



*Security and Reliability
in Control Systems Operations*

Securing Network Perimeters

How Operations & IT Can Benefit

Ron Mraz, Ph.D.
Owl Computing Technologies, Inc.



Owl Computing Technologies

- Ron Mraz, Ph.D. – Carnegie-Mellon
- Westinghouse, IBM Research
- President & CTO
 - 12 patents, others pending



Owl Computing Technologies

- ❑ Founded 1998 -- US owned & self-funded
- ❑ Business philosophy
 - Products, not projects
- ❑ Over 1,200 security solutions deployed
 - Power Gen (fossil, hydro, nuclear); process control, etc.
 - US DoD, Intel & US civilian agencies



Customer Case Studies

- Utility customers
 - Single solution protecting 22,000 critical assets to allow orderly and controlled updates.
 - Single solution consolidating 29 point to point links.
 - Remote monitoring saves effort in maintaining systems.
- DoD services provider
 - Single enterprise system more than doubled capacity of entire organizations capacity.
 - Provided a 50:1 footprint reduction of classified assets for customers requirements
- Intelligence services provider
 - Selected Owl Computing as the preferred transfer provider from head to head bake off competition.
- DoD
 - Consolidated video and file transfer solution.
 - Providing systems allows collect to be done in unclassified domains, reducing classified footprints.



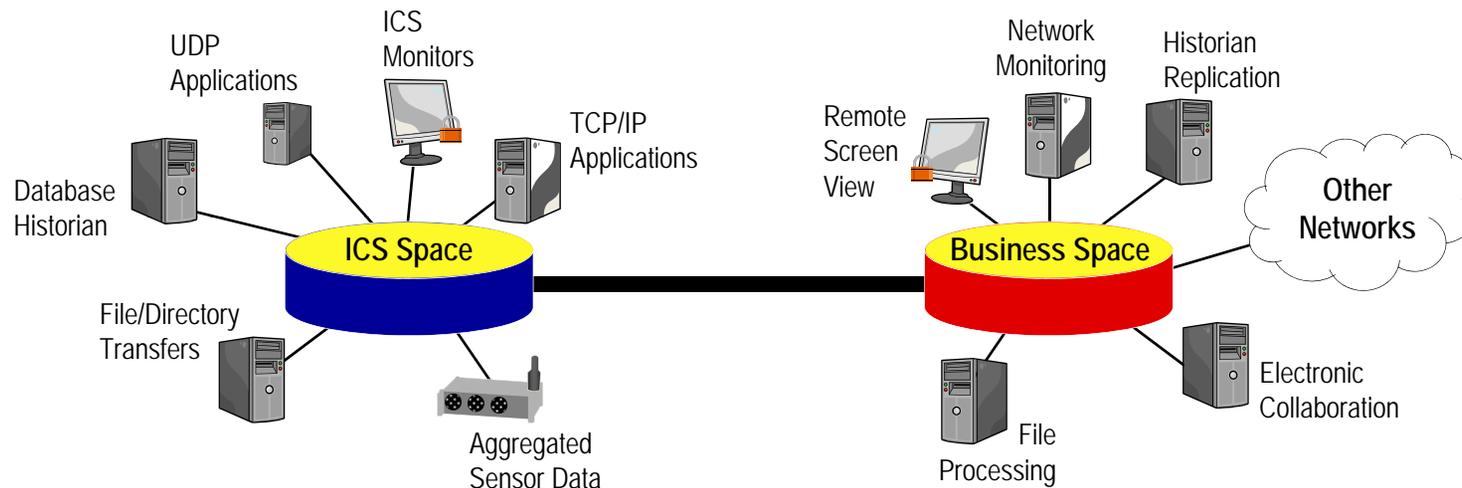
*It's not just about IT, and it's not just
about compliance. It's about*

- ❑ Cyber Security,
- ❑ Reliability,
- ❑ Availability of systems.

The definitions of success for the above are
different for O and IT systems.



O/IT Communications



Operations domain.
Can be 1000's of devices!

Information Tech Domain
Can be 1000's of clients!

This is what IT operations would like to have.

To support this, IT support processes need be applied to OT support?

Can 24/7 OT operations survive frequent routine upgrades as IT supports?



*Security standards are requiring
one or more of the following features in perimeter defenses*

- ❑ Hardware enforced unidirectional data flow
- ❑ Non-routable packets across the boundary
- ❑ True IP protocol break
- ❑ Role based management of the security device
- ❑ Detailed logging and auditing tools

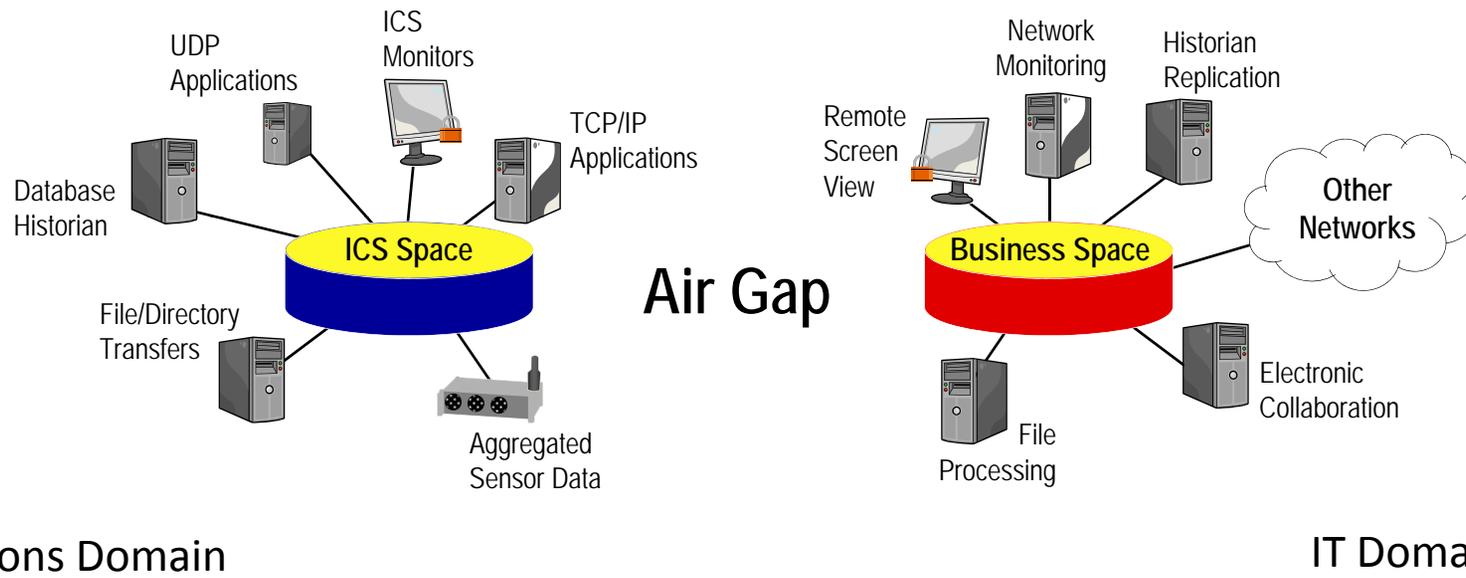


Other features in electronic perimeter defenses

- ❑ Electrical isolation
- ❑ Remote monitoring and management
- ❑ Fiber optic transfer
- ❑ System volatility
- ❑ Operating system hardening
- ❑ Data replay – buffering
- ❑ Failover
- ❑ Redundancy



O/IT True Security Separation



This is what security minded operations would like to see. With true physical isolation a policy of urgent system upgrades is not required. This saves time, resources and promotes scheduled maintenance. (ROI)

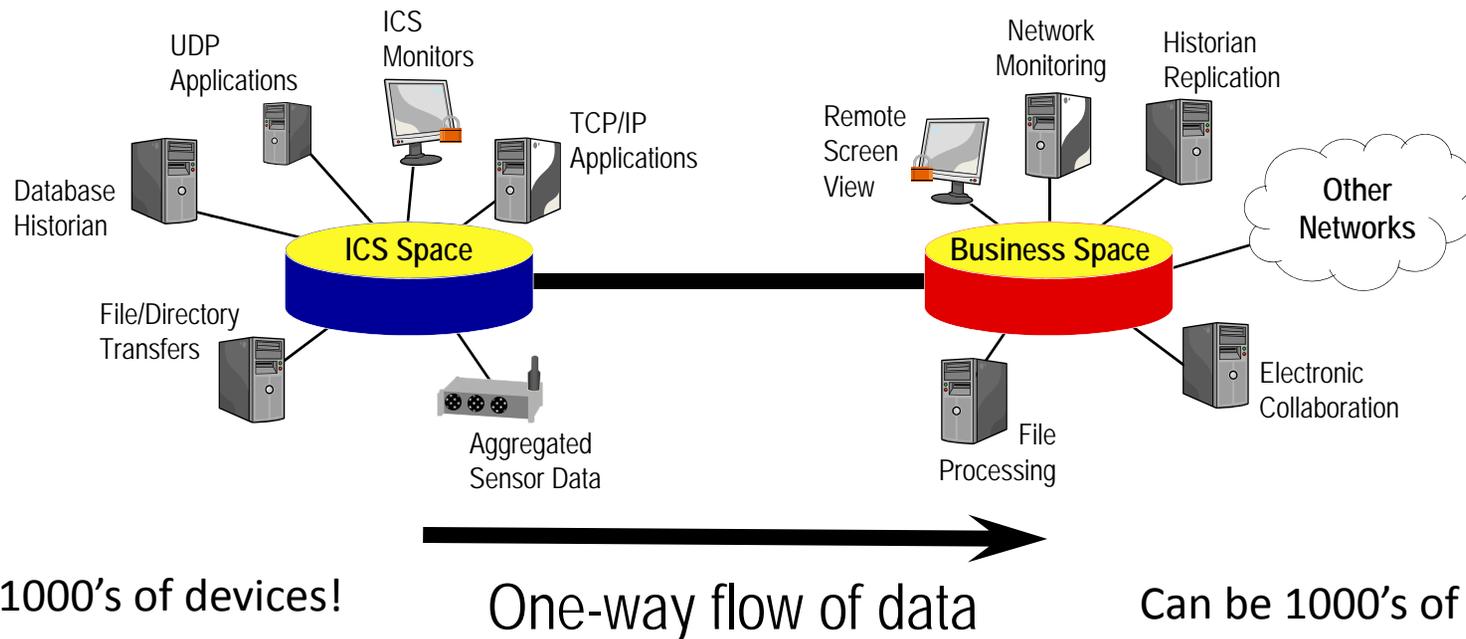


Industrial Control Systems Challenges

- ❑ Broad range of data types must be shared
SCADA, database historian, core monitoring, etc.
- ❑ Critical infrastructure must be protected
- ❑ Compliance with security standards
& regulations must be achieved



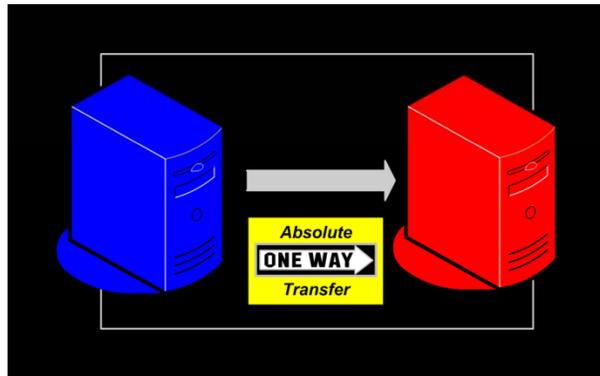
O/IT Secure Communications



This is what would logically satisfy both O and IT –
A one-way flow of non-routable data that is auditable and
has role based management with absolutely no return flow.



Hardware enforced unidirectional data flow

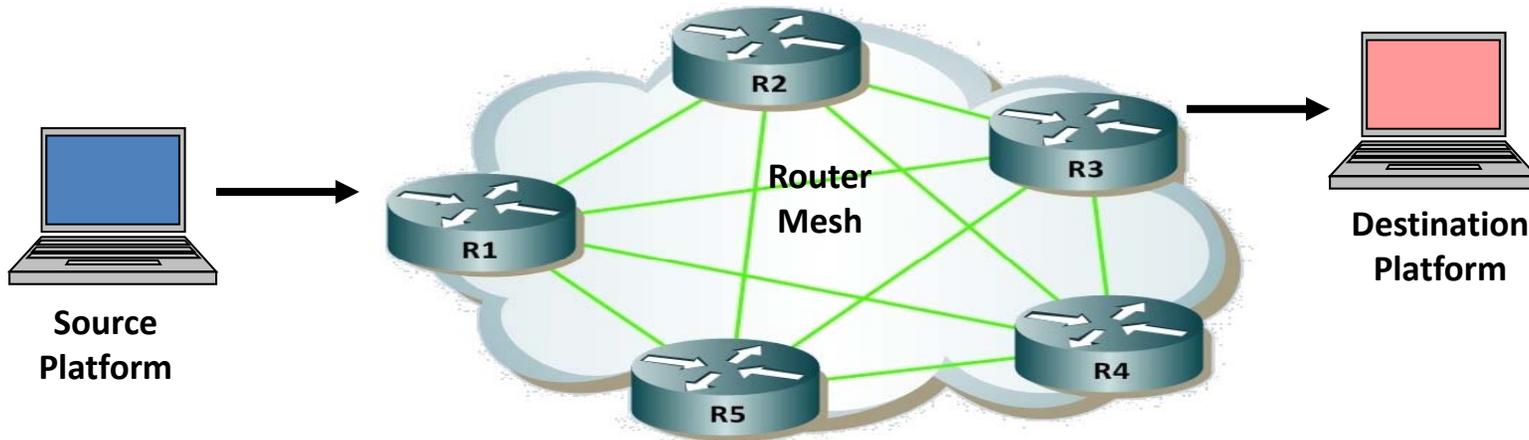


- Send computer connects through LED transmitter
- Receive computer connects through optical receiver
- Originator of data initiates movement
- Trust Nothing design - impossible for data to leak back



Non-routable packets across the boundary

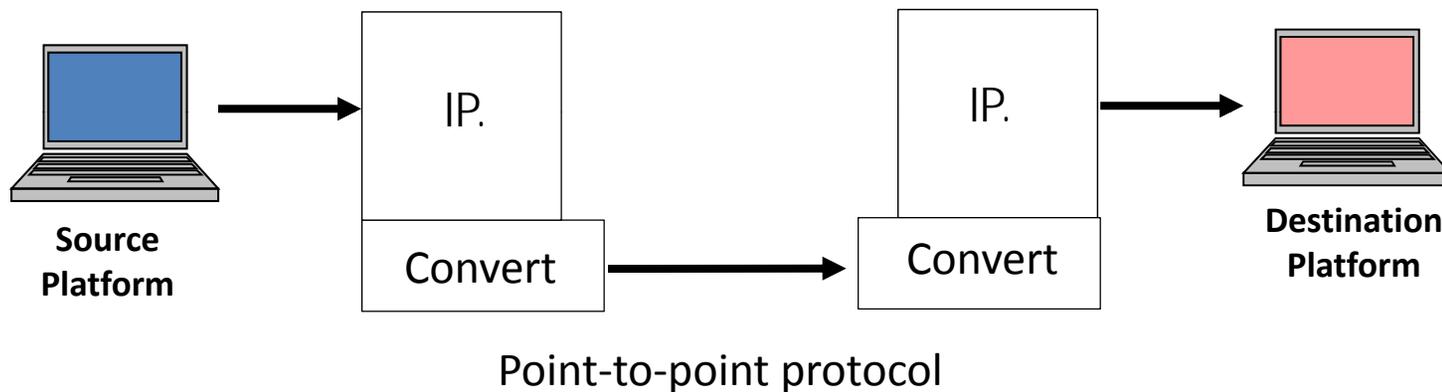
0	4	8	16	19	31
Version	IHL	Type of Service	Total Length		
Identification			Flags	Fragment Offset	
Time To Live	Protocol		Header Checksum		
Source IP Address					
Destination IP Address					
Options				Padding	



IP Packet is self-routable: contains source, destination address
We require a true point to point protocol



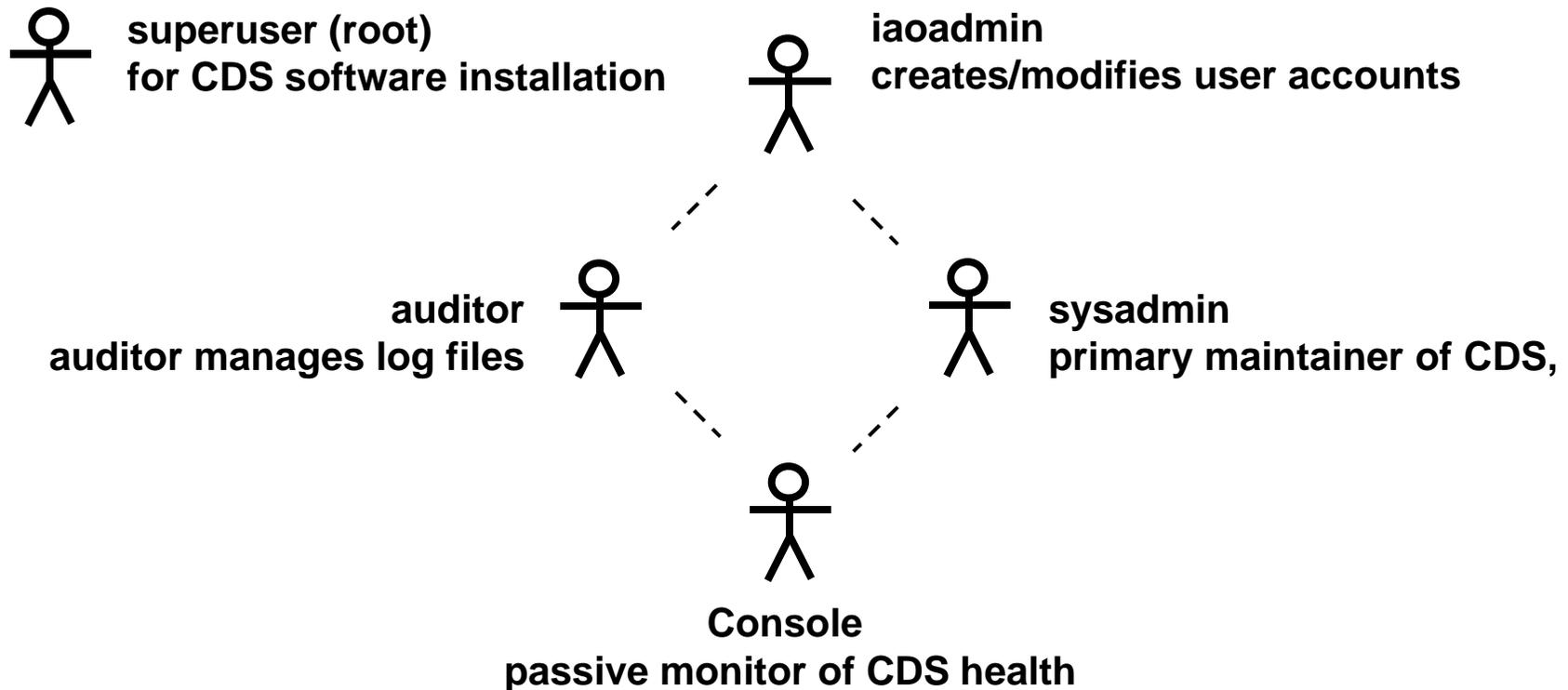
True IP protocol break.



When packets that cross the network boundary are converted to point to point packets. This satisfies both the protocol break and the non-routable packet requirements.



Role based management of the security device.



The ability to support other multiple login roles
in addition to an Admin or Root.

Some roles are restricted to only certain menu items.



Menu-driven Role Based Access & Control

- Role based use case access.
- No command line access for standard day to day operations.

```
#####
##      MAINTENANCE MODE      (BLUE) ##
#####
##      IAODADMIN TASKS      ##
##      CDS HEALTH MENU      ##
##-----##
##  1. Disk Usage            ##
##  2. Virtual Memory Statistics ##
##  3. Verify System Time    ##
##  4. Verify Network Connections ##
##  5. Verify CDS Status     ##
##  6. Examine CDS Logs     ##
##-----##
##  7. List Send Files      ##
#####
##  M. Return to Main Menu  ##
##  X. EXIT                 ##
#####
Make your selection:
```

```
#####
##      MAINTENANCE MODE      (BLUE) ##
#####
##      IAODADMIN TASKS      ##
##-----##
##  1. CDS Version Number   ##
##  2. CDS Health           ##
##  3. CDS Mode Changes     ##
##  4. System Management    ##
##  5. Audit Log Management ##
##  X. EXIT                 ##
#####
Make your selection:
#####
## Examine Current CDS Logs (BLUE) ##
##-----##
##  1. dd_send2500.log      ##
##  2. tcpfileserver.log   ##
##  3. owlPostProcess.log ##
##  4. owlProblemProcess.log ##
##  5. Scanning logs       ##
#####
##  M. Return to Main Menu  ##
##  X. EXIT                 ##
#####
Make your selection:
```

```
#####
##      MAINTENANCE MODE      (BLUE) ##
#####
##      AUDADMIN TASKS      ##
##-----##
##  1. CDS Version Number   ##
##  2. CDS Health           ##
##  3. CDS Mode Changes     ##
##  4. System Management    ##
#####
##  X. EXIT                 ##
#####
Make your selection:
#####
##      MAINTENANCE MODE      (BLUE) ##
#####
##      IAODADMIN TASKS      ##
##      CDS HEALTH MENU      ##
##-----##
##  1. Disk Usage            ##
##  2. Virtual Memory Statistics ##
##  3. Verify System Time    ##
##  4. Verify Network Connections ##
##  5. Verify CDS Status     ##
##  6. Examine CDS Logs     ##
##-----##
##  7. List Send Files      ##
#####
##  M. Return to Main Menu  ##
##  X. EXIT                 ##
#####
Make your selection:
```

(Role Based Menus)



Detailed logging and auditing tools

Refresh
Close

DFTS Filtered Log Events		
Date Time	Filename	Error Details
03/05-10-53:55	q203-test.dat	isValidPacketType: Invalid packet: FADE, bytesread = 144
03/05-10-59:25	q300mb.dat	data receive timeout (Duration = 00:02:00), PktCount = 10810
03/05-10-59:25	q300mb.dat	FileSizes: Exp: 314,572,800, Accum: 173,506,068
12/15-18-22:38	p200mb.dat	ERROR, ABORTED ... received NEW StartOfMag, Current PktCount = 8858
12/15-18-30:35	j203-test.dat	ERROR, ABORTED ... received NEW StartOfMag, Current PktCount = 2546
12/15-19-08:03	j203-test.dat	waitForStartPacket: Received non-header buffer, PktType: OFF0 (DATA), bytes_received: 16272
12/15-19-09:53	j203-test.dat	waitForStartPacket: Received non-header buffer, PktType: OFF0 (DATA), bytes_received: 16272
01/12-13-52:21	q300mb.dat	data receive timeout (Duration = 00:02:00), PktCount = 4746
01/12-13-52:21	q300mb.dat	FileSizes: Exp: 314,572,800, Accum: 76,166,740

Refresh
Close

```

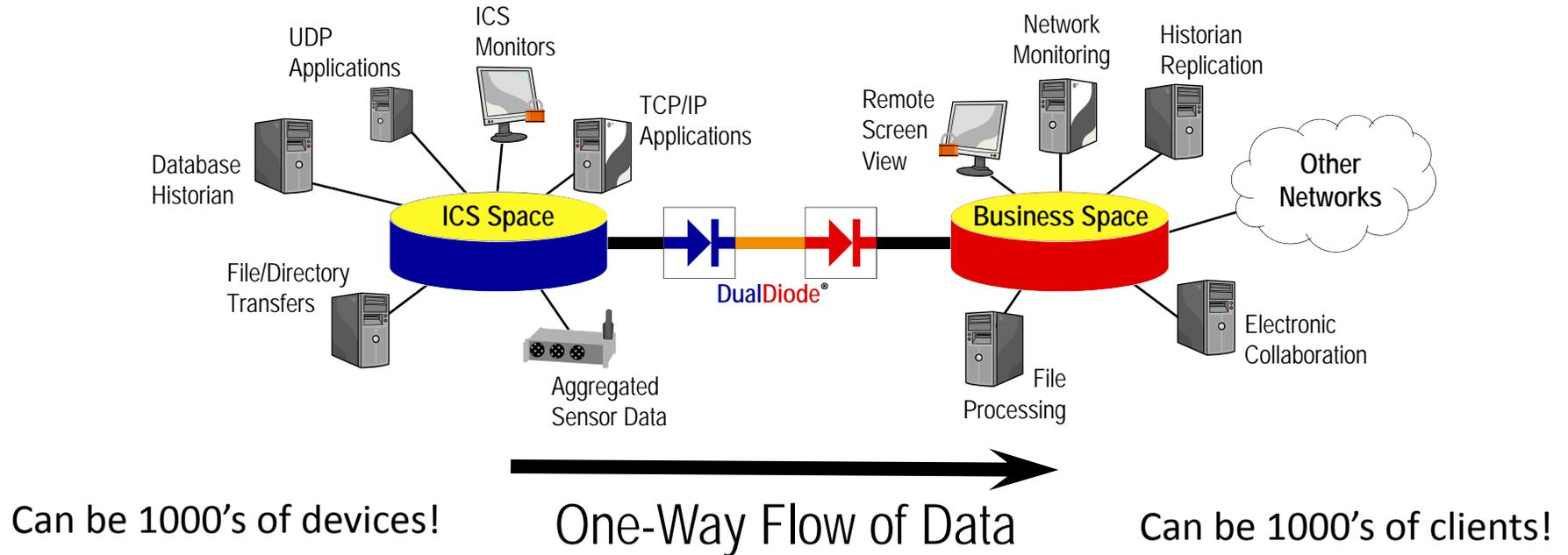
: archive: 1 days
: archdir: [/export/home/owl/logs/archive]
: filter : [/export/home/owl/logs/dd_send-????????-?????-???.log]
urrentTime = 2011-02-10 00:00:00
ilterTime = 2011-02-09 00:01:00
rchiving [/export/home/owl/logs/dd_send-20110208-153558-000.log]
rchiving [/export/home/owl/logs/dd_send-20110208-235958-000.log]
02/10-00:00:00 logs_CheckArchiveList: Number of Files Found = 4
02/10-00:00:00 logs_CheckArchiveList: Number of Files Archived = 2
02/10-00:00:00 Sent: 314,617,920 (29.30%) Rate: 40.706 (MB/s) Dur: 00:00:02 BF: 134 BFW: 0 DW: 0.05/1 msec FR: 0.03/1
msec
02/10-00:00:03 Sent: 419,490,560 (39.07%) Rate: 40.706 (MB/s) Dur: 00:00:03 BF: 135 BFW: 0 DW: 0.05/1 msec FR: 0.04/1
msec
02/10-00:00:05 Sent: 524,363,200 (48.84%) Rate: 40.939 (MB/s) Dur: 00:00:02 BF: 134 BFW: 0 DW: 0.05/1 msec FR: 0.04/1
msec
02/10-00:00:08 Sent: 629,235,840 (58.60%) Rate: 40.623 (MB/s) Dur: 00:00:03 BF: 135 BFW: 0 DW: 0.05/1 msec FR: 0.04/1
msec
02/10-00:00:10 Sent: 734,108,480 (68.37%) Rate: 40.872 (MB/s) Dur: 00:00:02 BF: 135 BFW: 0 DW: 0.05/1 msec FR: 0.03/1
msec
02/10-00:00:13 Sent: 838,981,120 (78.14%) Rate: 40.739 (MB/s) Dur: 00:00:03 BF: 134 BFW: 0 DW: 0.05/1 msec FR: 0.04/1
msec
02/10-00:00:15 Sent: 943,853,760 (87.90%) Rate: 40.756 (MB/s) Dur: 00:00:02 BF: 133 BFW: 0 DW: 0.05/1 msec FR: 0.04/1
msec
02/10-00:00:17 Sent: 1,048,726,400 (97.67%) Rate: 40.722 (MB/s) Dur: 00:00:02 BF: 134 BFW: 0 DW: 0.05/1 msec FR: 0.04/1

```

Here is shown the ability to remotely list and then browse log files of the Perimeter Defense system.



Operational Isolation



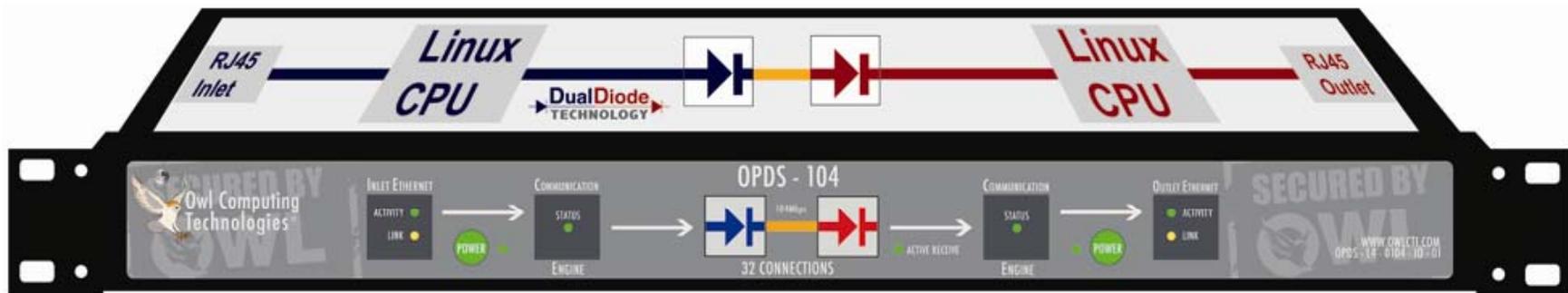
Can processes of IT support be applied to OT support?



Integrated Solution Engine

Demonstration of one-way transfer in a 1U enclosure.

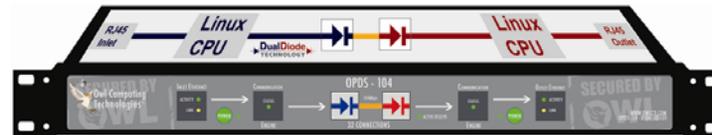
Blue and Red CPUs running Linux with Owl Dual Diode HW. Optical fiber connection and separate power supplies are internal to the enclosure.



Data
Source

Forward data path

Data
Destination

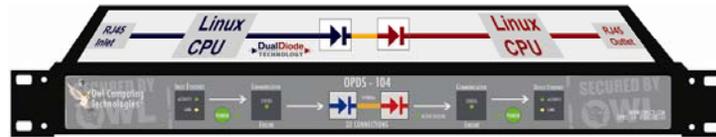


Owl One-Way Transfer Solutions

Mobile/Rugged
Tactical Solutions



1U Integrated Solutions



Enterprise Solutions



Owl Controlled Interfaces

52/104/155Mbps

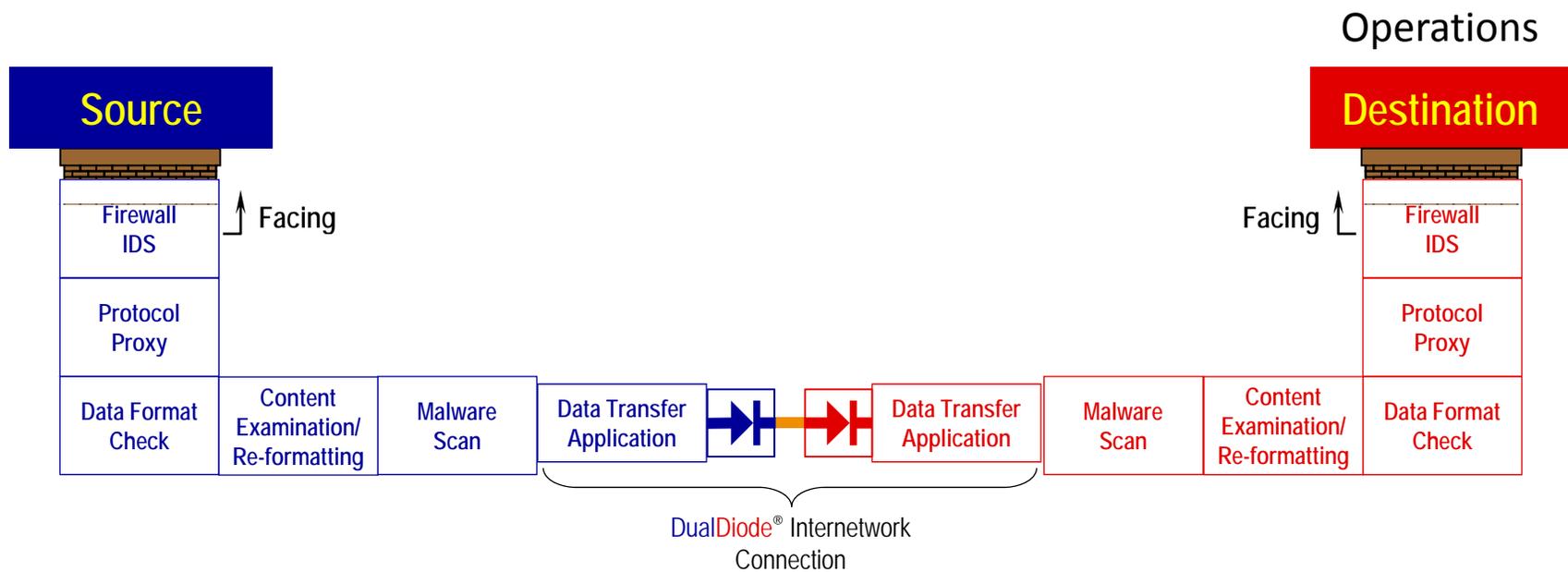
1.25/2.5Gbps

link speeds

All data types/formats



Point-to-point Secure One-Way Transfer



A Cross Domain solution includes content examination as well as self protection beyond hardware enforced policies for transfers into the operational domain.



Secure Acknowledgement Engine

- Based on US Patent 7,675,867 for a “One-Way Data Transfer System with Built-in Data Verification Mechanism.”
- Can also provide secure “scanned” transfer to Operational domains.

(Isolated Security Engine)



Operational
Domain



IT Domain



OPMS -- Owl Performance Management Service

- ❑ Global View of Monitored Systems Status
 - Monitor individual crossing, and multiple crossings
 - Status of individual data transfers
- ❑ Log File Monitor of Owl Applications
 - Errors noted from send-only & receive-only log files
- ❑ Application Support
 - All Owl applications
 - Custom application log files
- ❑ Browser-based Monitoring System
 - Supports Microsoft Internet Explorer 6+, Mozilla
 - User authentication, data encryption



Multiple Systems Remote Management

Management of multiple CDS installations monitored in the cloud.

Enhanced capabilities of the OPMS system including filtering and integration of third party applications.



Owl Computing Technologies, Inc. OWL PERFORMANCE MANAGEMENT SERVICE

Dashboard Setup Admin

Available Monitored Systems

Filter by: Systems Apps Type: Status: Filter View All Reset Counters Delete Idle

Status	System	Card	App	Type	Instance	Total Files	Total Bytes	Avg Rate (MB/s)	Error
✓	ecds-blue	2500	UPTS	BLUE	1	N/A	43,010,433,140	0.000	
✓	ecds-blue	2500	DFTS	BLUE	1	3516	1,484,291,890,351	41.97	
✓	ecds-blue	2500	TPTS	BLUE	1	N/A	122,585,983,666	0	
✓	ecds-blue	2500	RFTS	CLIENT	1	11599	121,940,553,939	0.84	
✓	ecds-blue	2500	SYSLOG	BLUE	1	N/A	0	N/A	
✓	ecds-red	2500	UPTS	RED	1	N/A	43,069,278,218	0.000	
✓	ecds-red	2500	DFTS	RED	1	3506	1,478,350,796,772	49.86	
✓	ecds-red	2500	TPTS	RED	1	N/A	122,375,757,558	0	
✓	ecds-red	2500	RFTS	SERVER	1	11591	121,835,488,060	5.40	

Owl Computing Technologies, Inc. Hostname: ecds-blue

Wednesday, February 16, 2011 2:48:59 PM

Monitor Info		Overall TCP Summary		Active TCP Connections (Last 10 Minutes)				
System	ecds-blue	Total Active Sessions	1	IP	Port	Sess Cnt	Chan Sess	Total Bytes
App	TPTS-BLUE-1	Total Bytes	763,136,254,040	192.168.252.191	2500	31	0	2,245,572
First Diode Activity	01/04-11:21:55	Total Packets	13,422,723	127.0.0.1	3500	97	1	762,712,099,840
Status	OK	Total Errors	0					

Reset View View Log View Errors

TCP Receive Data Status

Time:	Sess Num:	IP:	Bytes:	Rate:	Duration:	Num Pkts:
02/16-14:38:57	706752	127.0.0.1	49,880	0.039	00:00:01	1

© 2009 - 2010 Owl Computing Technologies, Inc.

Owl Computing Technologies, Inc. Hostname: ecds-red

Wednesday, February 16, 2011 2:35:08 PM

Monitor Info		Ten Minute Totals		Overall Totals	
System	ecds-red	Files	100	Total Files	72162
App	RFTS-SERVER-1	File Bytes	1,049,403,540	Total File Bytes	757,197,239,228
Status	OK	Errors	0	Average Rate (MB/s)	5.4
		Total Errors	0		

Reset View View Log View Errors

File Transfers

Average Rate (MB/Sec)

Active TCP Connections (Last 10 Minutes)

IP	Port	Sess Cnt	Chan Sess	Total Bytes
127.0.0.1	3500	100	1	759,934,888,318

File Transfer Activity: 100%

Initial Time: 02/16-14:22:46 Current Time: 02/16-14:22:46 Size (bytes): 27,583 File Name: DOSubmission.xml

Customer Challenges

- Data volume, velocity and variety are increasing
 - Solutions require scalable HW channels, SW streams, multiple ports.
- Multiple security domain work force
 - Solutions need to work seamlessly for the enterprise, regional and operational environments.
 - Legacy OS systems need to be considered.
 - Legacy unix, aging microsoft systems interoperation.
 - Role based menu operations.
 - Performance monitoring.
- Customer return-on-investment
 - Solutions designed for reuse to reduce accreditation efforts and facilitate time-to site test and deployment.
- Increased Threats
 - Complementary HW/SW based solutions provide hardened confidentiality, integrity and availability.



Implementation Roadmap

- ❑ Identify all protocols and applications that traverse the domain boundary.
Through application logs and existing firewall settings.
- ❑ Create a test bed to insure security equipment functionality.
Tests for bandwidth, latency, peak loads, connection streams, etc.
- ❑ Consider redundancy and failover conditions
- ❑ Review general concepts with inspectors, as appropriate
- ❑ Deploy

We have seen total time of above steps from 6 weeks to 6+ months



Summary

- ❑ The reason for cybersecurity recommendations is to maintain reliability and availability of the systems.
- ❑ Security standards have identified functions for security.
 - Hardware enforced unidirectional data flow
 - Non-routable packets across the boundary
 - True IP Protocol Break
 - Role based management of the security device
 - Detailed logging and auditing tools
- ❑ Designing a Perimeter Defense means more than domain isolation alone.
- ❑ The need for cost-effective monitoring & management follows with successful deployment.





*Security and Reliability
in Control Systems Operations*

Network Perimeters

Secured by Owl[®]

Thank you

rmraz@owlcti.com





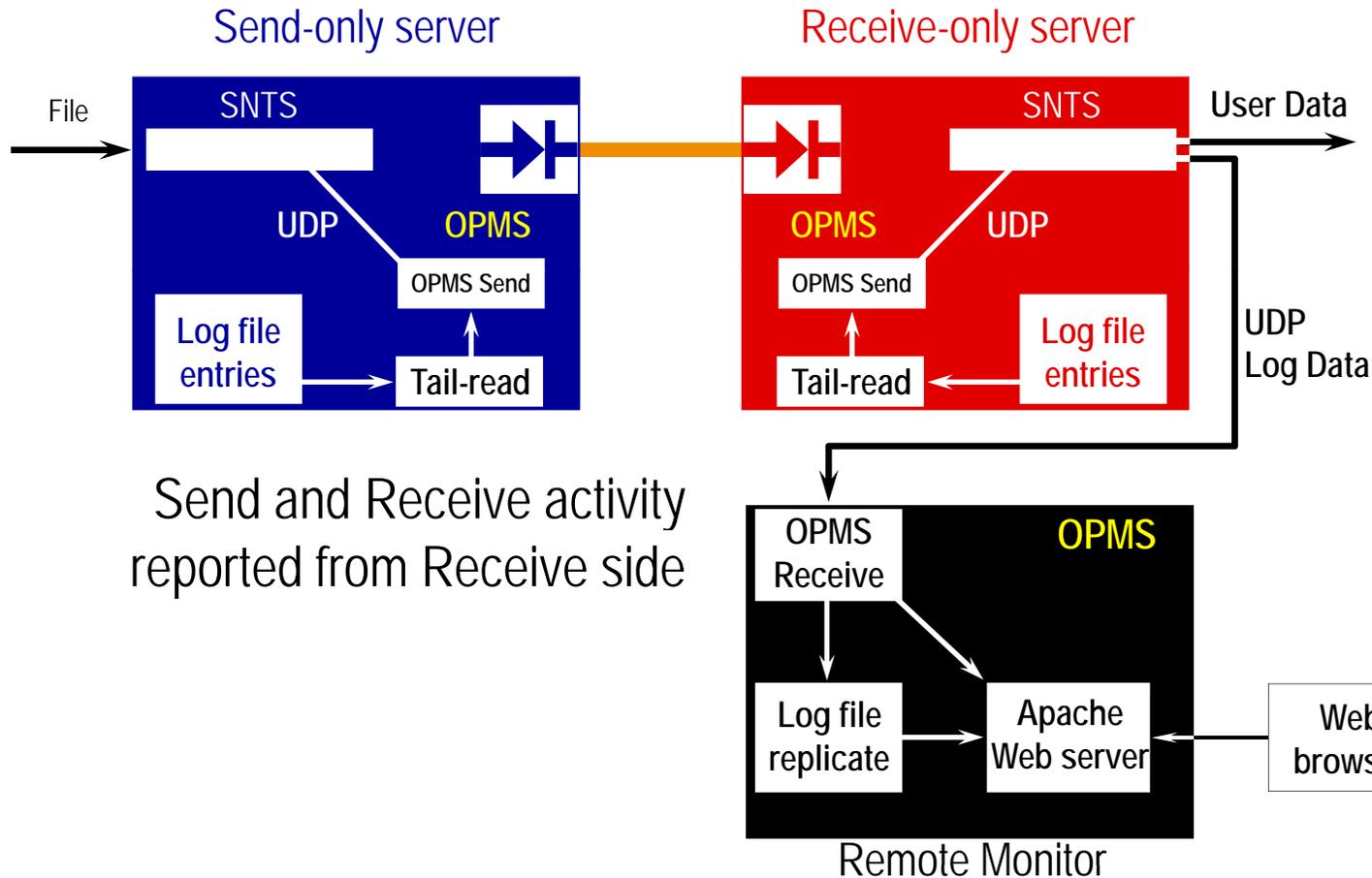
*In the Enterprise Core
At the Tactical Edge*

Securing Network Perimeters – How Operations & IT Can Benefit

The security and reliability of industrial control systems are under stress. A range of data types must be shared among diverse users outside the highly segregated control space. Critical infrastructure must be protected from external threats. Operators must comply with security standards, from bodies like NIST, and contained in regulation (NERC-CIP, etc.). As noted here, much of the discussion revolves around the impact these forces exercise on critical infrastructure from an IT perspective. There is a telling case to be made from a perspective that balances the needs of IT in protecting infrastructure networks AND the requirements placed on Operations (OT) to maintain continued reliable functions in the control space – power gen, water management, transportation grid, etc. This presentation highlights how satisfying the network protection and compliance tasks of IT can directly and cost-effectively assist OT in meeting its charter of optimal uptime.



OPMS Sample Configuration





*Security and Reliability
in Control Systems Operations*





*Security and Reliability
in Control Systems Operations*

