Oil and Gas Infrastructure Resilience

Al Rivero, PE

ANG Consulting, LLC

CREDC PACIFIC Northwest Industry Workshop

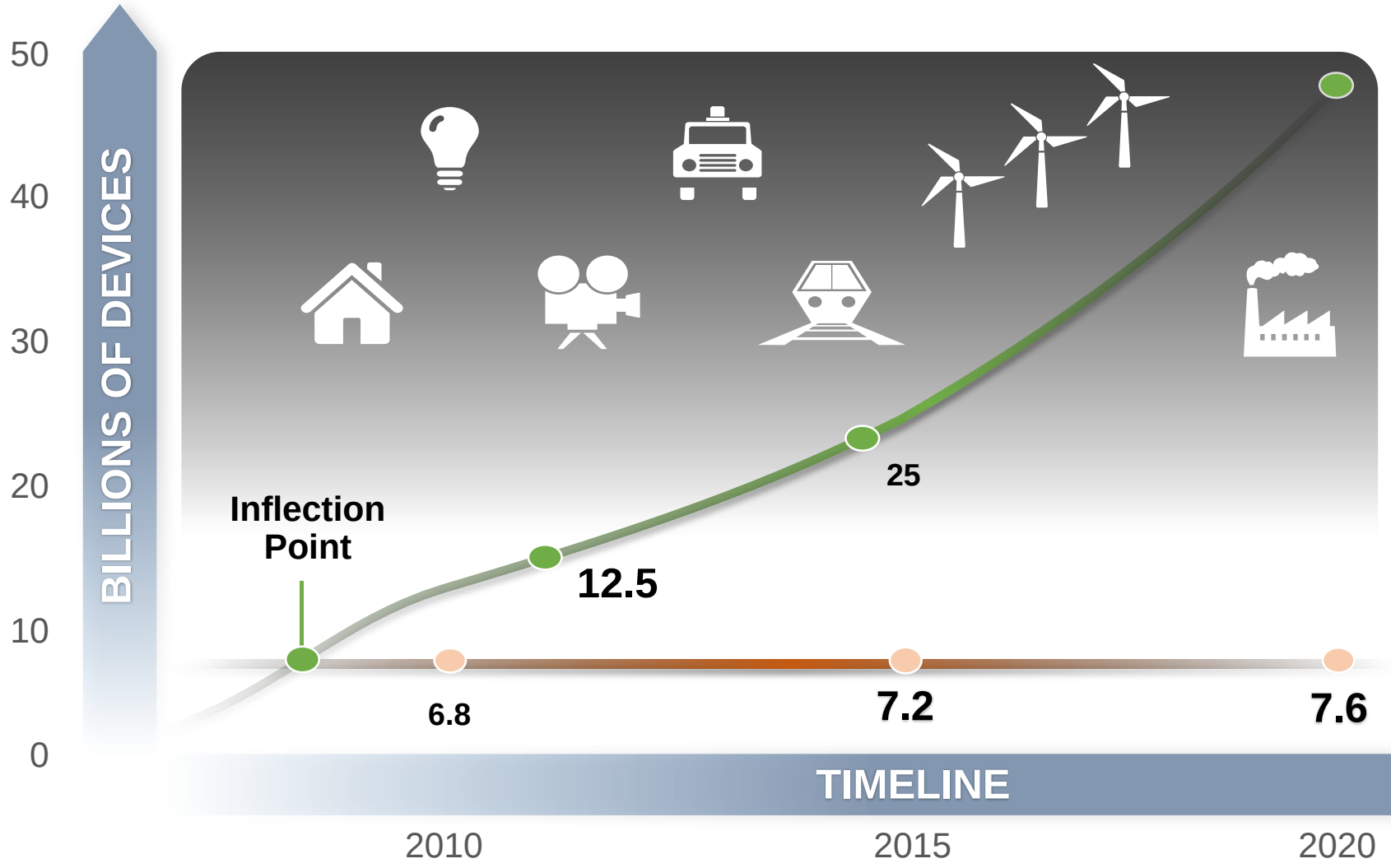
Cybersecurity Research Needs - an Energy Sector Perspective

November 28th – 29th 2017

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security | cred-c.org

IoT: Connecting the Unconnected



50 Billion

"Smart Objects"

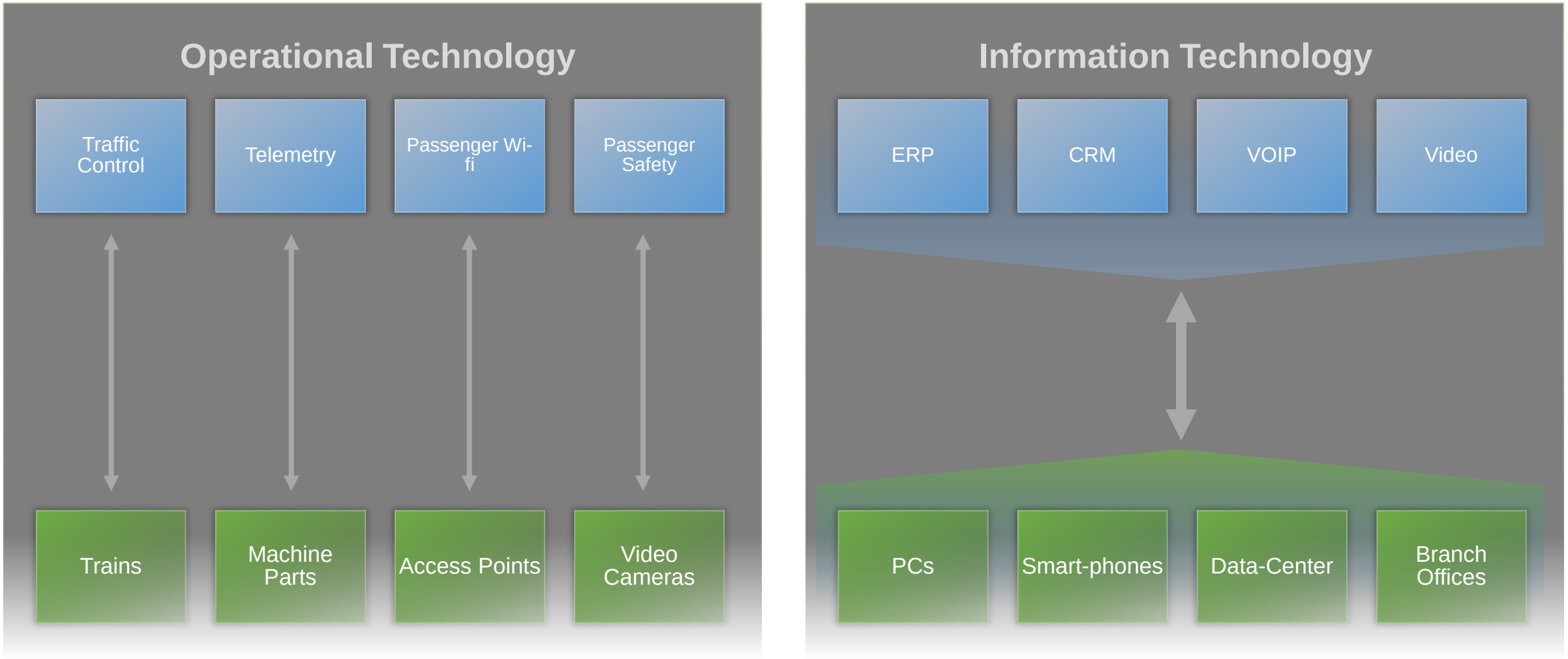
Rapid Adoption Rate of Digital Infrastructure:

5X Faster

Than Electricity and Telephony

World Population

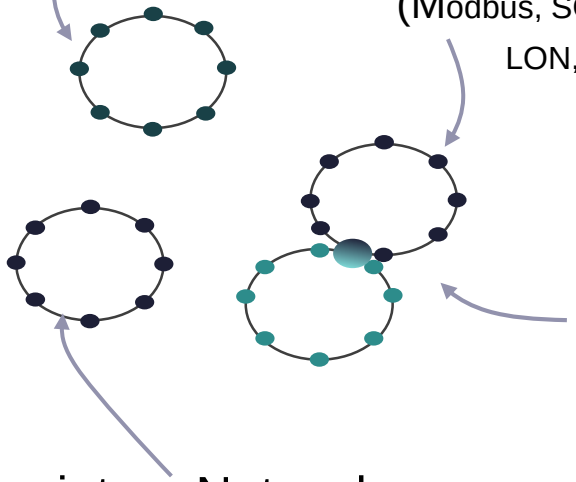
Converged, Managed Network



Shift in Architectural Philosophy

Closed Systems
(Little external interaction)

Various Protocols
(Modbus, SCADA, BACnet, LON, HART)

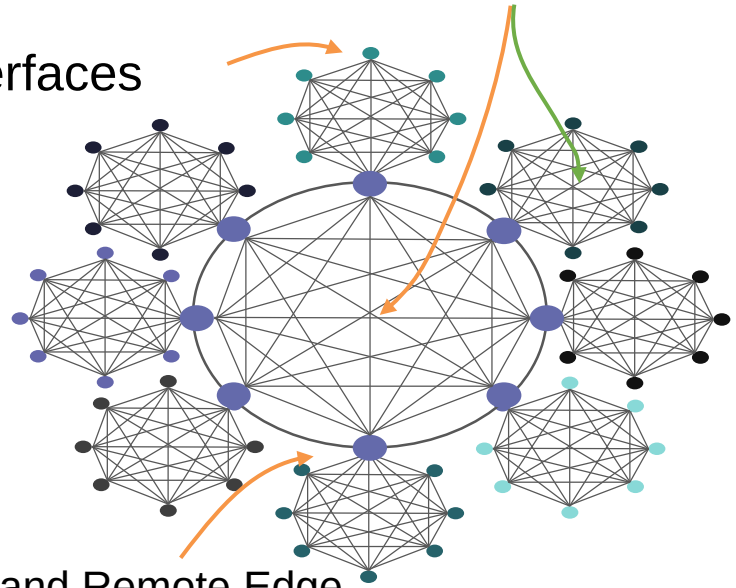


Protocol Gateways
(Inherently complex, inefficient and fragmented networks)

Proprietary Networks
(Usually layer 2 based)

Standardized Networks
(IP Based/ISO Stack)

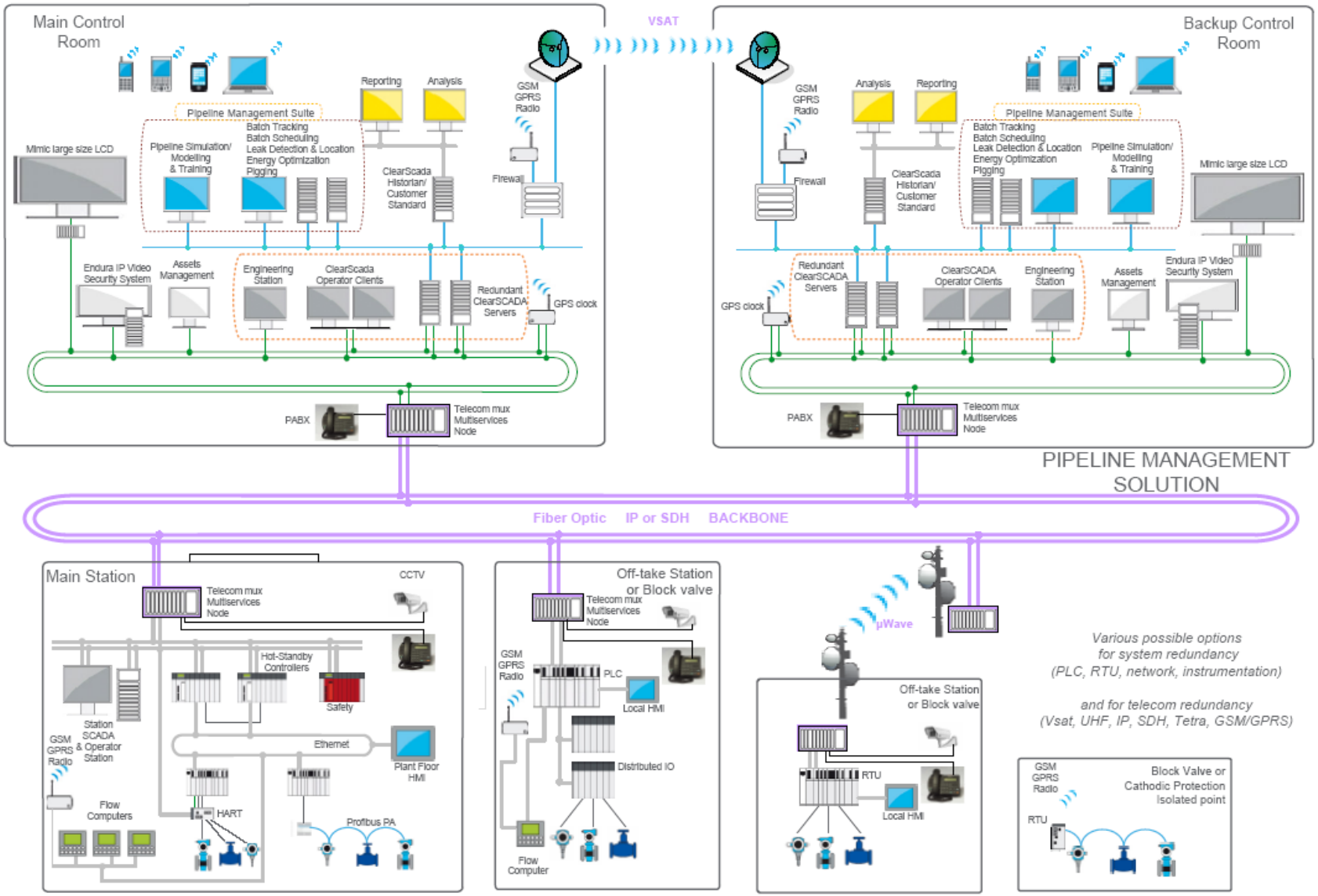
Standardized Interfaces
(Wireless/Wired)



Geographically Distributed and Remote Edge Systems
(support for IP and non-IP)

From → **To**

Typical Oil and Gas Monitoring



Client Survey 21 Respondents

- Gaps in Technology
  - Slow to respond to threats
  - White Listing has many gaps in Industrial Networks
  - Struggling between White Listing and Black Listing
  - Current OS Environment Complexity (MS 72% and Lunix/Unix 28%)
- What Keeps you awake at night
  - 3rd Party connections (Vendors, Contractors, Maintenance)
  - Field Wireless Connection
  - Site Access (Controlling field access, Monitoring facilities, Drones becoming a major issue*)
  - MS Only AD Managed by third party

Client Survey 21 Respondents

- Needs for Closing the Gaps
  - Real White Listing solutions for IoT (Backend Network)
  - Real time scanning and blocking of 3rd party connections and threats
  - Faster Black Listing ID and role out capabilities
  - Skinny MS OS*, Lower patching
- Would industry be whiling to share in cost to develop
  - Most industry segments feel they invest in research through there, funded industry partners and vendors. But the progress has been slow
- What do you feel is needed to expedite the research
  - Most feel they have done everything possible except the trusted insider, not sure how to manage this threat.
  - No known real threat – not personal

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

http://cred-c.org

@credcresearch

facebook.com/credcresearch/

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security