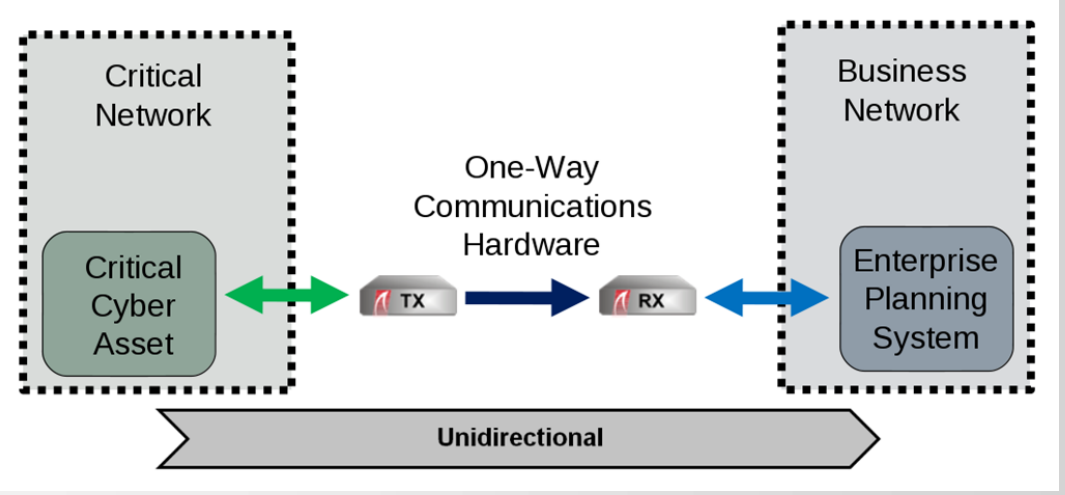
WATERFALL
One Way to Connect

One-way Myths: Common Misperceptions about Unidirectional Gateways

Lior Frenkel, Co-Founder and CEO
Waterfall Security Solutions

Unidirectional Gateways

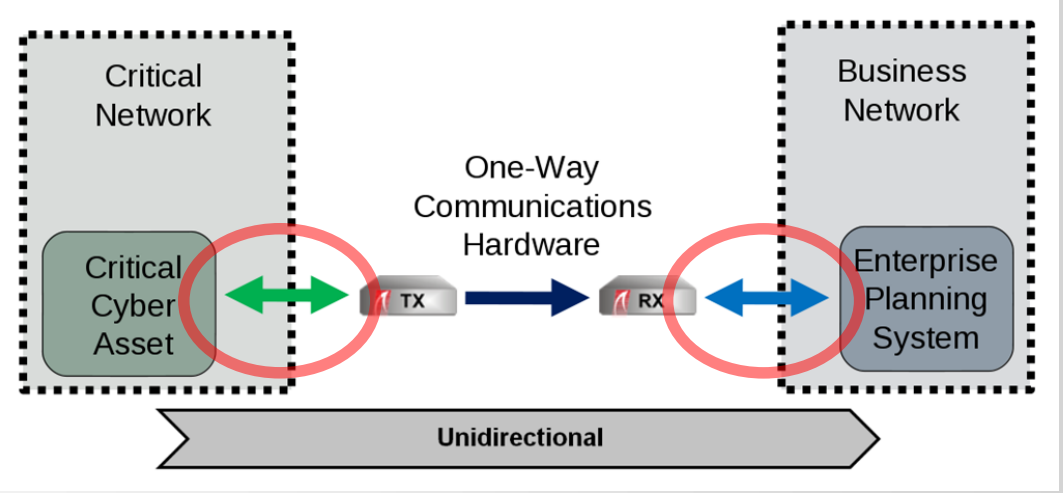
- Hardware protection: one-way fibre-optic link
- Transmitter = laser, Receiver = photocell
- Strong security: absolute protection from external network access
- Transmitter gathers data using bidirectional protocols
- Receiver publishes data using bidirectional protocols
- No zero-day vulnerability
- can turn photocell into laser
- Deployed routinely in many
- industries



Many misconceptions...

Myth: I can't use gateways – I use bi-directional protocols

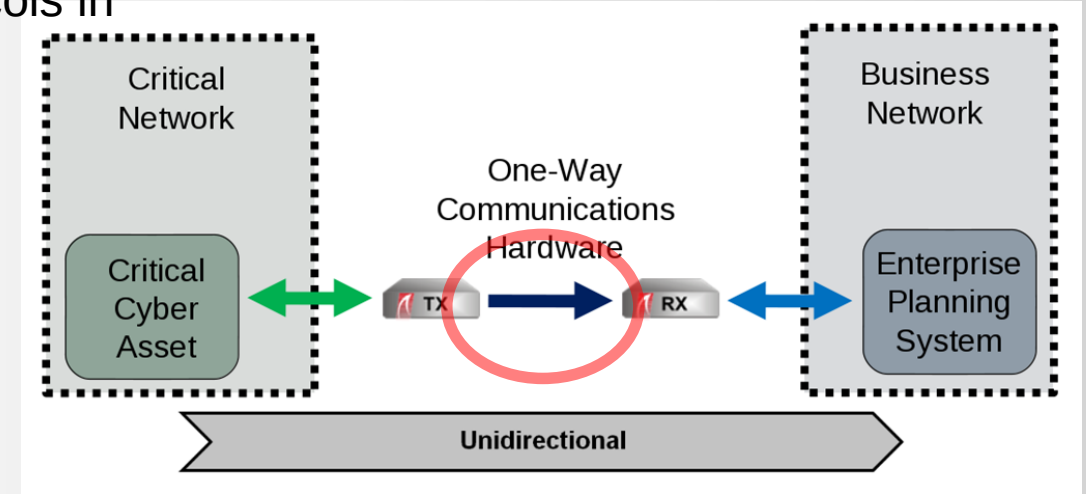
- Most often ***real information flow*** is unidirectional, even if protocol is bidirectional
  - Unidirectional Gateways offer strong security
- Identify information you need moved to the business network
  - Gather information using conventional protocols
  - Send across one-way link
  - Publish information using conventional protocols
- Receiver emulates original data
- sources
- No changes needed to source
- or destination applications



You can use Gateways

Myth: Emulating 2-Way Protocol Compromises Unidirectionality

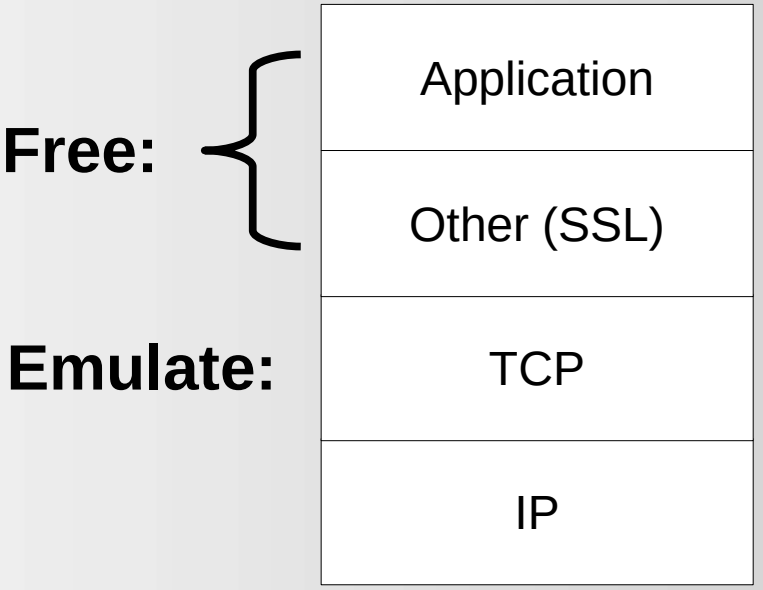
- Hardware only sends light in one direction – fundamentally unidirectional
- Conventional bi-directional protocols used only on transmitting network and receiving network
- Lesson: we are not ***emulating*** 2-way protocols.
  - ***Configurable Application*** gathers data on source network and publishes it in destination network
  - Application ***uses*** 2-way protocols in
  - transmitter and receiver
  - Application sends data over
  - one-way protocol



Application, not Emulation

Myth: OK, I'm Convinced – Let's Emulate TCP and We're Done!

- Vast majority of network protocols ride on TCP
- Emulate TCP and we get those other protocols for “free”
- Emulate UDP as well and we are done!



Myth: OK, I'm Convinced – Let's Emulate TCP and We're Done!

- Vast majority of network protocols ride on TCP
- Emulate TCP and we get those other protocols for “free”
- Emulate UDP as well and we are done!

Query/Response/Acknowledge:

Query/Response/Acknowledge:

Emulate:

Application
Other (SSL)
TCP
IP

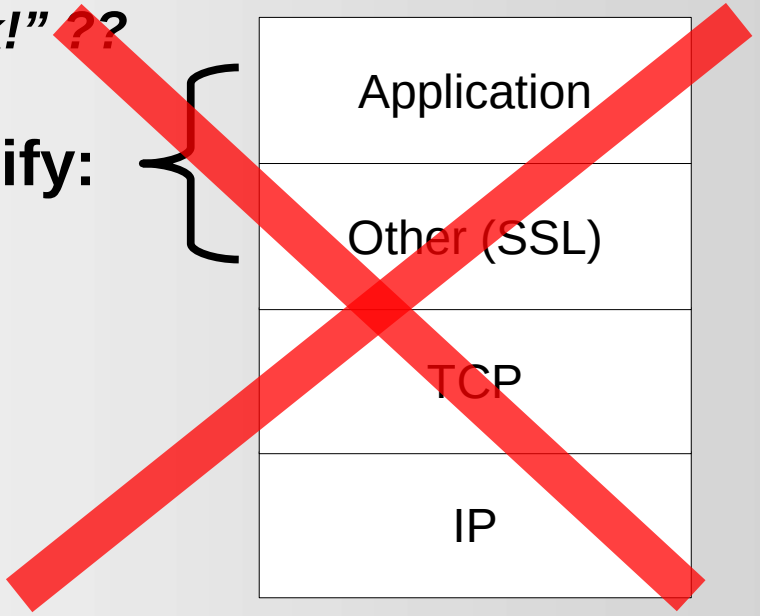
Myth: No, I Really Think I Can Do It!

- I have source code for application layer – rip out queries / responses / acks
- And isn't syslog already unidirectional UDP?

And When Something Goes Wrong?

- Congestion problems, synchronization problems, permission problems
- ***"Error: I just dropped a packet. Good luck!" ??***
- Applications know what they want to
- accomplish
- Applications emit meaningful error
- messages when things go wrong
- Things always go wrong in complex systems

Modify:



Application, not Emulation

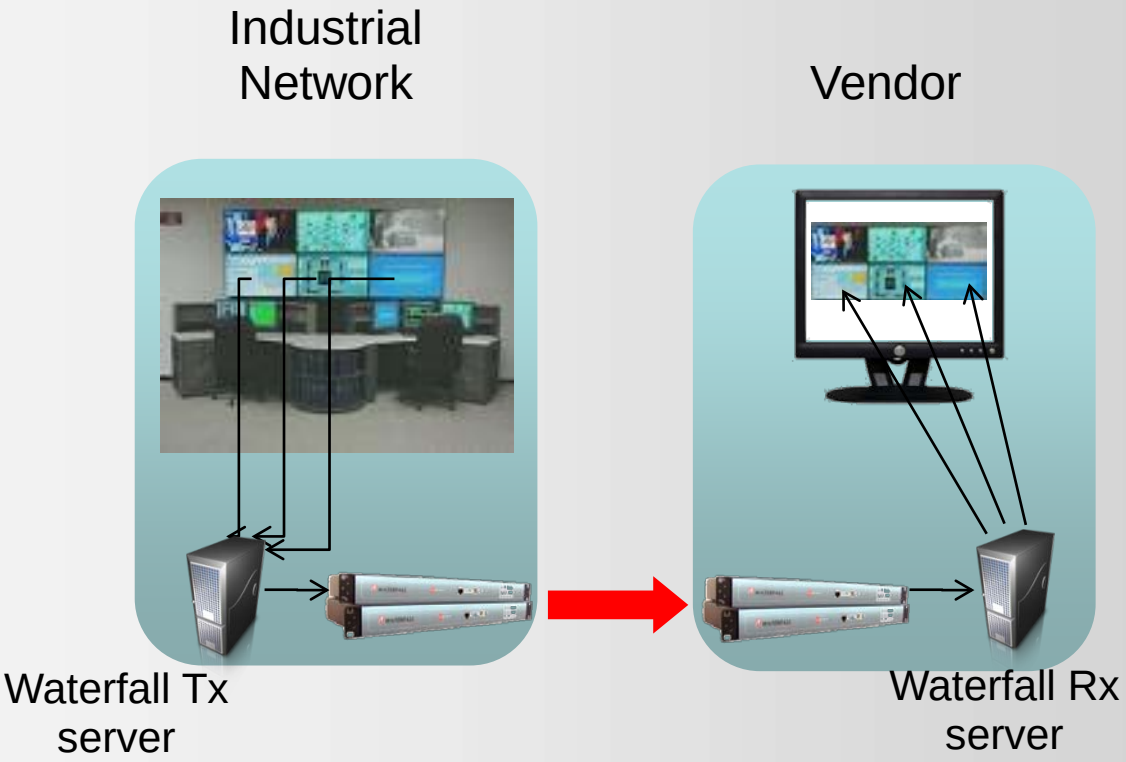
Myth: Dropped Packets?? Without Acks / Nacks / Retransmissions, One-Way Communications Are Unreliable

- Anything is unreliable if enough components fail at the same time
- Serious Engineering:
  - High signal quality
  - High throughput
  - Low latency
  - Support for throughput-constrained environments
  - High availability / redundant links
  - All data sent twice
  - Buffer everything, detect failures, raise alerts
  - Very rare: request manual intervention to trigger retransmission

High Quality Communications

Myth: Unidirectional Remote Support Is Impossible

- “Remote Screen View” = real time view of protected computer screens
- View only – no mouse movement, no commands



Myth: One-way Gateways Are Only For Nuclear Generation

- Many kinds of firms use gateways, especially fossil generation and water utilities
- Many businesses want strong security
  - Absolute protection from network attacks
  - Protection from configuration errors and omissions
- Delay in deployment of Unidirectional Gateways increases costs and risks

Myth: One-way Cost "Too Much" to Configure and Maintain

- Unidirectional Gateways reduce compliance costs:
  - No remote access / access denied logs to review and audit
  - Less complex perimeter protections – lower vulnerability assessment and audit costs
  - Less documentation, fewer procedures to follow – the technology continues to secure your network even if mistakes are made occasionally.
- Whitepapers are available detailing how costs are reduced for NIST 800-53 and NERC-CIP.

Many Connectors

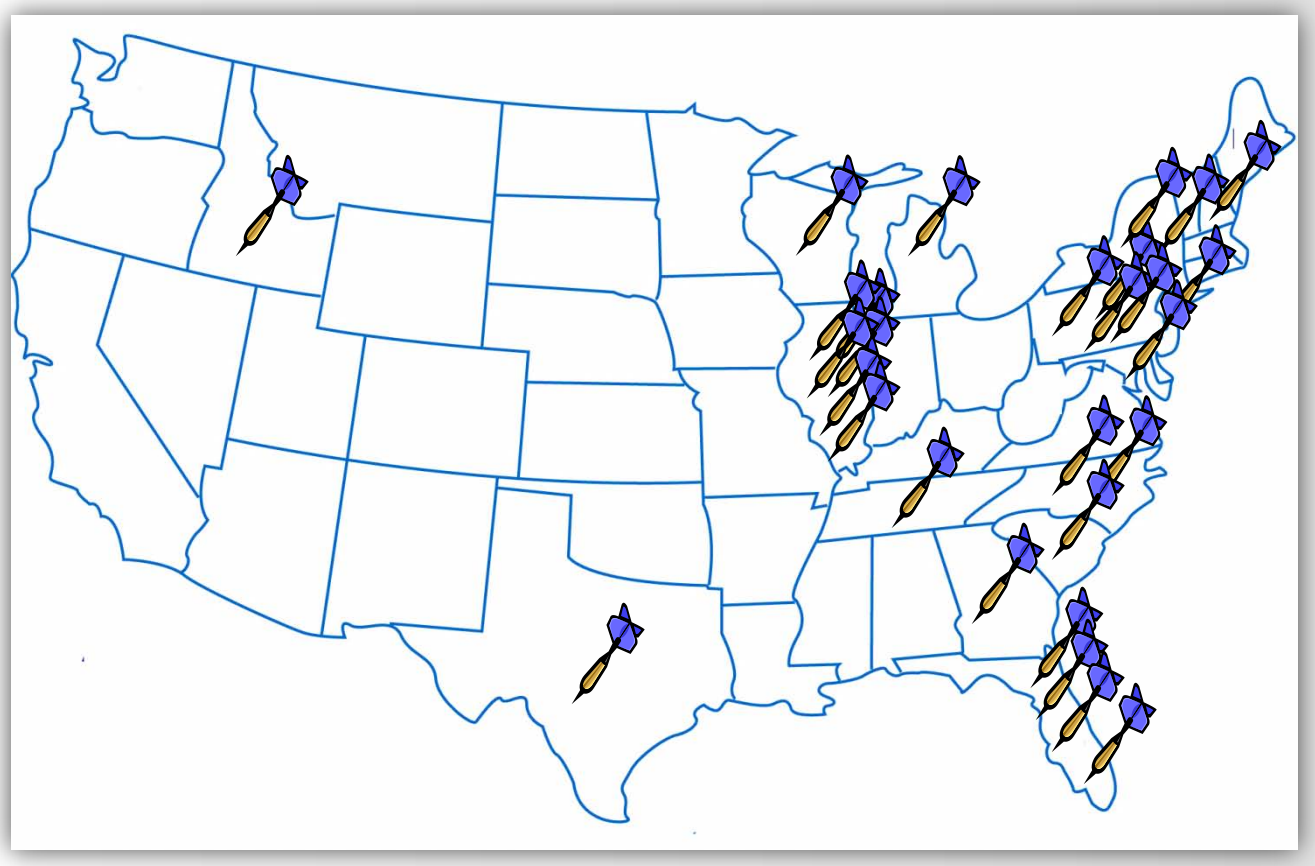
- **Industrial Applications/Historians**
  - OSISoft PI, GE iHistorian, GE iFIX, Scientech
  - R*Time, Instep eDNA, GE OSM, Siemens
  - WinCC, SINAUT
- **IT Monitoring Applications**
  - Log Transfer, SNMP, SYSLOG
  - CA Unicenter, CA SIM, HP OpenView
  - Matrikon Alert Manager
- **File/Folder Mirroring**
  - Folder, tree mirroring, remote folders (CIFS)
  - FTP/FTFP/SFTP/TFPS/RCP
- **Remote Screen View™**
- **Industrial Protocols**
  - Modbus, OPC (DA, HDA, A&&E)
  - DNP3, ICCP
- **Other Connectors**
  - UDP, TCP/IP
  - NTP, Multicast Ethernet
  - Video/Audio stream transfer
  - Mail server/mail box replication
  - IBM Websphere MQ series
  - Antivirus updater, patch (WSUS) updater
  - Remote Print server

Waterfall in North America

- Department of Homeland Security selected Waterfall's technology for its National Cyber Security Test-bed
- US Patent covering SCADA/Control Networks security using Unidirectional Gateways
- Passed cyber security assessment by Idaho National Laboratories
- Pike Research named Waterfall as key player in the cyber security market
- Strategic partnership and cooperation with: OSIsoft, GE, Siemens, and many other major industrial vendors
- Large installed base in the industrial critical infrastructure, in the US and Canada

Waterfall implementations in the US

Over 15 states, more than 28 operational sites



Looking Forward

- Unidirectional Gateways are a mature technology
- Gateways work in many more environments than are evident at first glance
- Unidirectional Gateways offer strong security:
  - Absolute protection from attacks by insiders and remote adversaries via enterprise network
  - Even firewalls have zero-day vulnerabilities: CISCO just published a long list of firewall and router firmware revisions.
  - Hardware has no zero-days – no malware can turn a photocell into a laser
- New advanced threats demand advanced protections