

*Architecting
Control System Cyber Assets
with Secure One-Way Information Transfer*

- ❑ About Owl Computing
- ❑ Operational & Business Needs
- ❑ Critical Infrastructure Cybersecurity
- ❑ Integrated Perimeter Defense
- ❑ Monitoring Perimeter Defense Performance



- ❑ Founded 1998; US owned and self-funded
Dr. Ron Mraz – President & CTO
- ❑ Business philosophy
Supported product solutions; not projects
- ❑ Continued record customer acceptance
- ❑ Over 1,000 DualDiode[®] systems deployed



Energy & Power Utilities Customers

- ❑ Nuclear & Fossil Power Generators
 - Tennessee Valley Authority
 - Duke Energy Company
 - American Electric Power
 - Energy Northwest
 - Arizona Public Service

- ❑ 25+ Operational US Sites



Government / NGO Customers

- ❑ US Intelligence Community
- ❑ Department of Defense (all branches)
- ❑ DoJ, DHS, DoS, DoE, etc.
- ❑ European MoDs
- ❑ Telecoms



Primary Operational Needs

What needs cyber protection? What threatens cyber assets?

- ❑ Level-4 critical digital assets
- ❑ Viruses
- ❑ Botnets
- ❑ Unauthorized access

Malicious or unintentional



Primary Business Needs

What information must be collected? How is it collected?

- ❑ Information from level-4 to levels-3/2 and beyond
Data historian content, Modbus, SCADA, etc.
- ❑ Via two-way S/W firewalled connections
Problematic
- ❑ Portable media – sneakernet
“Does not cut it” – NIST standards, federal regulations

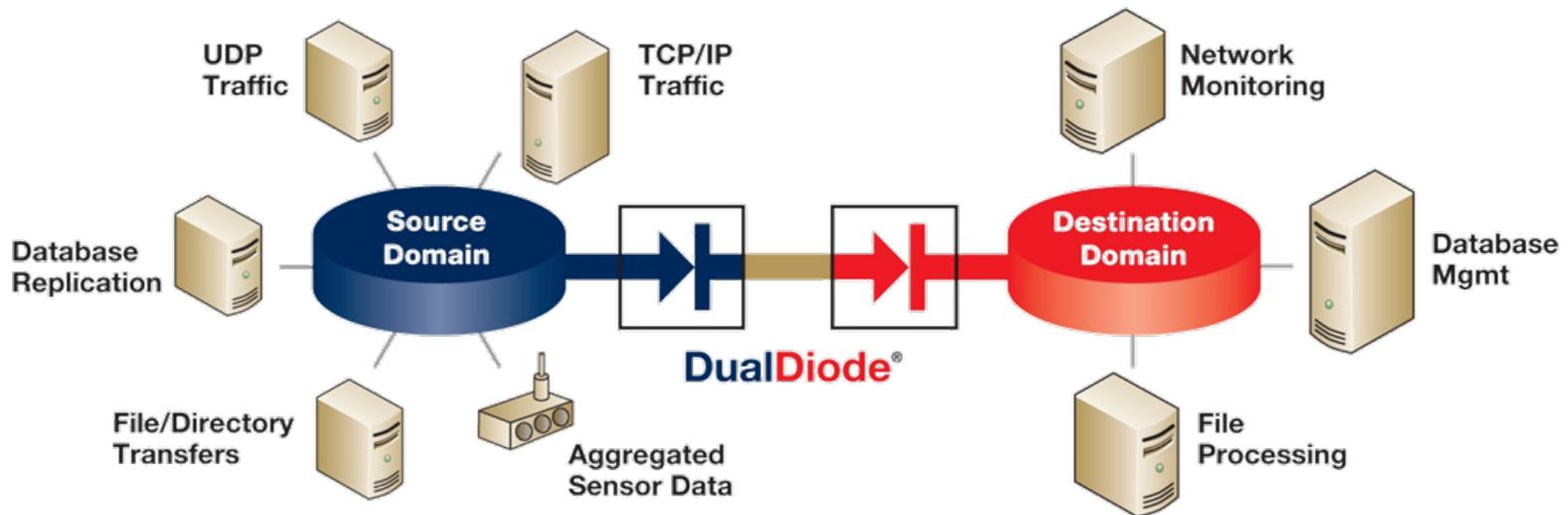


Critical Infrastructure Cybersecurity Requirements & Compliance

- ❑ NERC-CIP
- ❑ NIST network security controls
- ❑ National Information Assurance Partnership -- NSA



Operational Needs



Level-4 to levels 3/2 data "push"

Level 4 Network-to-Business Networks Data Flow

- ❑ Control system / historian / SCADA vendors provide native TCP/UDP/file transport to security perimeter boundary
Native Vendor Service **NVS** (e.g., InStep eDNA UDP interface)

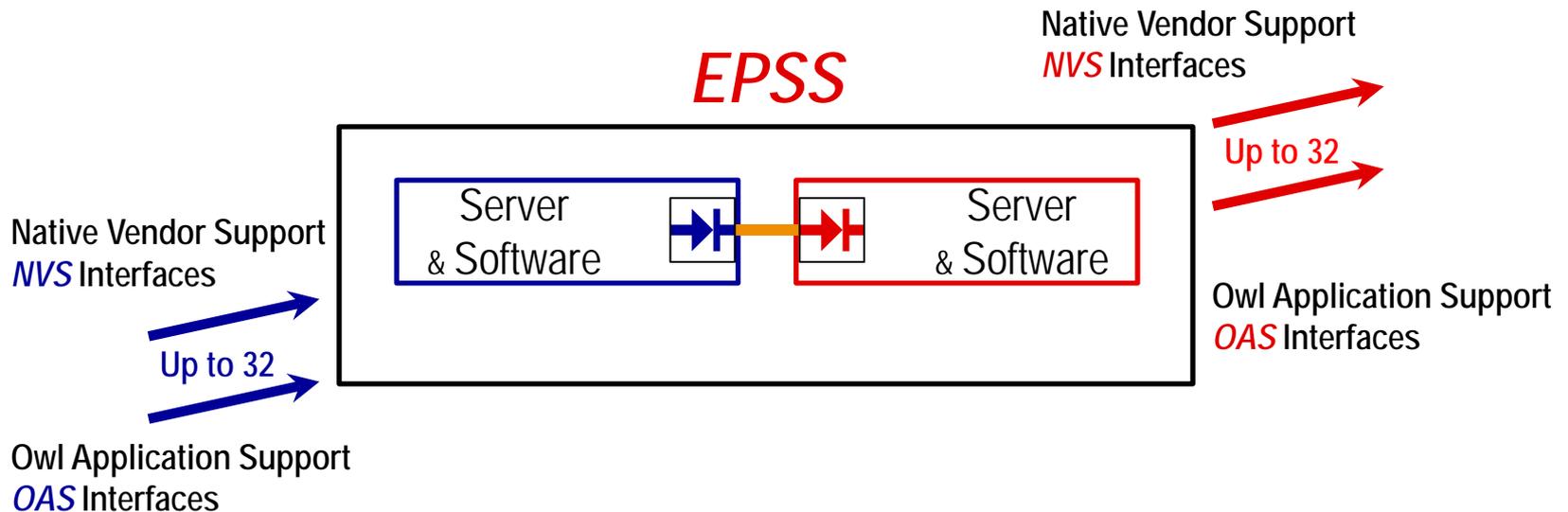
OR

- ❑ Transport service (or operator) develops transport “connectors” to bring data to perimeter boundary
Owl Application Service **OAS** (e.g., OSIsoft PI System)

-
- ❑ Network service provider transports data across security perimeter to control system/historian/SCADA apps



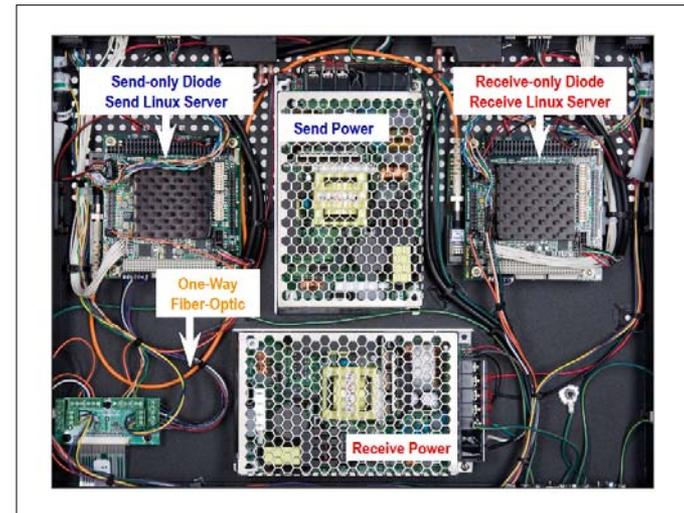
Electronic Perimeter Security Solution



Electronic Perimeter Security Solution



EPSS Internal



Across the Secure IT Perimeter

Level-4 Segregated  Levels-3/2

Information Confidentiality – non-routable “protocol break”
& absolute one-way transfer

Information Integrity – content management & data filtering

Information Availability – locked-down operating systems

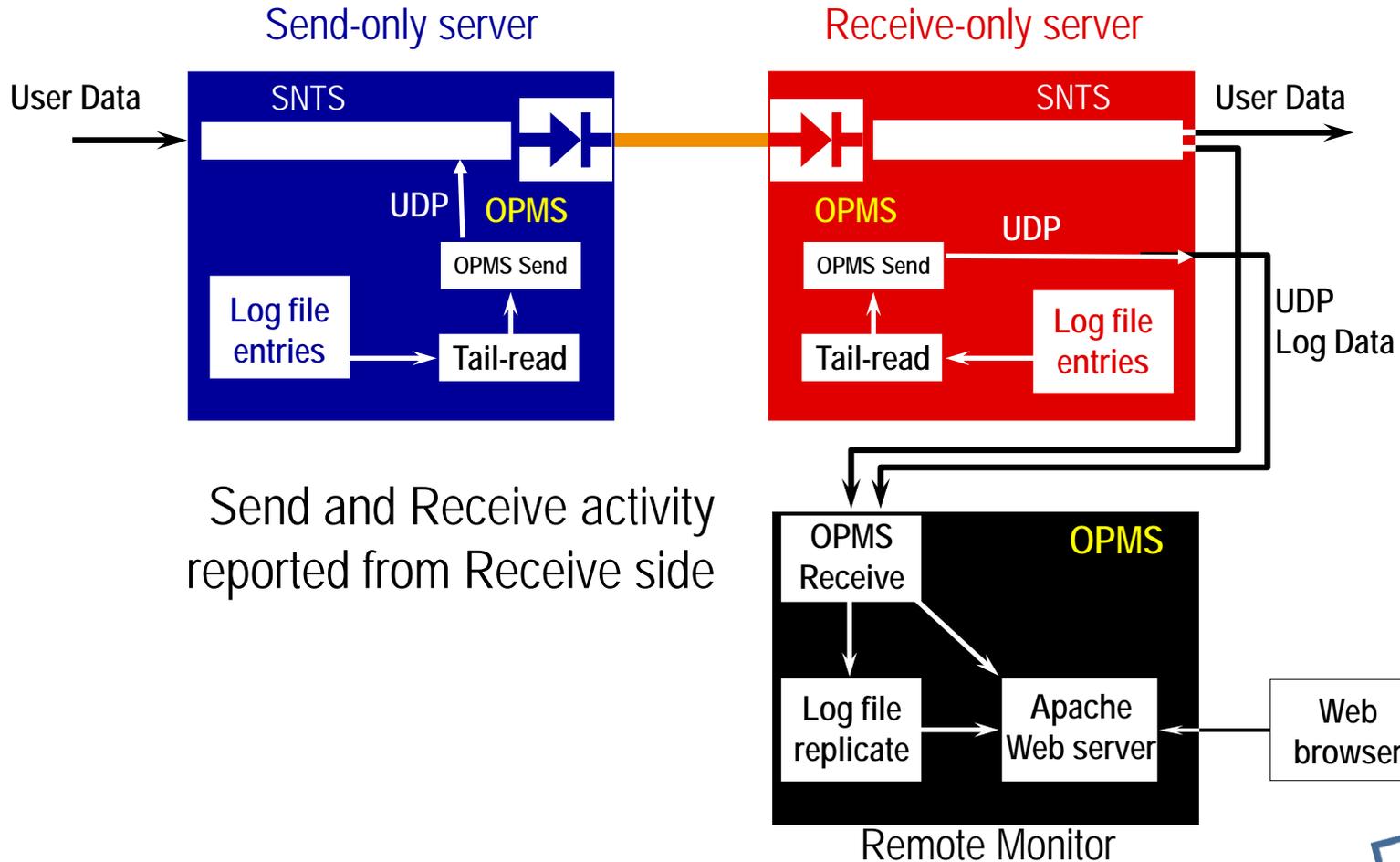


OPMS -- Owl Performance Management Service

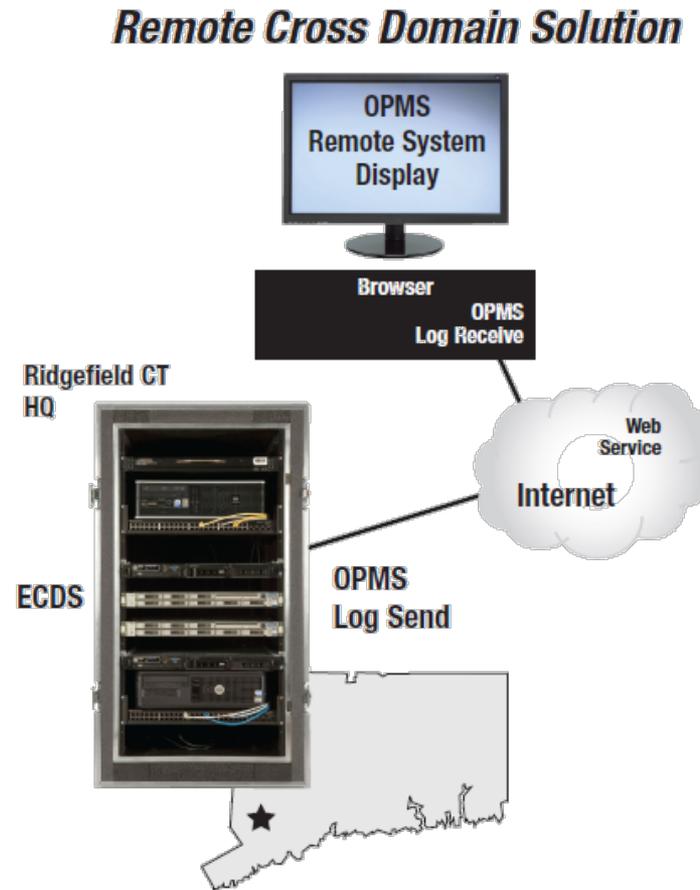
- ❑ Global View of Monitored Systems Status
 - Monitor individual crossing, and multiple crossings
 - Status of individual data transfers
- ❑ Log File Monitor of Owl Applications
 - Errors noted from send-only & receive-only log files
- ❑ Application Support
 - All Owl applications
 - Custom application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



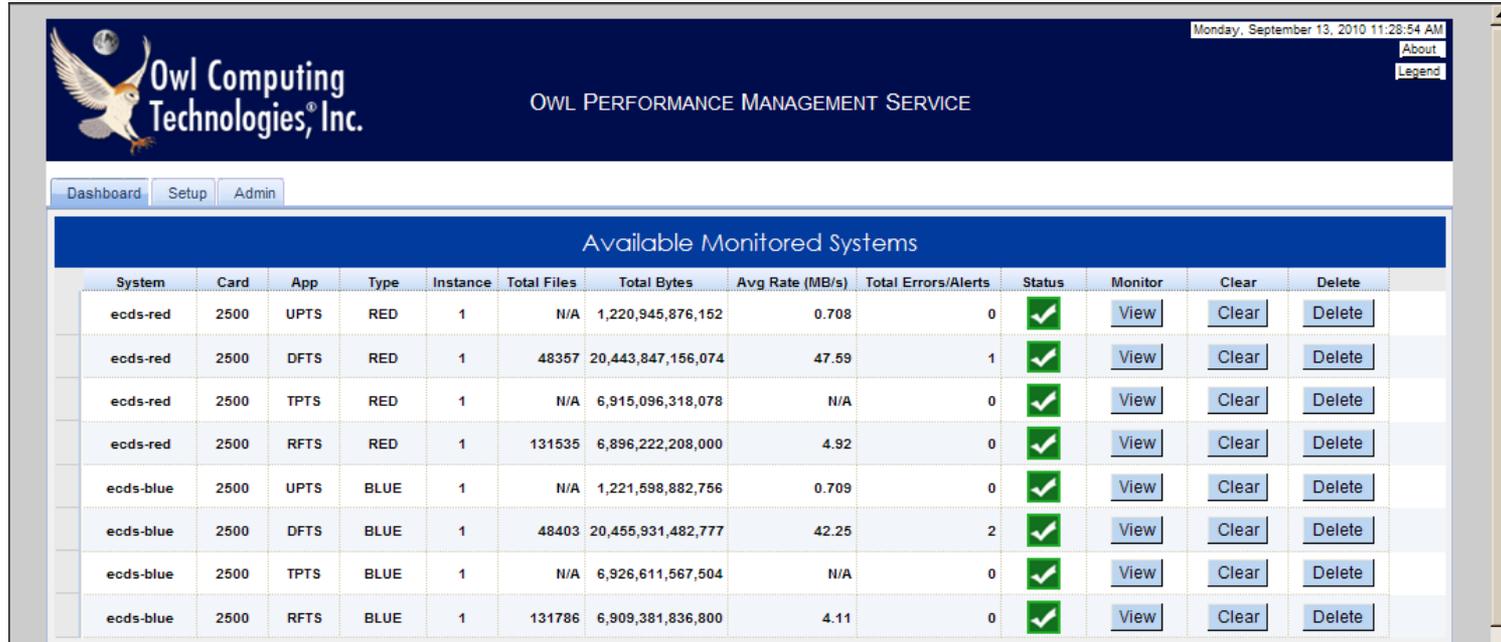
OPMS Sample Configuration



OPMS Dashboard View



OPMS Dashboard View



Monday, September 13, 2010 11:28:54 AM
About
Legend

Owl Computing Technologies, Inc.
OWL PERFORMANCE MANAGEMENT SERVICE

Dashboard Setup Admin

Available Monitored Systems

System	Card	App	Type	Instance	Total Files	Total Bytes	Avg Rate (MB/s)	Total Errors/Alerts	Status	Monitor	Clear	Delete
ecds-red	2500	UPTS	RED	1	N/A	1,220,945,876,152	0.708	0	✓	View	Clear	Delete
ecds-red	2500	DFTS	RED	1	48357	20,443,847,156,074	47.59	1	✓	View	Clear	Delete
ecds-red	2500	TPTS	RED	1	N/A	6,915,096,318,078	N/A	0	✓	View	Clear	Delete
ecds-red	2500	RFTS	RED	1	131535	6,896,222,208,000	4.92	0	✓	View	Clear	Delete
ecds-blue	2500	UPTS	BLUE	1	N/A	1,221,598,882,756	0.709	0	✓	View	Clear	Delete
ecds-blue	2500	DFTS	BLUE	1	48403	20,455,931,482,777	42.25	2	✓	View	Clear	Delete
ecds-blue	2500	TPTS	BLUE	1	N/A	6,926,611,567,504	N/A	0	✓	View	Clear	Delete
ecds-blue	2500	RFTS	BLUE	1	131786	6,909,381,836,800	4.11	0	✓	View	Clear	Delete

- ❑ Overview of monitored systems
- ❑ Summary of performance data
- ❑ Red/Green status indicator
- ❑ Ability to select individual system



Summary

- ❑ ICS cybersecurity needs growing in capacity reqs & in varieties of data types
- ❑ Greater institutional pressure to comply with standards & requirements
- ❑ Legacy networks CAN be cybersec-modified with relative ease
- ❑ Need for cost-effective monitoring follows with successful deployment



Information Assurance

Secured by Owl®

Thank you

rmraz@owlcti.com
jmenoher@owlcti.com
www.owlcti.com

