RSAConference2016

Abu Dhabi | 15–16 November | Emirates Palace

Connect to Protect

SESSION ID: CIN-T07

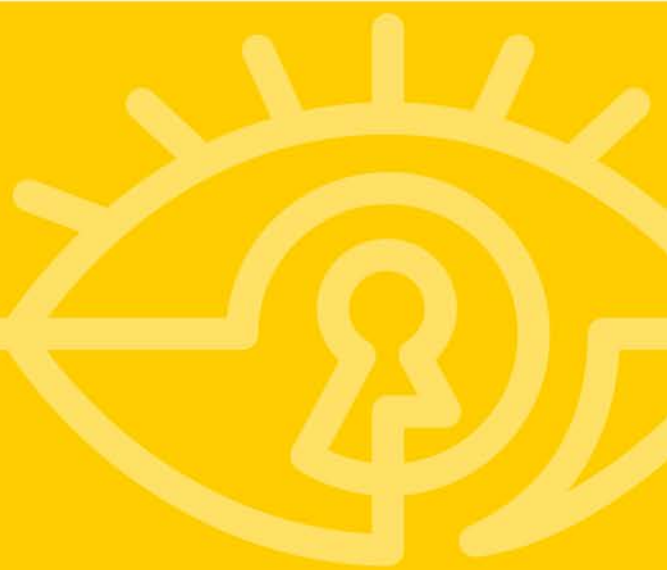
Deployments of Unidirectional Communication between ICS OT & Corporate IT

Gilles Loridon
CEO
Global Security Network

#RSAC

Content

- Unidirectional Communication: introduction to the technology
- Case study 1: is transferring 400,000 files per minute to Honeywell PHD server a good idea?
- Case study 2: my ICS protocol (i.e. Modbus) is bidirectional, how can I use data diodes?
- Case study 3: how to **save** truckload of money and increase security with Pi to Pi replication.



Unidirectional Communication: the technology

Business Case

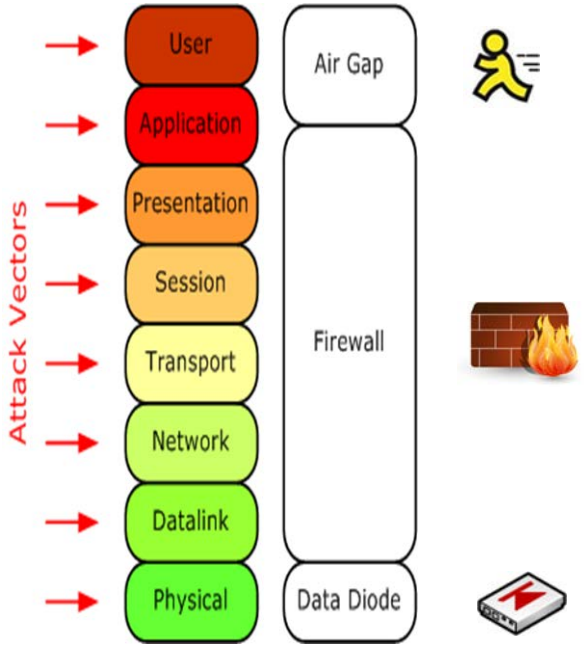
Critical National Infrastructure companies have/should have physically isolated plant networks hosting systems that are:

- Critical to the national economy and the safety of its people.
- If compromised can cause lost of life, huge financial and environmental cost.

ISSUE

- These plant networks need to send information to corporate networks without compromising security that is provided by physical network isolation

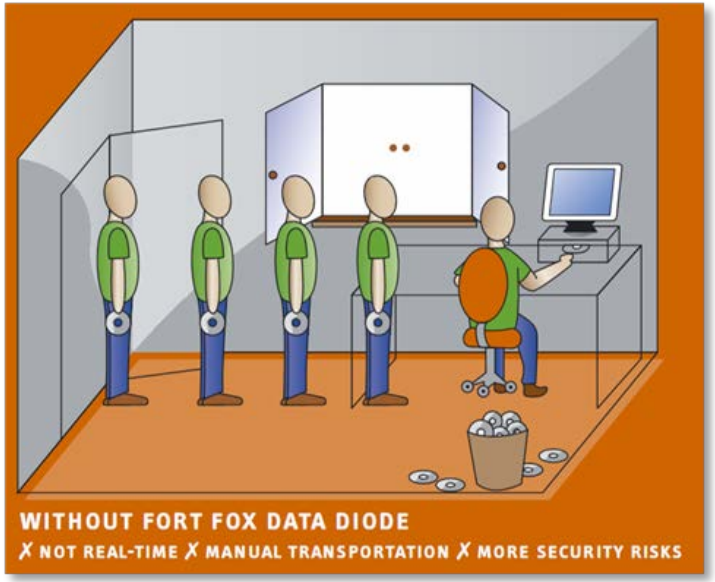
Network Boundary Options



- Air Gap:
  - Not Real-time & time consuming
- Firewall:
  - Vulnerabilities, misconfiguration & disgruntled staff
- Data Diode:
  - Real-time one-way. Period.

Existing Solution – Air Gap t

- To export data from the critical / high security network an **AIR GAP** solution is used.
- Employees put data on removable media like a CDROM, USB device, magnetic tape.
- The data is **manually imported** into the corporate network.



- **Problems**
  - Labor intensive manual process
  - Delay in transferring data
  - Data leakage issues

GLOBAL SECURITY NETWORK

Usual solution: firewall

- To deploy an IT Firewall and enable a rule-based one way data transfer.

Problems:

- Firewall is based on firmware, software and logic and is therefore vulnerable to attacks
- Is the Firewall setup properly?
- Back doors, covert channel???
- No guarantee of data traffic not going back to the external network.

CISO & Fortinet CVEs

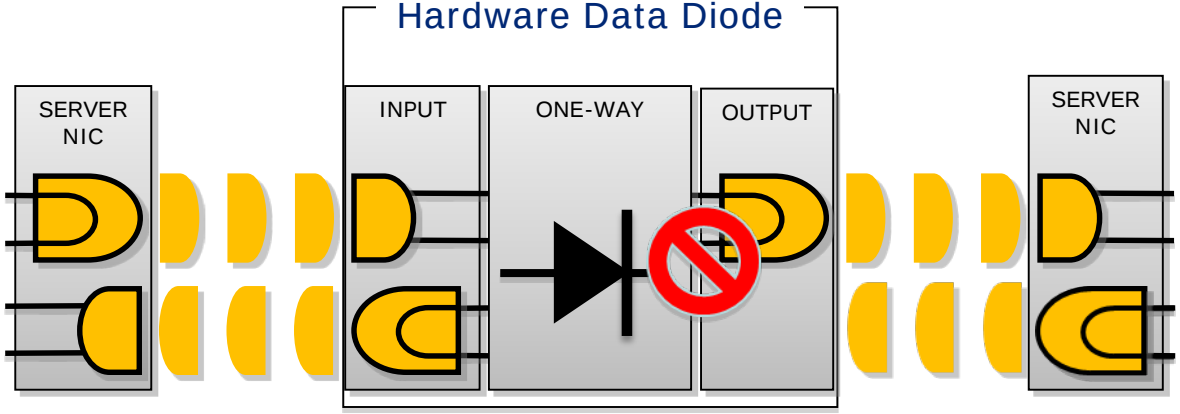
1	CVE-2016-1300	79	XSS	2016-01-27	2016-01-28	4.3	None	Remote	Medium	Not required	None	Partial	None
Cross-site scripting (XSS) vulnerability in Cisco Unity Connection (UC) 10.5(2.3009) allows remote attackers to inject arbitrary web script or HTML via a crafted URL, aka Bug ID CSCux82582.														
1	CVE-2016-1909	264		2016-01-15	2016-01-21	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
FortiOS 4.x before 4.3.17 and 5.0.x before 5.0.8 has a hardcoded passphrase for the Fortimanager_Access account, which allows remote attackers to obtain administrative access via an SSH session.														
2	CVE-2015-8038	79	XSS	2015-11-02	2015-11-03	4.3	None	Remote	Medium	Not required	None	Partial	None
Multiple cross-site scripting (XSS) vulnerabilities in the Graphical User Interface (GUI) in Fortinet FortiManager before 5.2.4 allow remote attackers to inject arbitrary web script or HTML via the (1) sharedjobmanager or (2) SOMServiceObjDialog.														
3	CVE-2015-8037	79	XSS	2015-11-02	2015-11-03	4.3	None	Remote	Medium	Not required	None	Partial	None
Multiple cross-site scripting (XSS) vulnerabilities in the Graphical User Interface (GUI) in Fortinet FortiManager before 5.2.4 allow remote attackers to inject arbitrary web script or HTML via the (1) SOMVpnSSLPortalDialog or (2) FGDMngUpdHistory.														
4	CVE-2015-7362	264	+Priv	2016-01-08	2016-01-12	7.2	Admin	Local	Low	Not required	Complete	Complete	Complete
Fortinet FortiClient Linux SSLVPN before build 2313, when installed on Linux in a home directory that is world readable and executable, allows local users to gain privileges via the helper/subroc setuid program.														
5	CVE-2015-5965	20		2015-08-11	2015-08-11	5.0	None	Remote	Low	Not required	None	Partial	None
The SSL-VPN feature in Fortinet FortiOS before 4.3.13 only checks the first byte of the TLS MAC in finished messages, which makes it easier for remote attackers to spoof encrypted content via a crafted MAC field.														
6	CVE-2015-5737	264		2015-09-03	2015-09-04	7.2	None	Local	Low	Not required	Complete	Complete	Complete
The (1) mdare64_48.sys, (2) mdare32_48.sys, (3) mdare32_52.sys, (4) mdare64_52.sys, and (5) Fortishield.sys drivers in Fortinet FortiClient before 5.2.4 do not properly restrict access to the API for management of processes and the Windows registry, which allows local users to obtain a privileged handle to a PID and possibly have unspecified other impact, as demonstrated by a 0x2220c8 ioctl call.														
7	CVE-2015-5736	264	Exec Code	2015-09-03	2015-09-04	7.2	None	Local	Low	Not required	Complete	Complete	Complete
The Fortishield.sys driver in Fortinet FortiClient before 5.2.4 allows local users to execute arbitrary code with kernel privileges by setting the callback function in a (1) 0x220024 or (2) 0x220028 ioctl call.														
8	CVE-2015-5735	264		2015-09-03	2015-09-04	7.2	None	Local	Low	Not required	Complete	Complete	Complete
The (1) mdare64_48.sys, (2) mdare32_48.sys, (3) mdare32_52.sys, and (4) mdare64_52.sys drivers in Fortinet FortiClient before 5.2.4 allows local users to write to arbitrary memory locations via a 0x226108 ioctl call.														
9	CVE-2015-4077	200	+Info	2015-09-03	2015-09-04	2.1	None	Local	Low	Not required	Partial	None	None
The (1) mdare64_48.sys, (2) mdare32_48.sys, (3) mdare32_52.sys, and (4) mdare64_52.sys drivers in Fortinet FortiClient before 5.2.4 allows local users to read arbitrary kernel memory via a 0x22608C ioctl call.														
10	CVE-2015-3626	79	XSS	2015-08-11	2015-08-11	4.3	None	Remote	Medium	Not required	None	Partial	None
Cross-site scripting (XSS) vulnerability in the DHCP Monitor page the Web User Interface (WebUI) in Fortinet FortiOS before 5.2.4 on FortiGate devices allows remote attackers to inject arbitrary web script or HTML via a crafted hostname.														
11	CVE-2015-3620	79	XSS	2015-05-12	2015-05-14	4.3	None	Remote	Medium	Not required	None	Partial	None
Cross-site scripting (XSS) vulnerability in the advanced dataset reports page in Fortinet FortiAnalyzer 5.0.0 through 5.0.10 and 5.2.0 through 5.2.1 and FortiManager 5.0.3 through 5.0.10 and 5.2.0 through 5.2.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.														
12	CVE-2015-3293	200	+Info	2015-04-14	2015-04-15	4.0	None	Remote	Low	Single system	Partial	None	None
FortiMail 5.0.3 through 5.2.3 allows remote administrators to obtain credentials via the "diag debug application httpd" command.														
13	CVE-2015-2323	310		2015-08-11	2015-08-11	6.4	None	Remote	Low	Not required	Partial	Partial	None
FortiOS 5.0.x before 5.0.12 and 5.2.x before 5.2.4 supports anonymous, export, RC4, and possibly other weak ciphers when using TLS to connect to FortiGuard servers, which allows man-in-the-middle attackers to spoof TLS content by modifying packets.														
14	CVE-2015-2281	119	Exec Code Overflow	2015-03-19	2015-09-10	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Stack-based buffer overflow in collectoragent.exe in Fortinet Single Sign On (FSSO) before build 164 allows remote attackers to execute arbitrary code via a large PROCESS_HELLO message to the Message Dispatcher on TCP port 8000.														

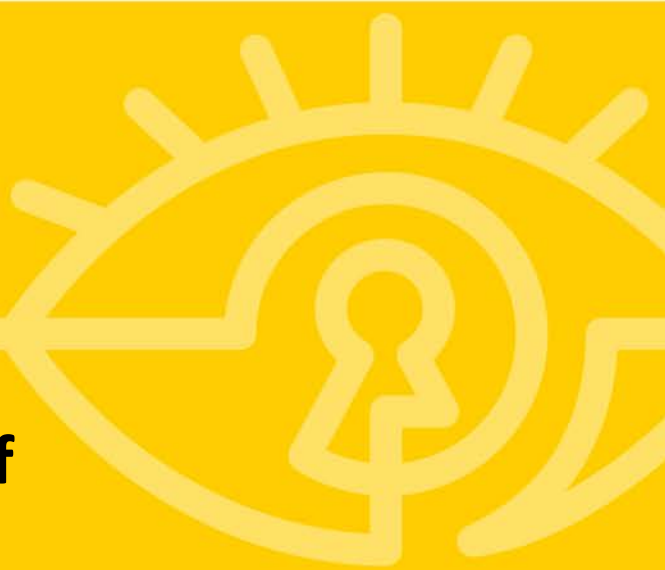
GLOBAL SECURITY NETWORK

Data Diode Solution

- One-way communication physically secured by Hardware Data Diode
- Hardware only (no software / logic on the DD)
- Impossible to penetrate/attack
- Certified devices (the only **CC EAL 7+** certified device in the world)

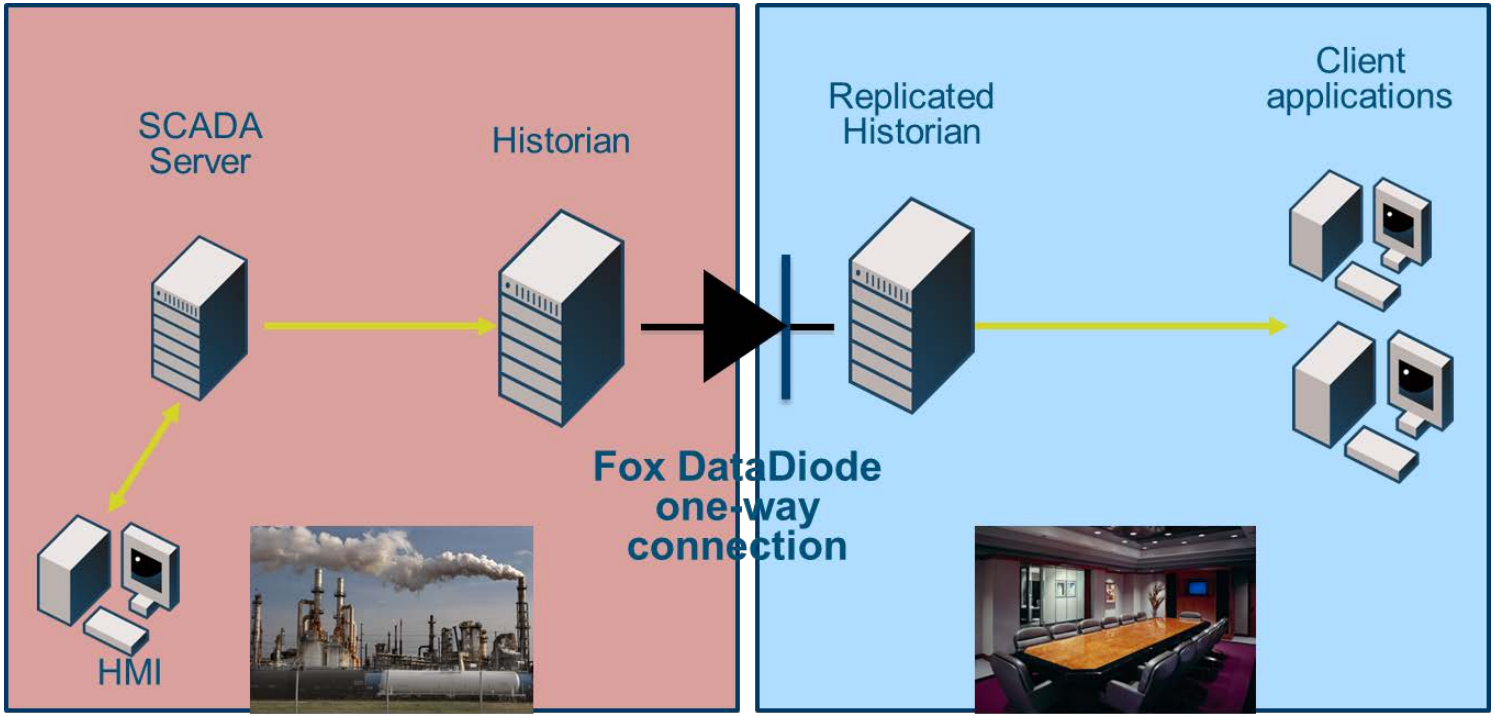
How it works?


Hardware Data Diode
SERVER NIC
INPUT
ONE-WAY
OUTPUT
SERVER NIC
LIGHT EMITTER
LIGHT RECEIVER
Possible
Impossible



Case study 1: One way replication of Historian server between OT and IT

Historian replication setup



So far so good

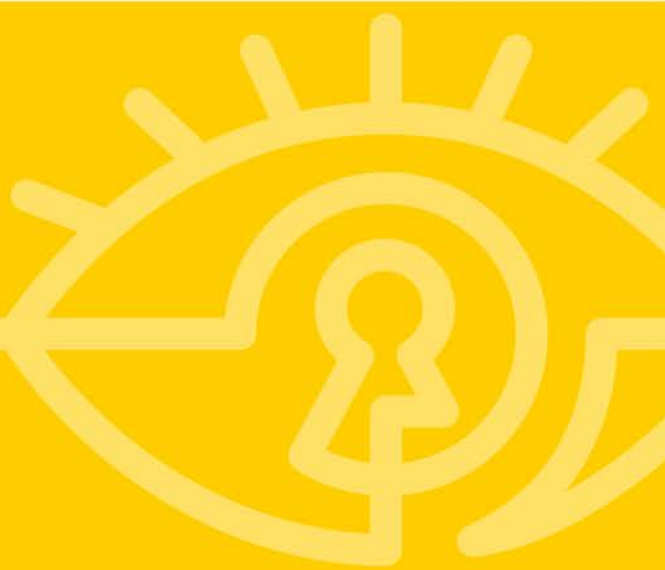
- Existing Honeywell PHD server with millions of data points in back log.
- Master PHD server connected to Slave PHD server with 1 Gbps network connection
- OT Engineers familiar with the historian protocols
- Factory Acceptance Test: few thousands data points replicated from OT to IT through FTP file transfer. FAT passed with flying colours.

Issues

- To process the backlog the OT Engineers sent hundreds of thousands files per minute through the Data Diode to one single network share folder.
- Surprise, surprise: the file sharing sever crashed, I/O kernel panic.
- The OT Engineers blamed the donkey (=Data Diode)

Solution

- We developed a packer/unpacker software to pack the files into a single zip before sending it through the diode.
- We unpacked the files in Ram Disk to the Windows server and on temporary folders.
- A much better design would have been to use a TCP stream to send the data points across the Diode.



Case Study 2: Modbus Master Slave replication

NPP segregation within OT networks

The challenge:

Nuclear Power Plant Data extracted from RTU over Modbus

Customer requirements

Segregate OT operations from OT monitoring network

Highest assurance to prevent Cyber-attacks

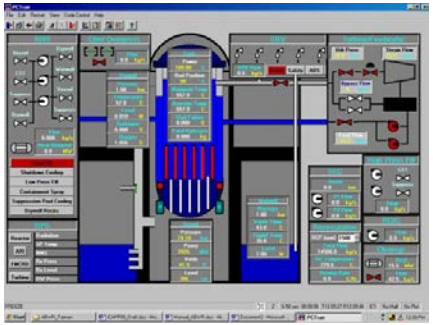
Being able to send information to headquarters

GLOBAL SECURITY NETWORK

Modbus technical challenge

RTU Modbus Slave
on OT Control

Supervision Modbus Master
on OT Monitoring



Read coil #124 status?

coil #124 is ON

Technical solution

RTU Modbus Slave
on OT Control

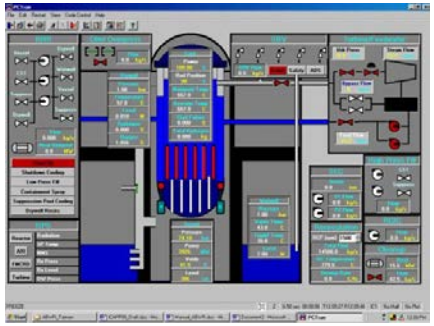
Modbus
Fake Master

Modbus
Fake Slave

Supervision Modbus Master
on OT Monitoring

Read coil #124 status?

Read coil #124 status?

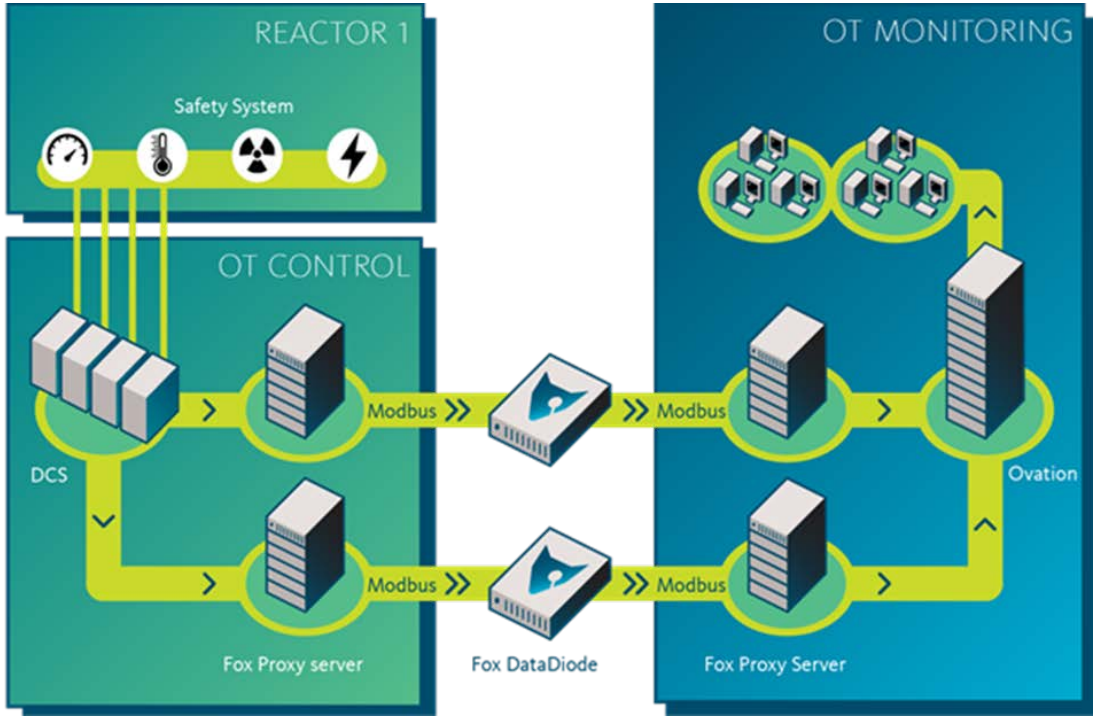


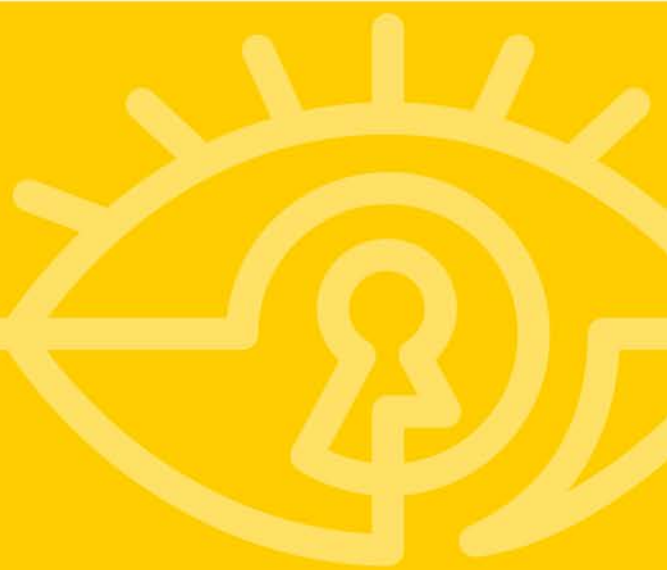
coil #124 is ON

coil #124 is ON

coil #124 is ON

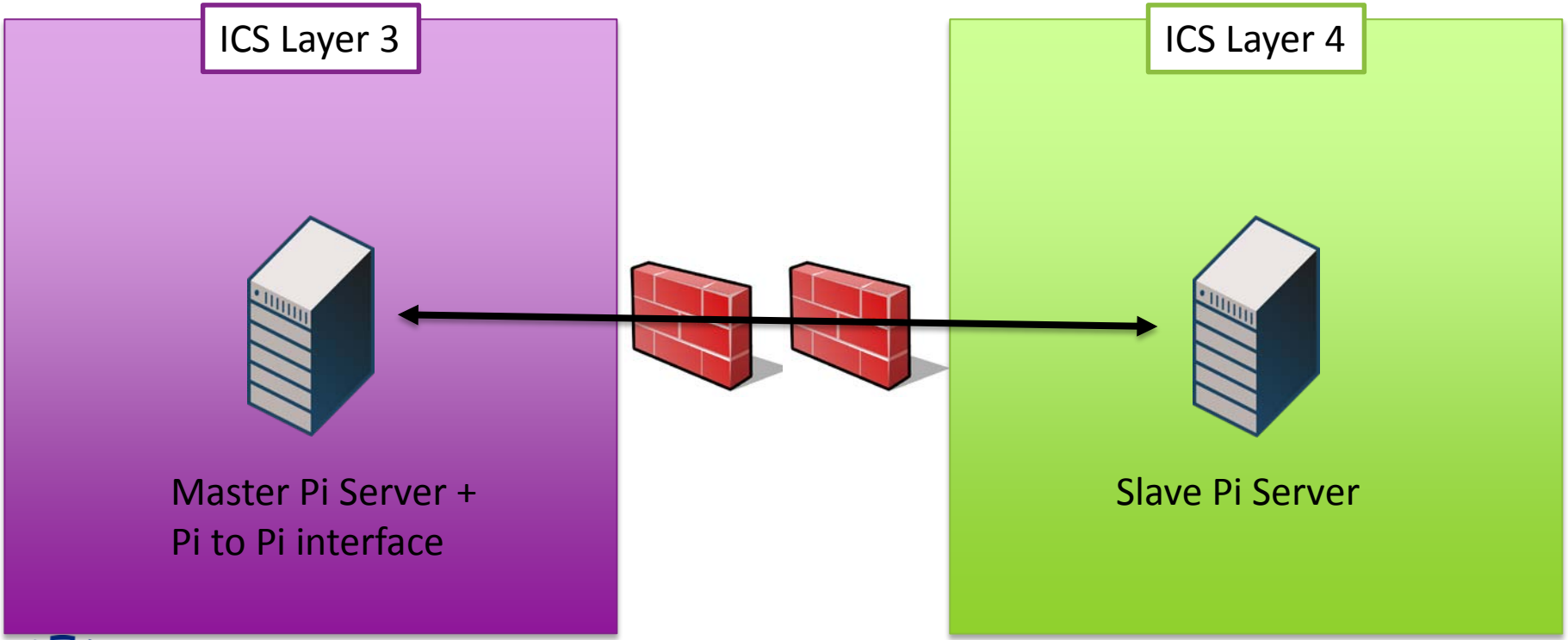
Final Solution



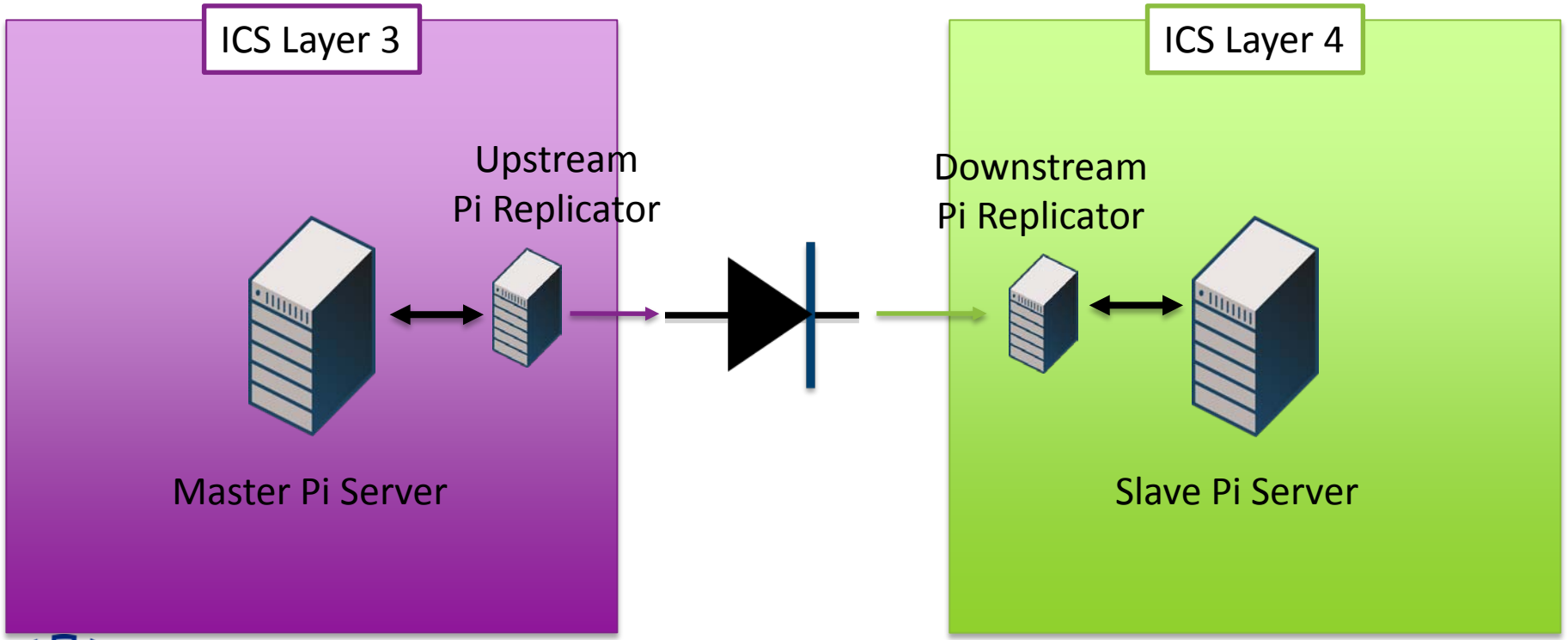


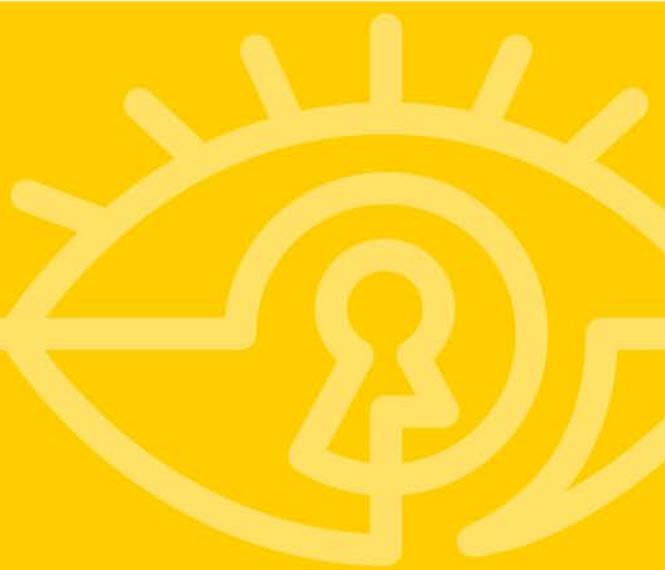
Case Study 3: Pi to Pi replication

Usual setup


ICS Layer 3
ICS Layer 4
Master Pi Server +
Pi to Pi interface
Slave Pi Server

Data Diode setup: major savings





Wrap-up and Q&A

“Apply” Slide

- Always involve the Data Diode guys as early as possible in the project design.
- Even if your technical protocol is two ways, as long as your Business requirement is one-way, there should be a diode solution.
- Data Diode could be sold to management as a way to save CAPEX and big time OPEX.
- If you have to have ICS L3 to L4 communication, you should consider one-way communication.
- If you need to implement zone/conduit between critical safety systems and OT network, you should consider Diodes.

Q&A

- All questions welcomes!
- Thank you, shoukran and merci!