

YOU GET A DIODE

AND YOU GET A DIODE

EVERYONE GETS A DIODE !

imgflip.com

WAVESTONE

Arnaud SOULLIE

Arnaud.SOULLIE@wavestone.com