

Are converged OT/IT Transport networks immune from attack?

2016 NYS Cyber Security Conference

June 8-9, 2016



www.QEDNATIONAL.com

ARUP

Critical Infrastructure

- ▶ Chemical
- ▶ Commercial Facilities
- ▶ Communications
- ▶ Critical Manufacturing
- ▶ Dams
- ▶ Defense Industrial Base
- ▶ Emergency Services
- ▶ Information Technology
- ▶ Food & Agriculture
- ▶ Government Facilities
- ▶ Healthcare & Public Health
- ▶ **Transportation**
- ▶ Water & Wastewater
- ▶ Nuclear Reactors, Materials & Waste
- ▶ Financial Services
- ▶ Energy

*US Department of Homeland Security,
December 2003*

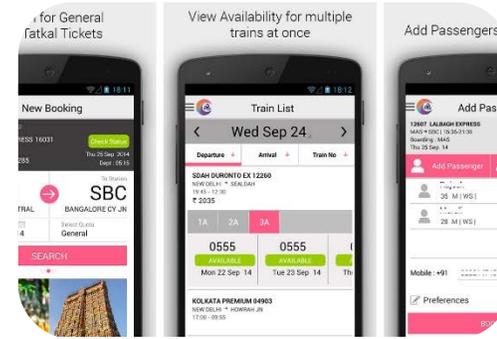
Current and Emerging Railway Services



Electronic Ticketing & Payment



WiFi



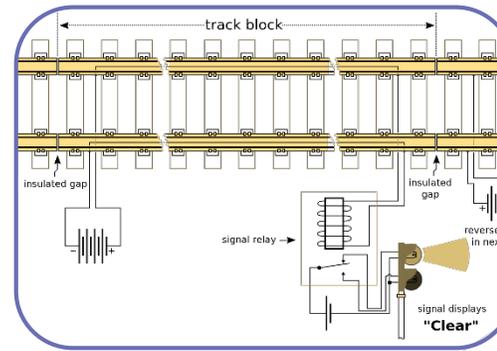
Intelligent Transport Services



Video Surveillance



Communication Based Train Control



Positive Train Control

Future - Urbanization

Population of the world's cities

Present Day	Projected for 2050
4.2 billion	7 billion

Demand for efficient and effective urban services will increase substantially.



Agenda

- ▶ Introduction
- ▶ Current Trends
- ▶ Transport Communication Systems
- ▶ Cyber Risk Management
- ▶ Questions & Answers



Presenters



Anthony Concolino
QED National

*Former Citi, Reuters
Systems Engineering
Product Management
IT/Risk Management*
aconcolino@qednational.com
212-481-6868x119



Ken Garmson
ARUP, Inc.

*Former UK Ministries
of Defense & Transport
Systems Engineering
Intelligent Transport*
ken.garmson@arup.com
212-897-1548



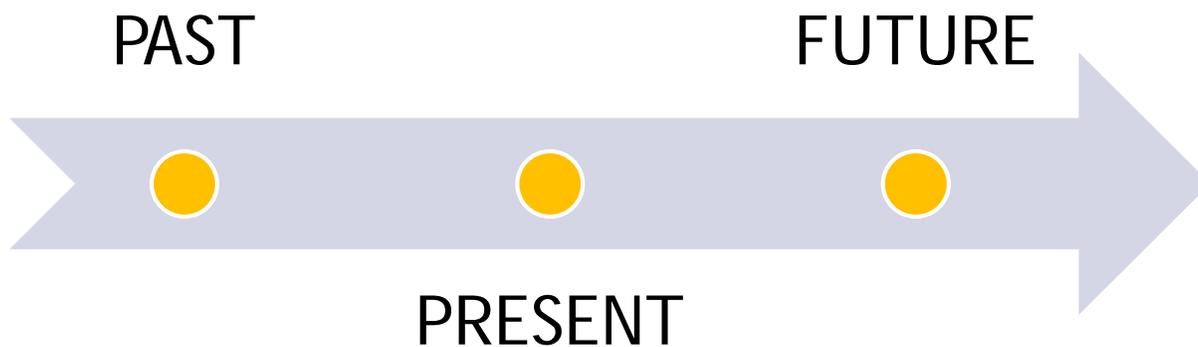
Russell Kiernan
QED National

*Former Merrill Lynch, Citi
Information Security
Risk Management
Enterprise Architecture*
rkiernan@qednational.com
212-481-6868x111

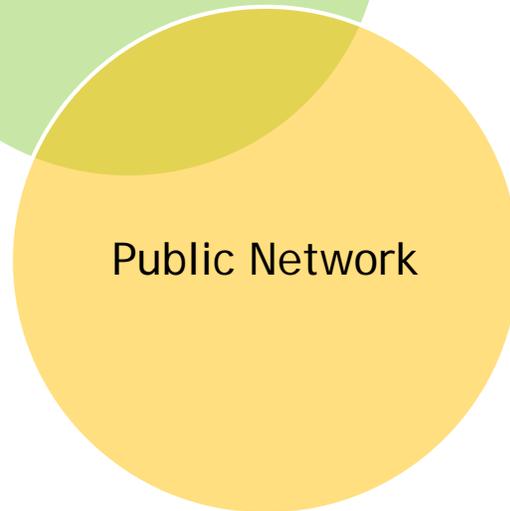
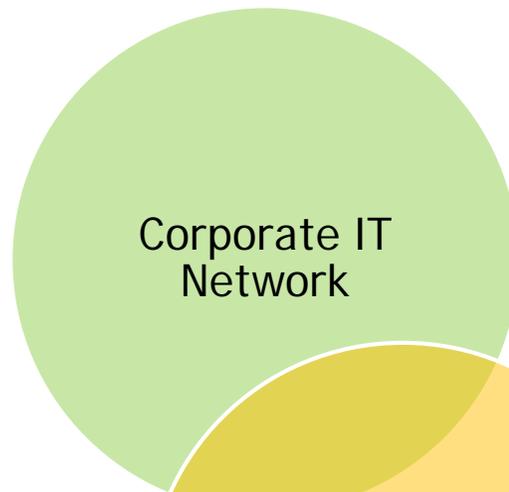
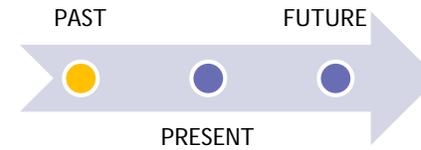
Transport Communication System Convergence



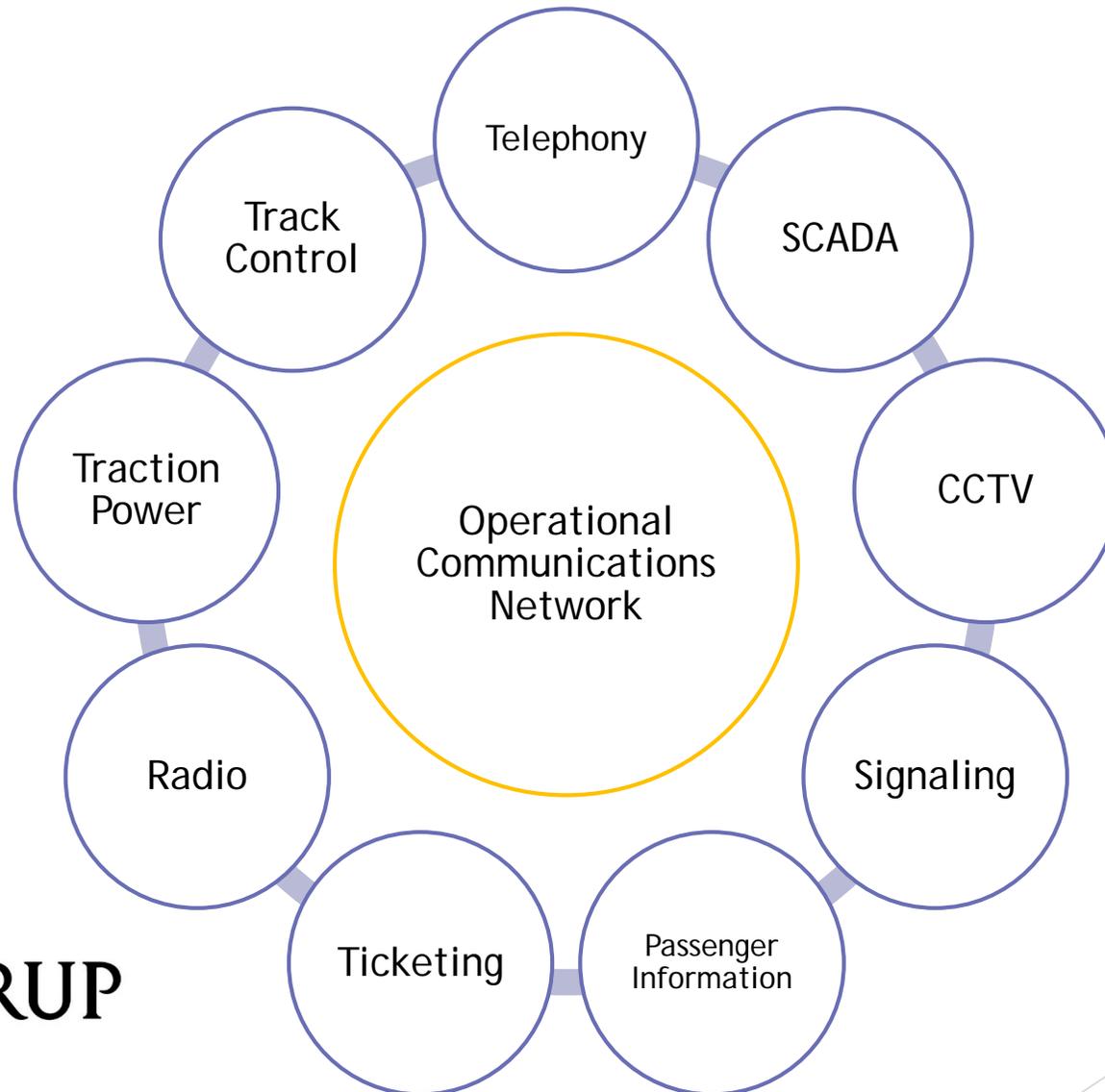
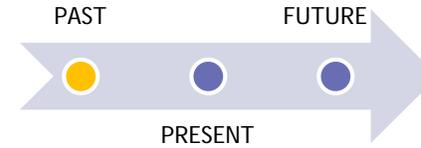
Ken Garmson



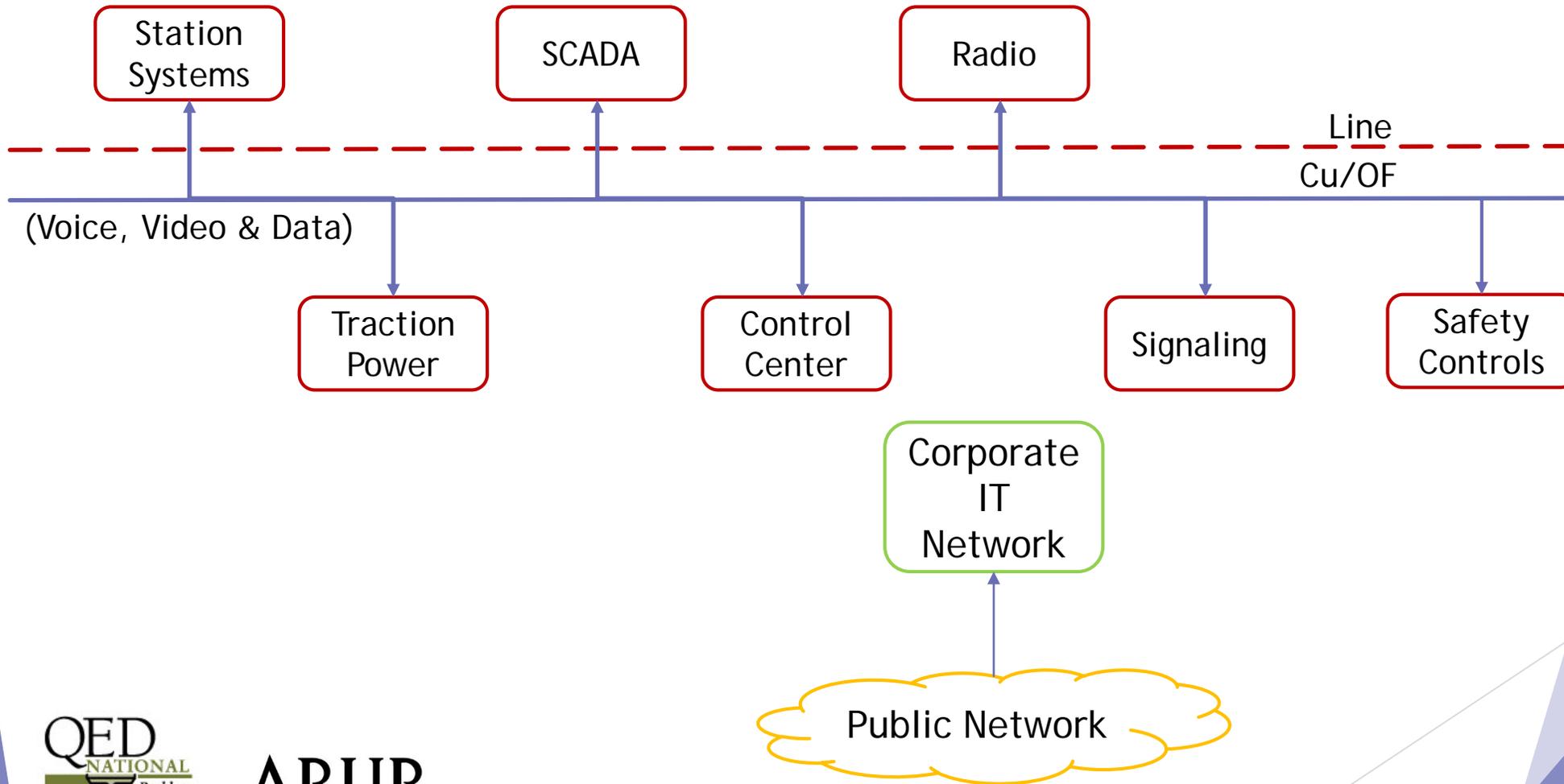
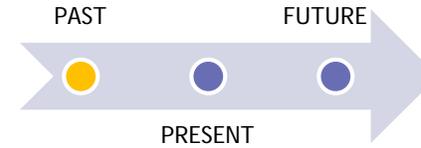
The Air Gap



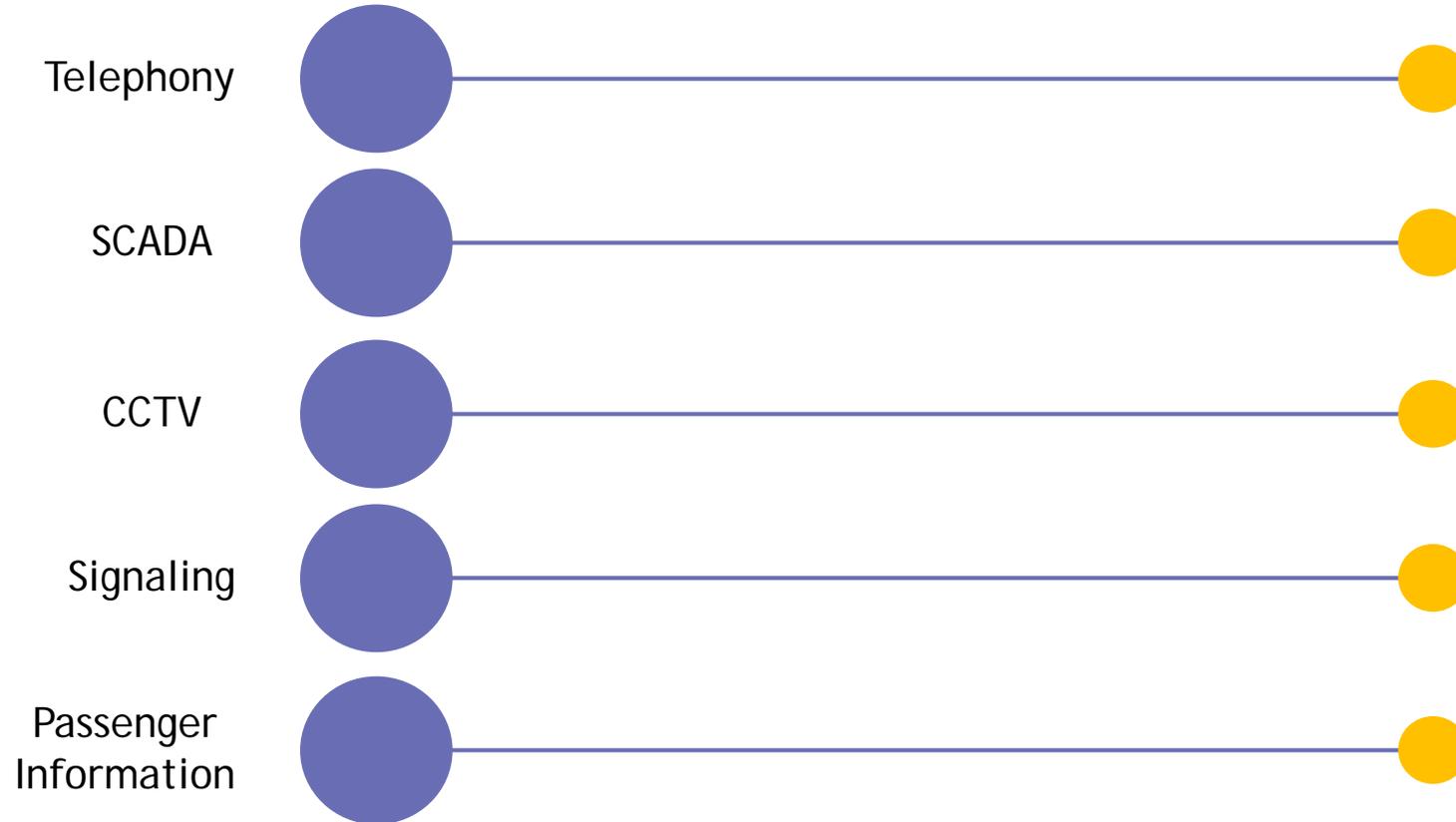
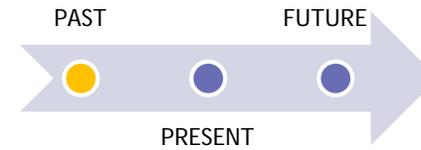
Operational Systems



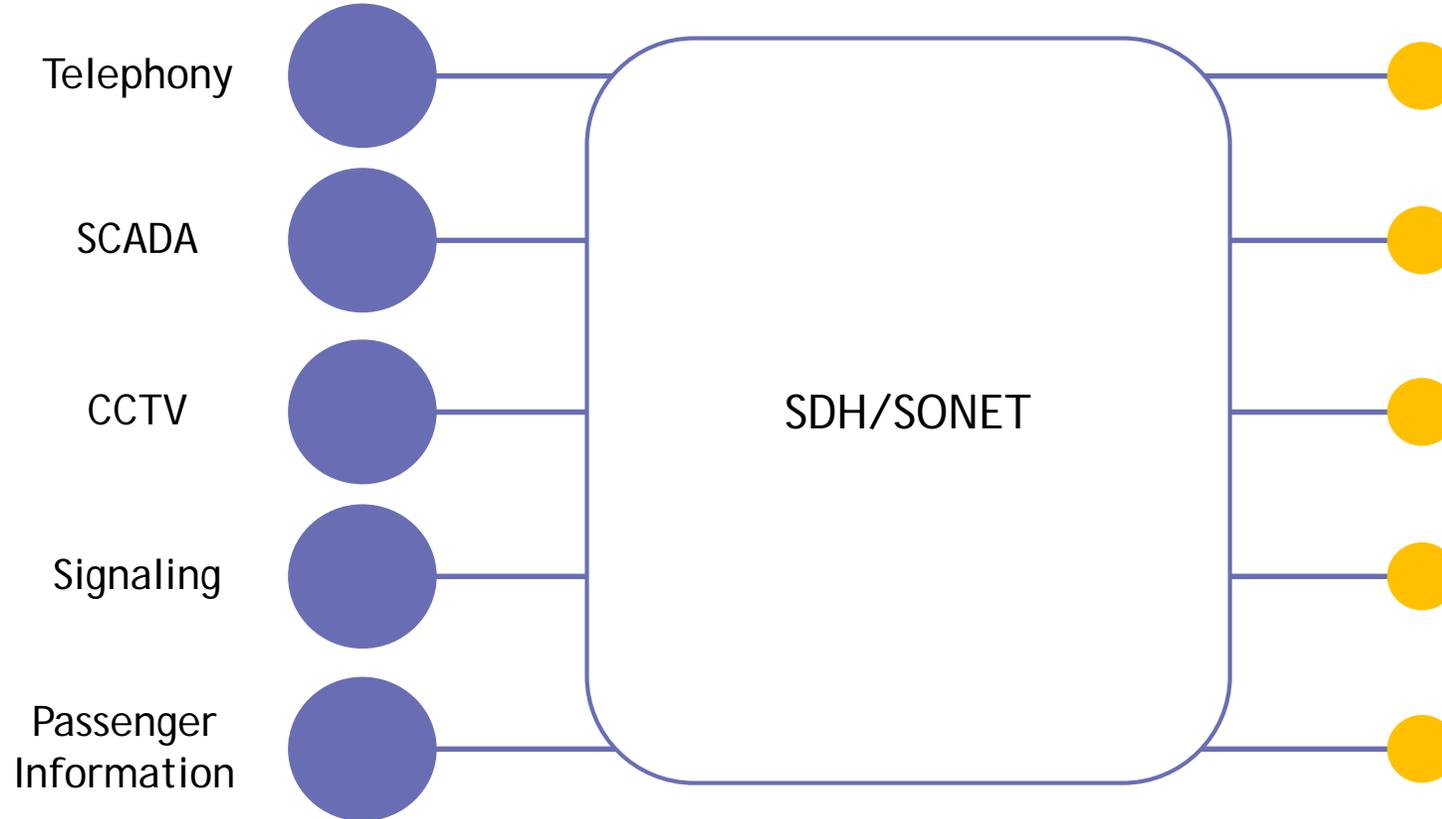
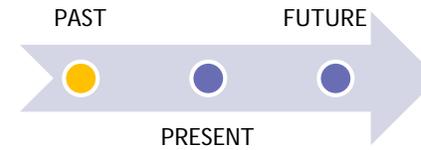
System Architecture



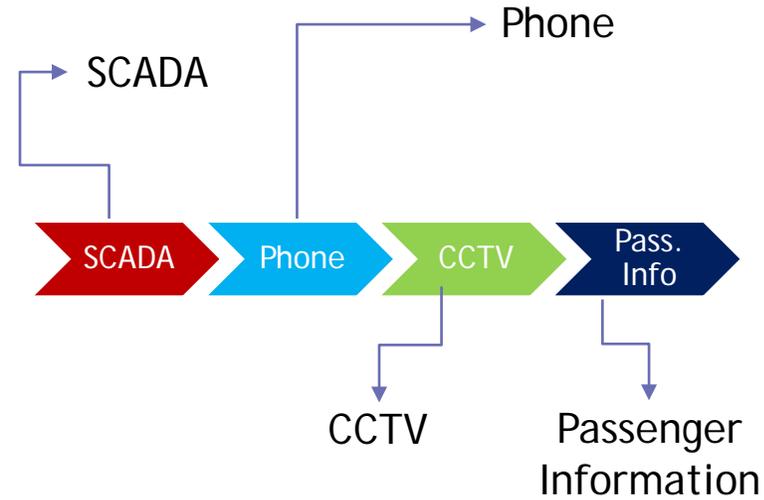
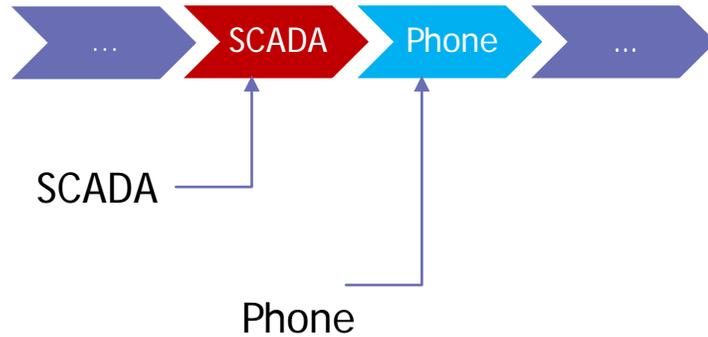
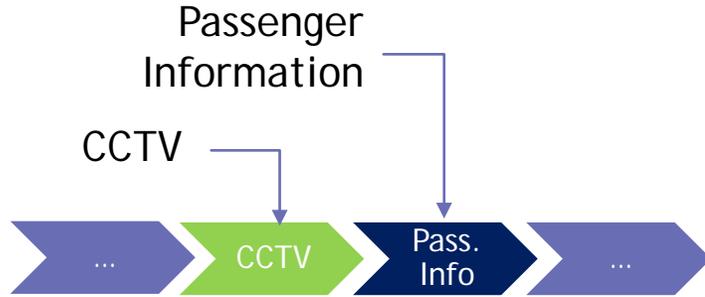
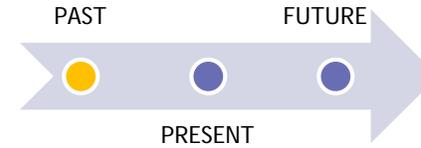
Systems Communication



SDH Communication Systems



SDH Transmission Paths



- Path Fixed (Direct Connection)
- Mixed Traffic Types



SDH



Virtual Container

Migration to IP based Communication Systems



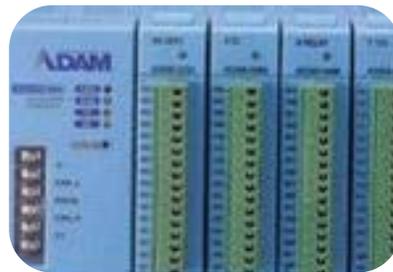
RS 485



Video



Audio

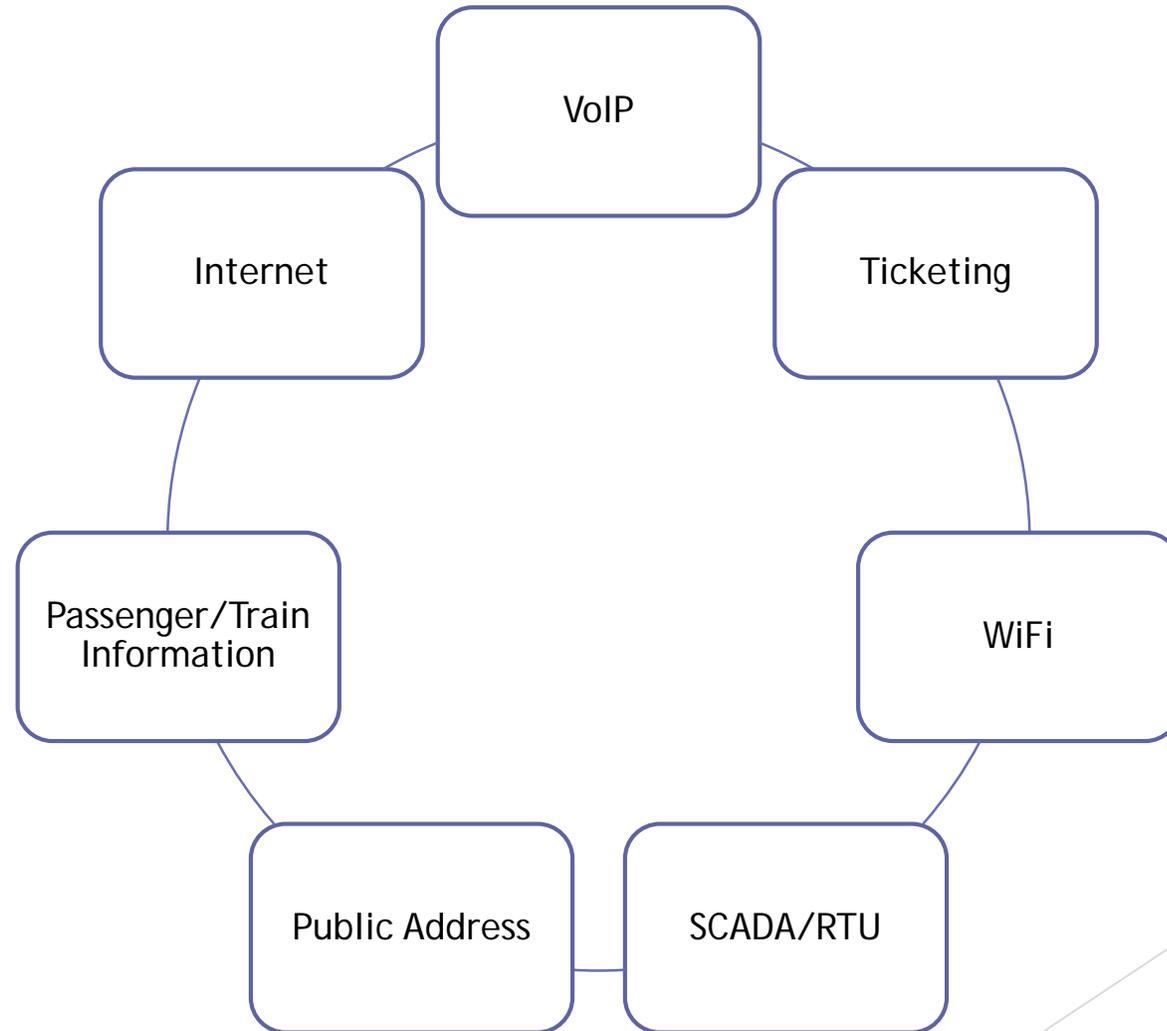


Modbus
SCADA RTU

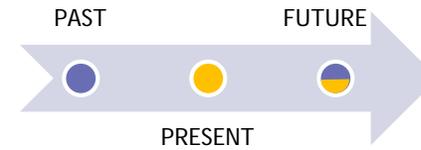


Legacy to IP
converter

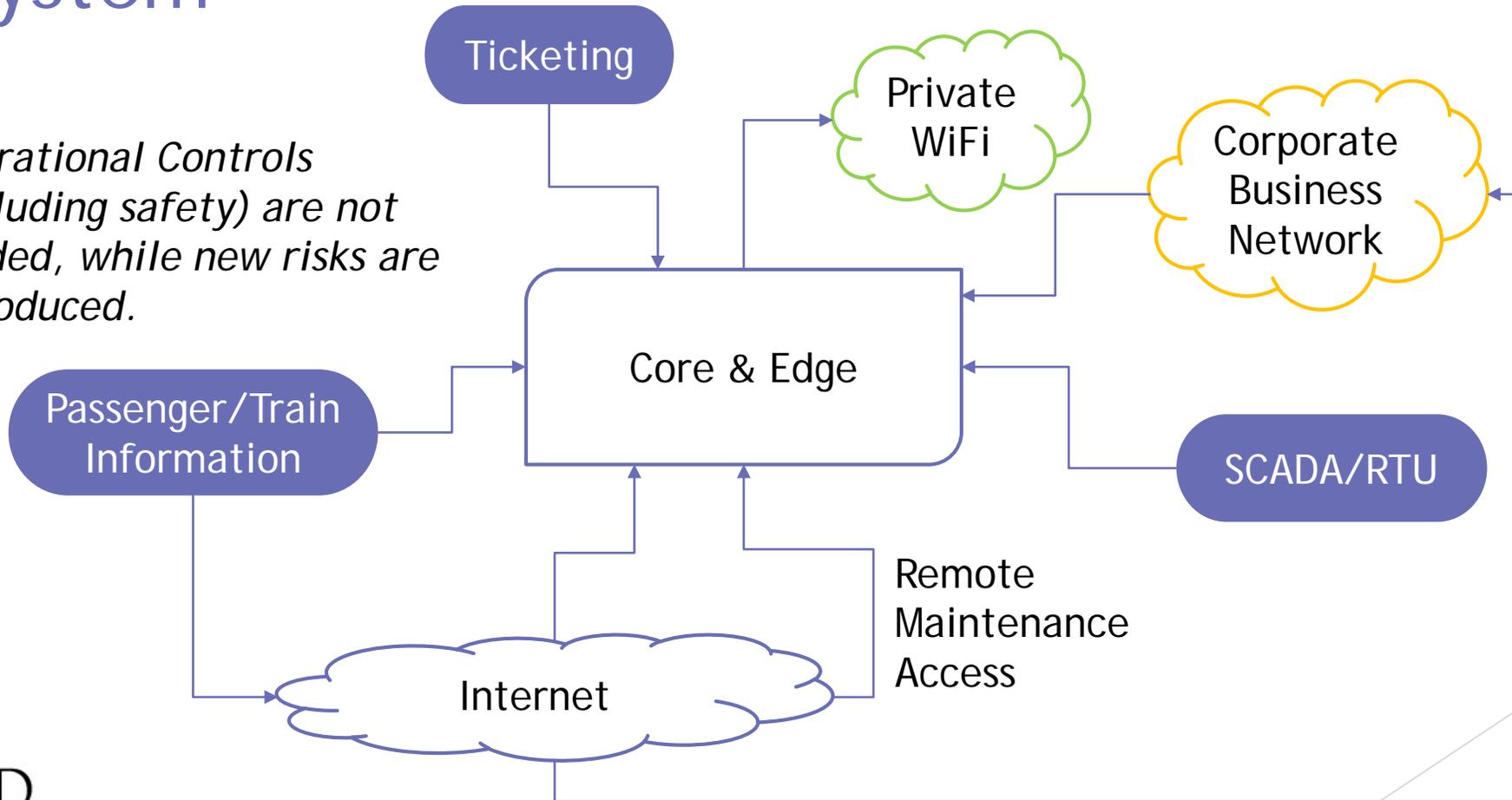
Present Systems Support



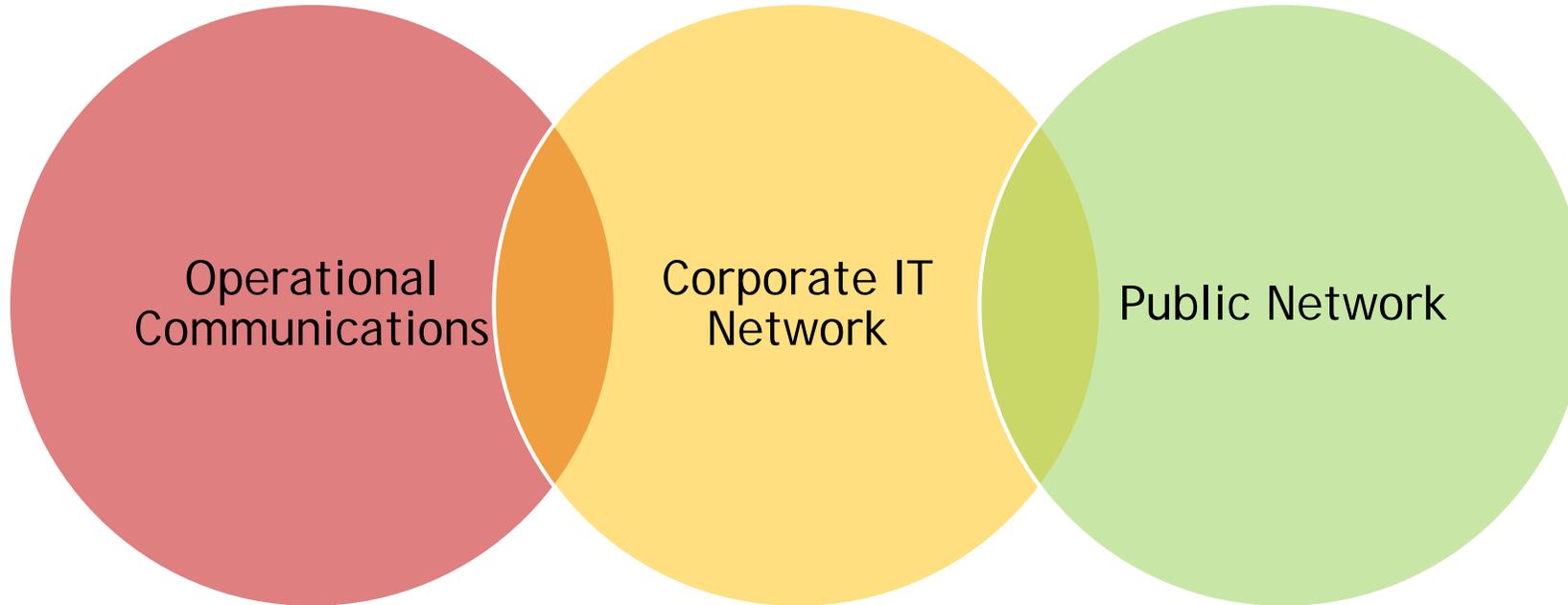
IP Network Communication System



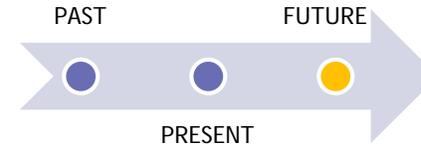
Operational Controls (including safety) are not eroded, while new risks are introduced.



Convergence of the Air Gap



Air Gap Replacement



Improving Critical Infrastructure Cybersecurity



Russell Kiernan

"The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront."

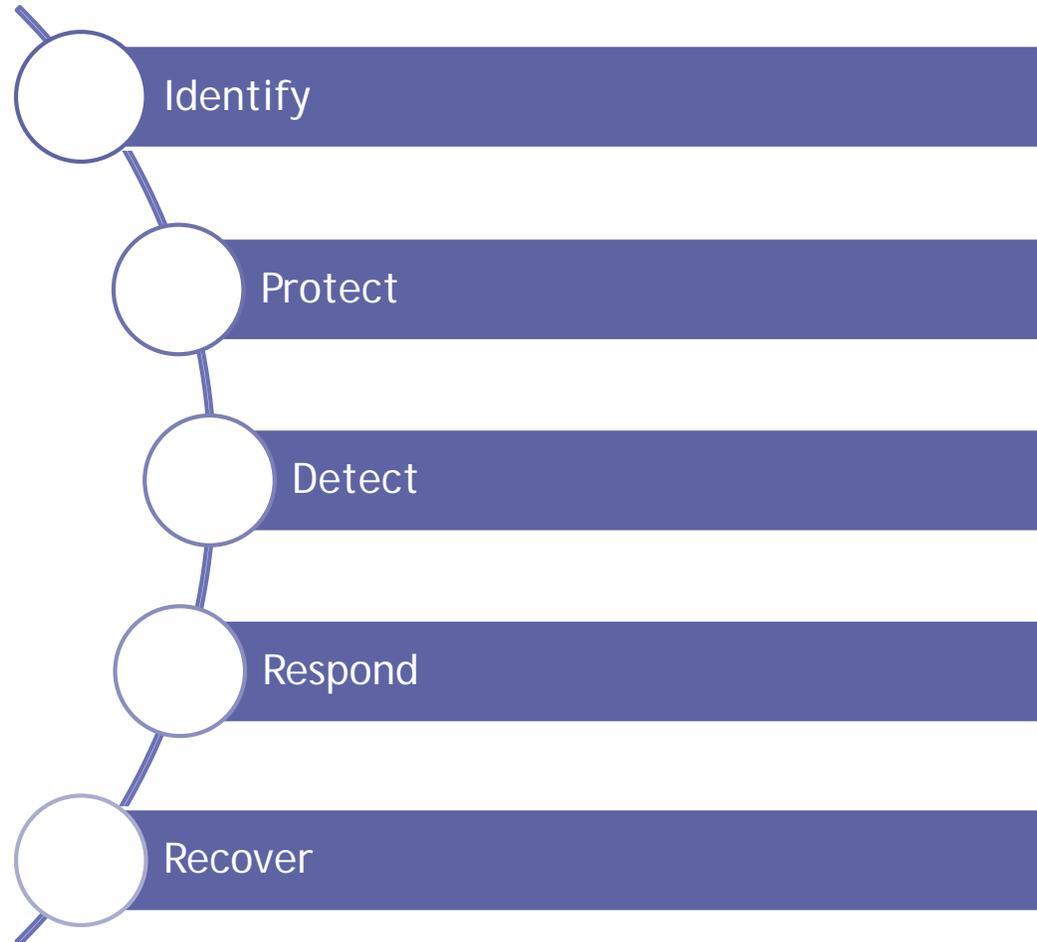
-Executive Order 13636



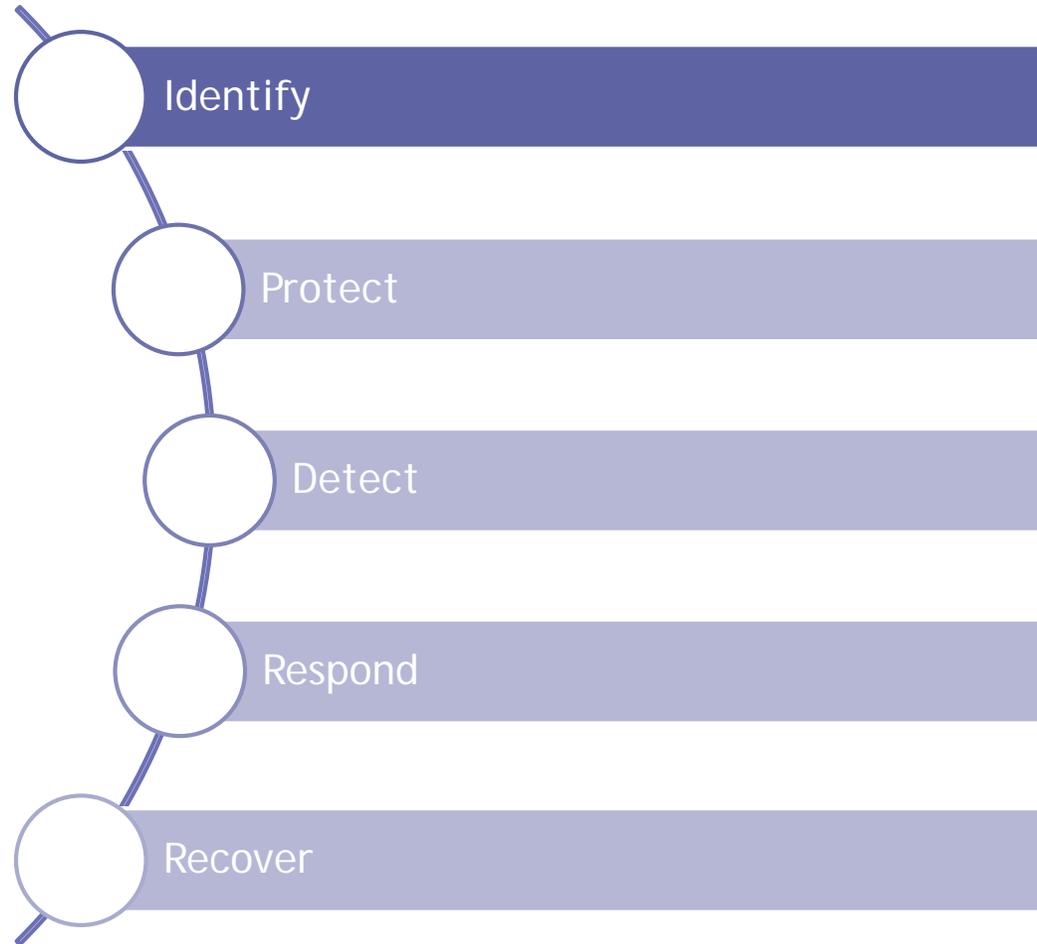
NIST



NIST Cybersecurity - Framework Core

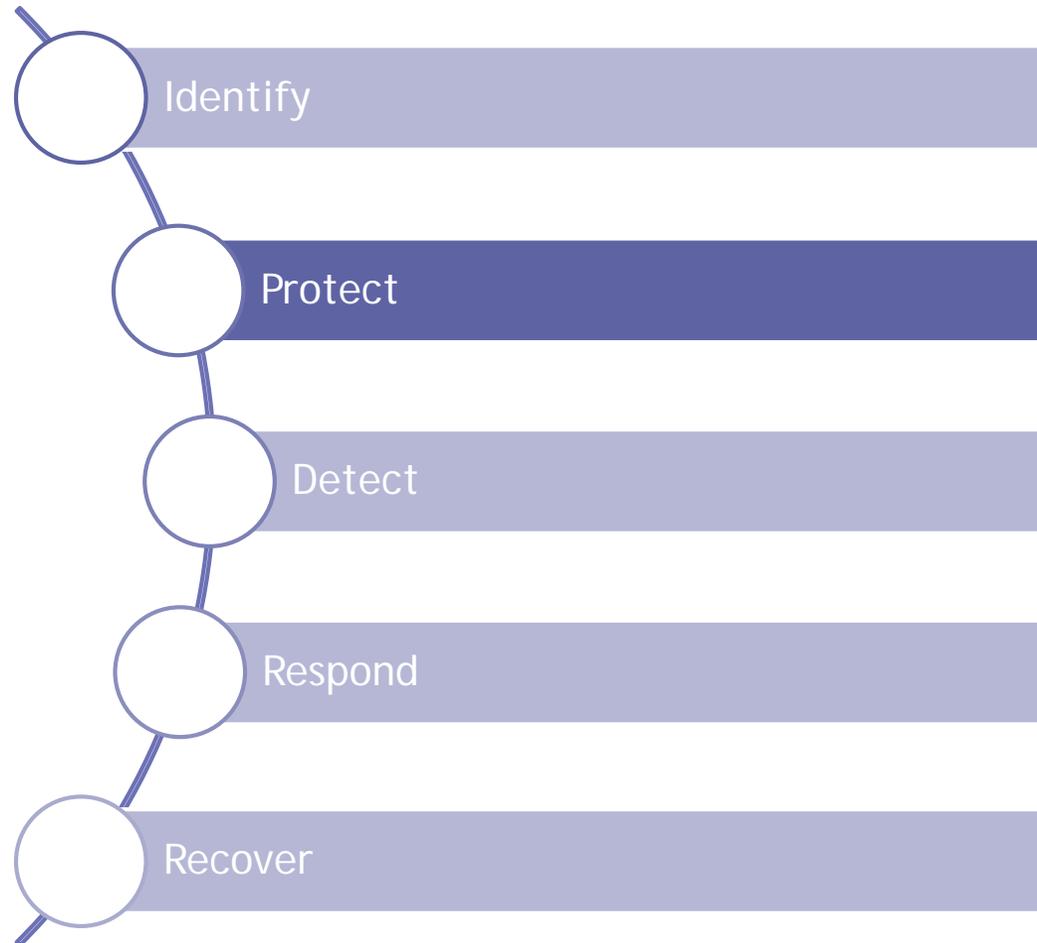


Core Framework - Identify



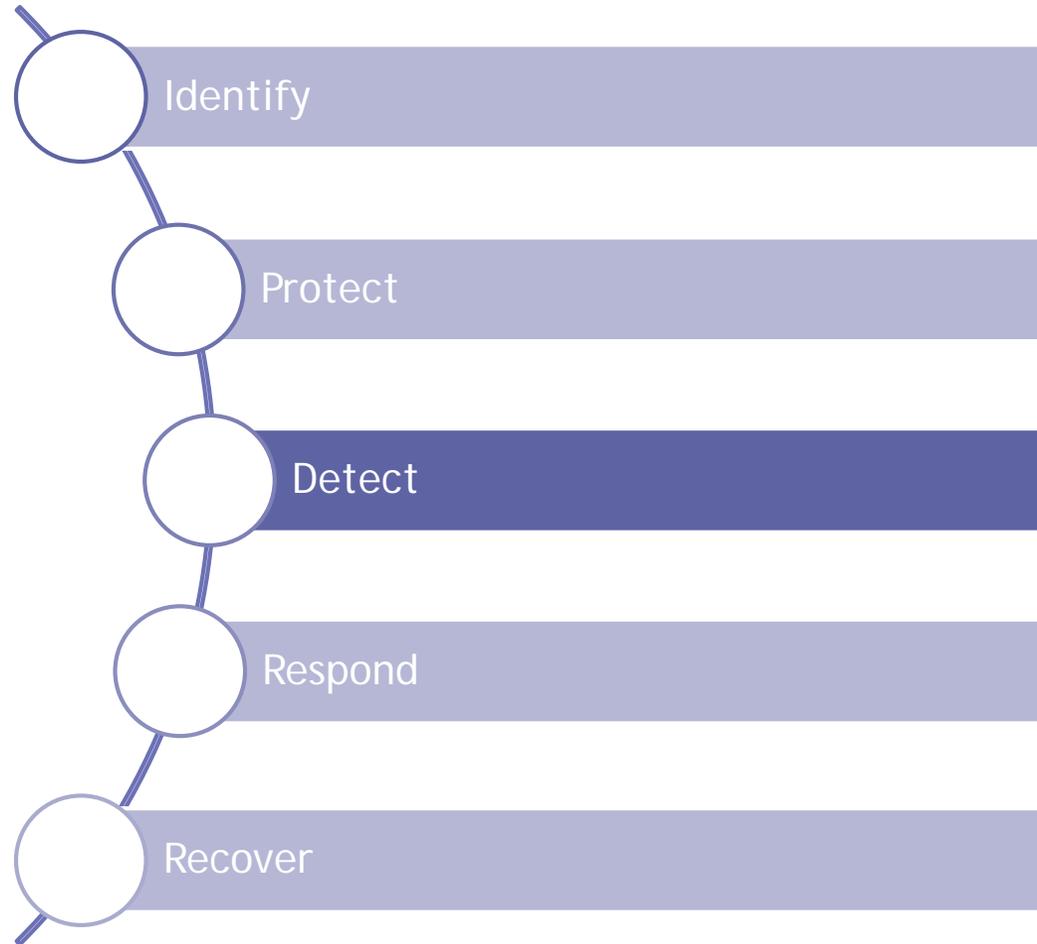
- ▶ Asset Management
- ▶ Business Environment
- ▶ Governance
- ▶ Risk Assessment
- ▶ Risk Management Strategy

Core Framework - Protect



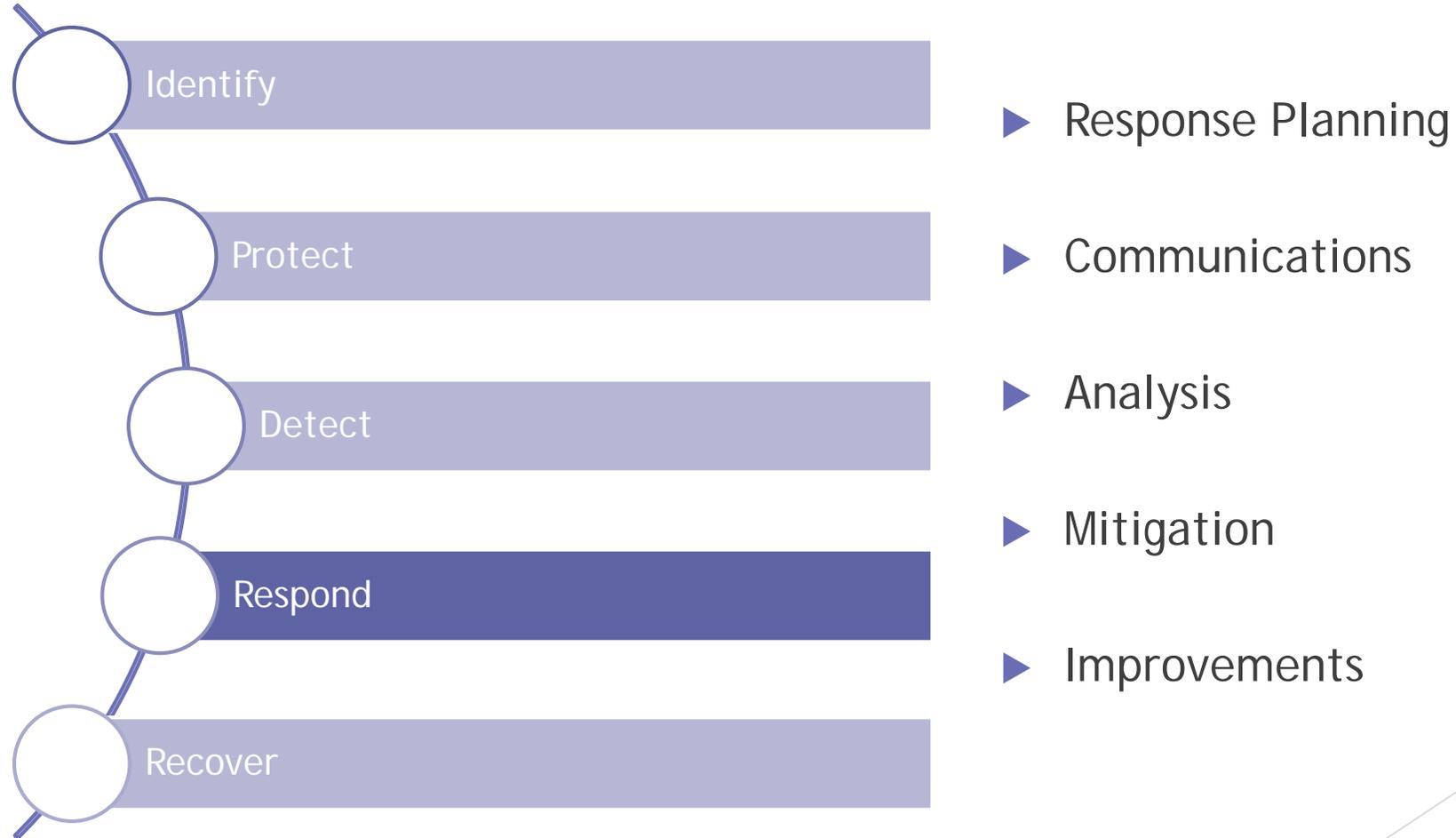
- ▶ Access Control
- ▶ Awareness and Training
- ▶ Data Security
- ▶ Information Protection Processes & Procedures
- ▶ Maintenance
- ▶ Protective Technology

Core Framework - Detect

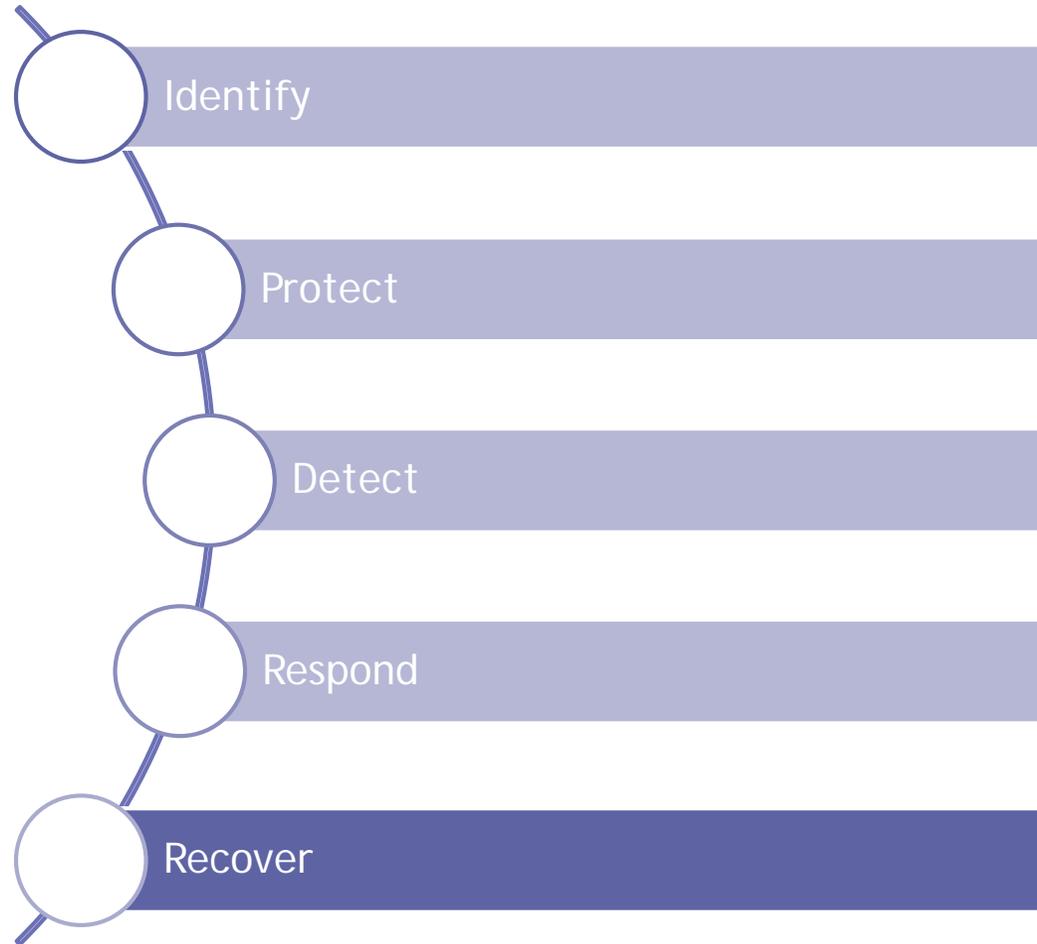


- ▶ Anomalies and Events
- ▶ Security Continuous Monitoring
- ▶ Detection Processes

Core Framework - Respond



Core Framework - Recover



► Recovery Planning

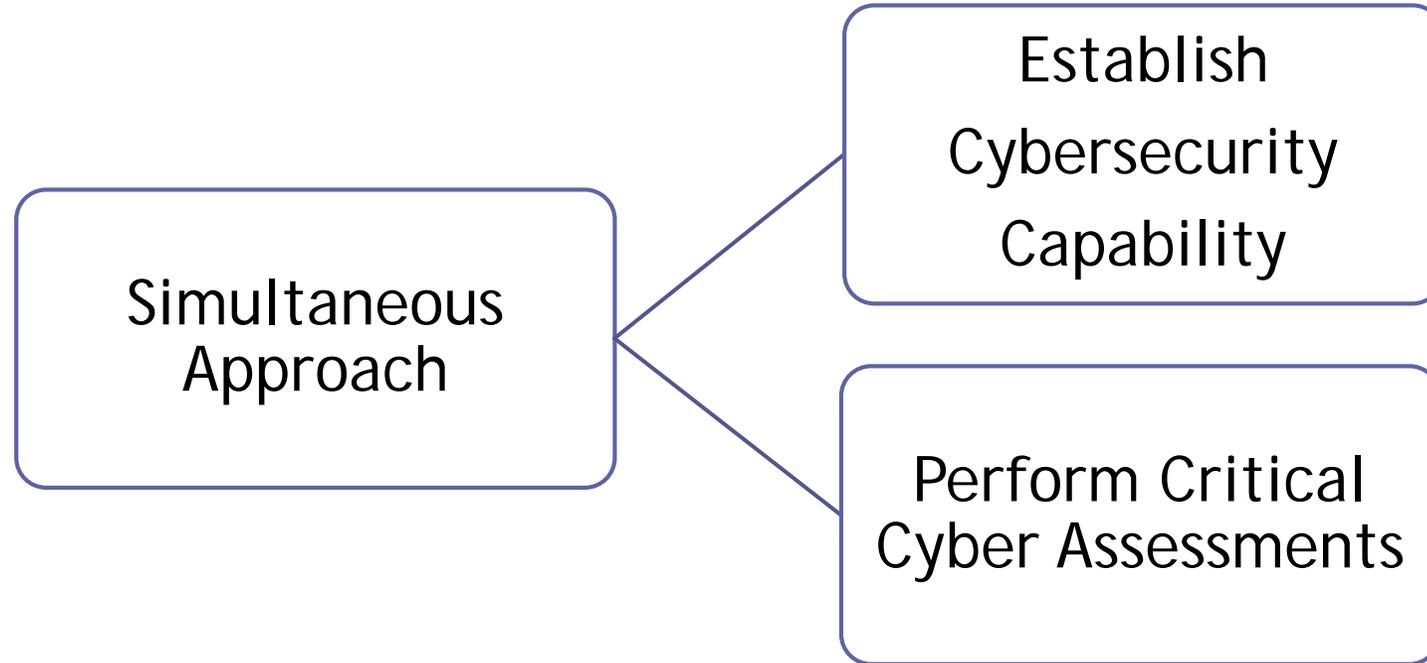
► Improvements

► Communications

Implement/Enhance Cyber Capability

- ▶ Step 1: Prioritize and Scope
- ▶ Step 2: Orient
- ▶ Step 3: Create a Current Profile
- ▶ Step 4: Conduct a Risk Assessment
- ▶ Step 5: Create a Target Profile
- ▶ Step 6: Determine, Analyze, and Prioritize Gaps
- ▶ Step 7: Implement Action Plan

Suggested Implementation



Perform Critical Cyber Assessments

- ▶ Vulnerability Assessment
- ▶ External Penetration Testing
- ▶ Internal Penetration Testing
- ▶ Wireless Assessment
- ▶ Breach/Intrusion Detection

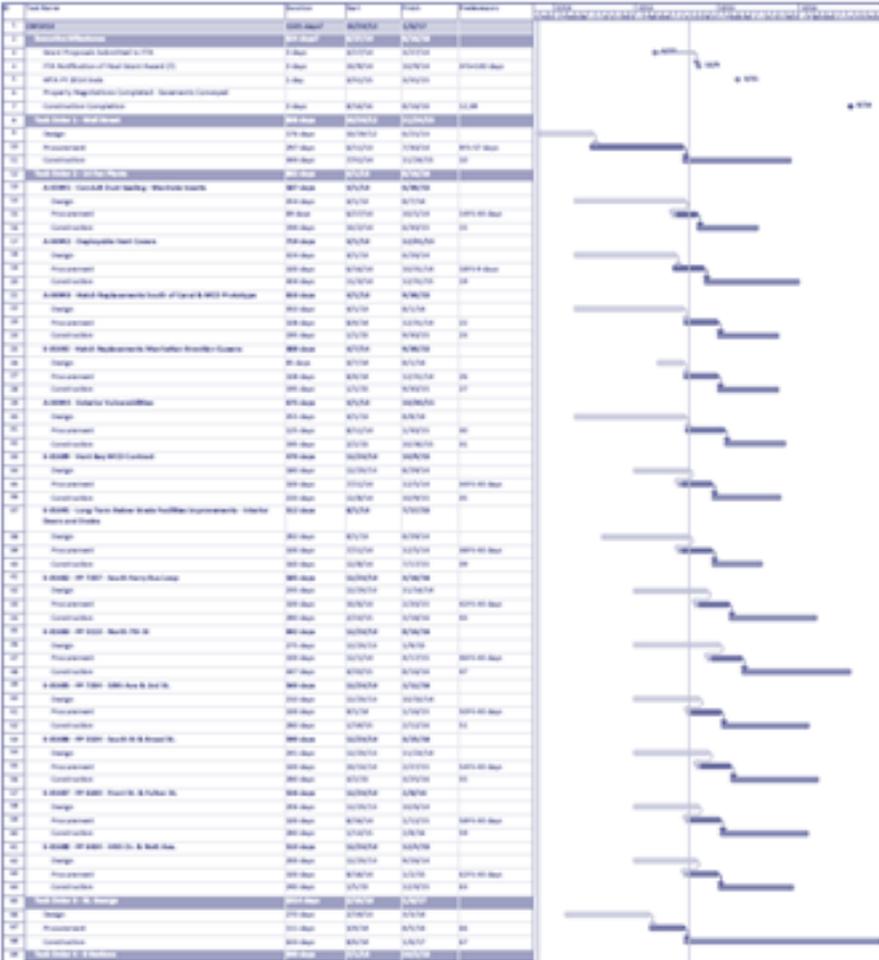


Critical Cyber Assessments - Outcome

Report & Remediate

RISK RATING TABLE

I M P A C T	5	M	H	H	H	H
	4	M	M	H	H	H
	3	L	L	M	M	H
	2	L	L	L	L	M
	1	L	L	L	L	L
		1	2	3	4	5
		PROBABILITY				



Enhanced Security and Resilience



A comprehensive and persistent capability to more effectively address cybersecurity risk for processes, information, and systems directly involved in the delivery of critical infrastructure services.

Summary

- ▶ Collective responsibility of all stakeholders involved
- ▶ Air Gap erosion through the convergence of networks
- ✓ Evaluate risks of newly converged systems
- ✓ Implement enhanced controls
- ✓ Develop comprehensive and persistent Cyber Risk capability