IWS Communication; Challenges & Security Risks for Water Utilities

Water Research Foundation, Project # 04670

Bob Daly, Principal Consultant, EMA

Mary Smith, Project Manager, WRF

EMA

THE Water Research FOUNDATION

June 14, 2018

Agenda

1. WRF Project #04670 Introduction
2. Utility Survey Findings
3. Considerations for IWS Communications and Security
4. Emerging Technologies
5. Conclusions

– Advancing the Science of Water

Advancing the science of water to improve the quality of life

- Member-Supported, non-profit research collaborative
- Integration of WRF and WE&RF – January 1st, 2018
- 1,200 subscribers - water, wastewater, stormwater, and reuse
- 2,300 research studies, $700M Value

Denver, CO

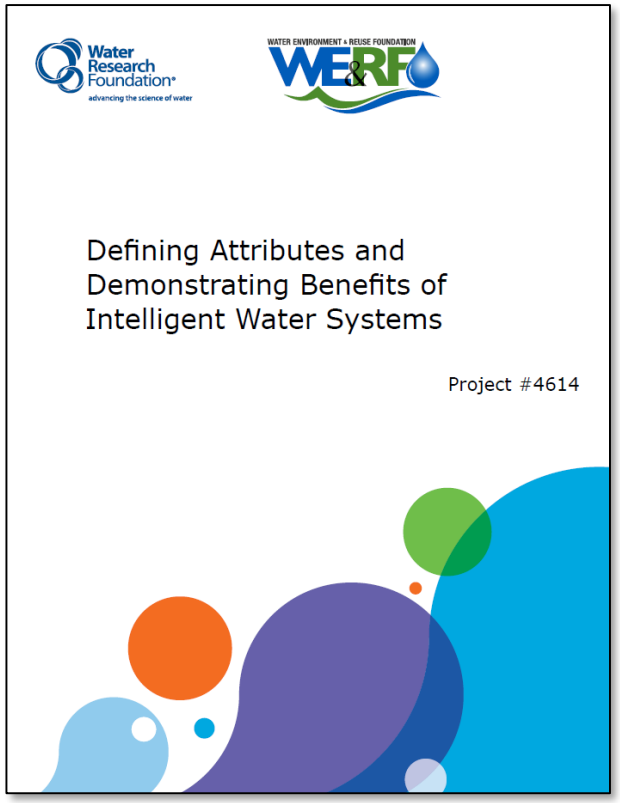
Alexandria, VA

Section 1

WRF Project #04670 Introduction

WRF Research Track

- Area Focus Program Research Track was established in 2015 – *Defining Attributes and Demonstrating Benefits of Intelligent Water Networks.*
- Initial Project - #04614 (published in 2017) – surveyed the field and identified research projects for the track.
- This Project - #04670 is one of the projects recommended by #04614.



Source: WRF Project # 04614

Need for Project #04670

- Utilities use a wide range of information systems as part of IWS
- Information systems often evolved independently
- As a result, cybersecurity, performance, and integration challenges exist
- Project #04670 needed to:
  - Inventory types of systems and associated communication media and protocols
  - Provide guidance to help utilities select best communication and cybersecurity

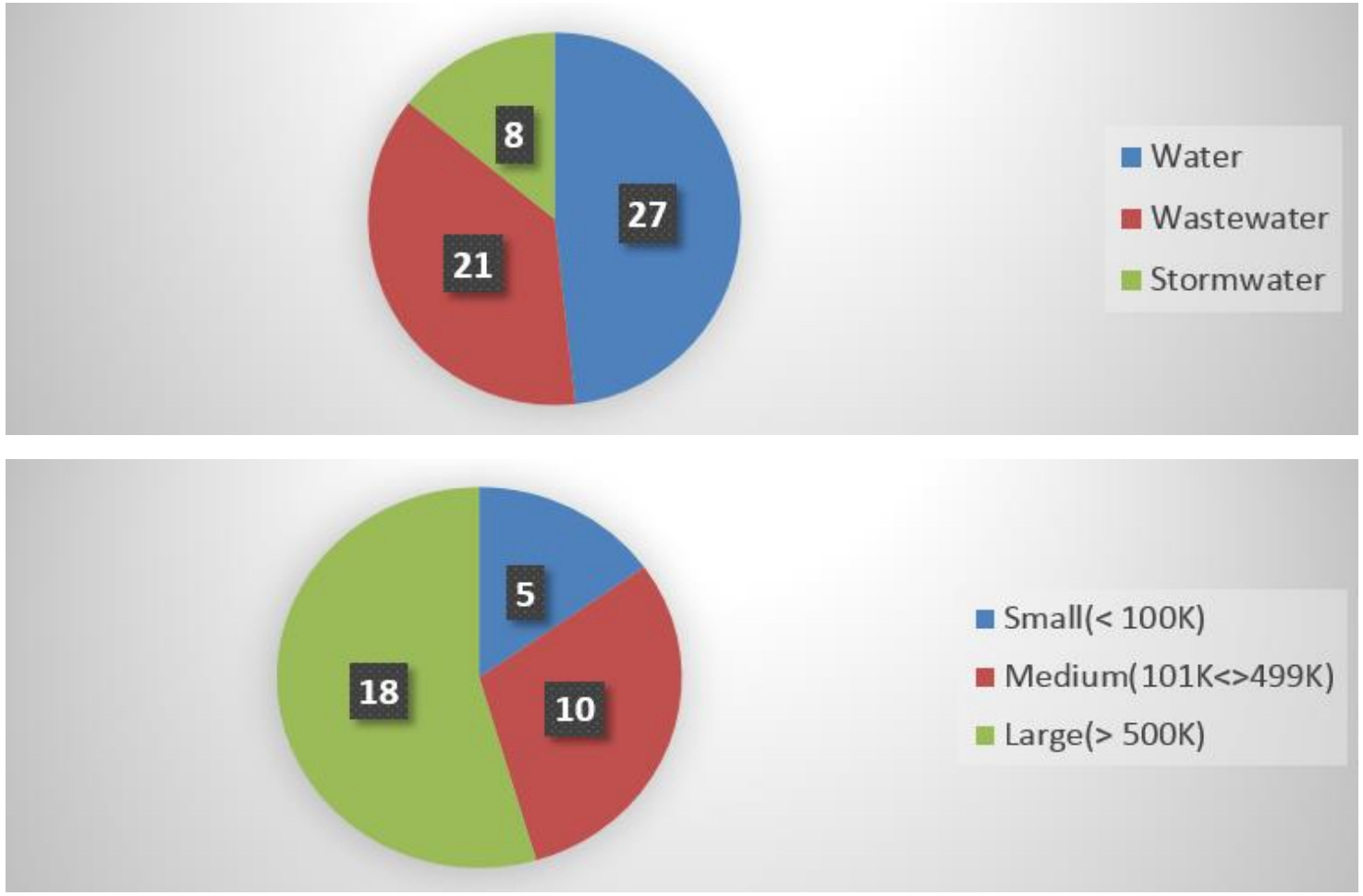
Project Approach

- Work with Utility Advisory Panel (UAP) from 8 utilities and WRF Project Advisory Committee (PAC) from 4 additional utilities
- Perform a utility survey to understand the current situation
- Explore emerging technologies
- Conduct workshop to review findings with UAP and PAC
- Create final report and tool to provide guidance

Section 2

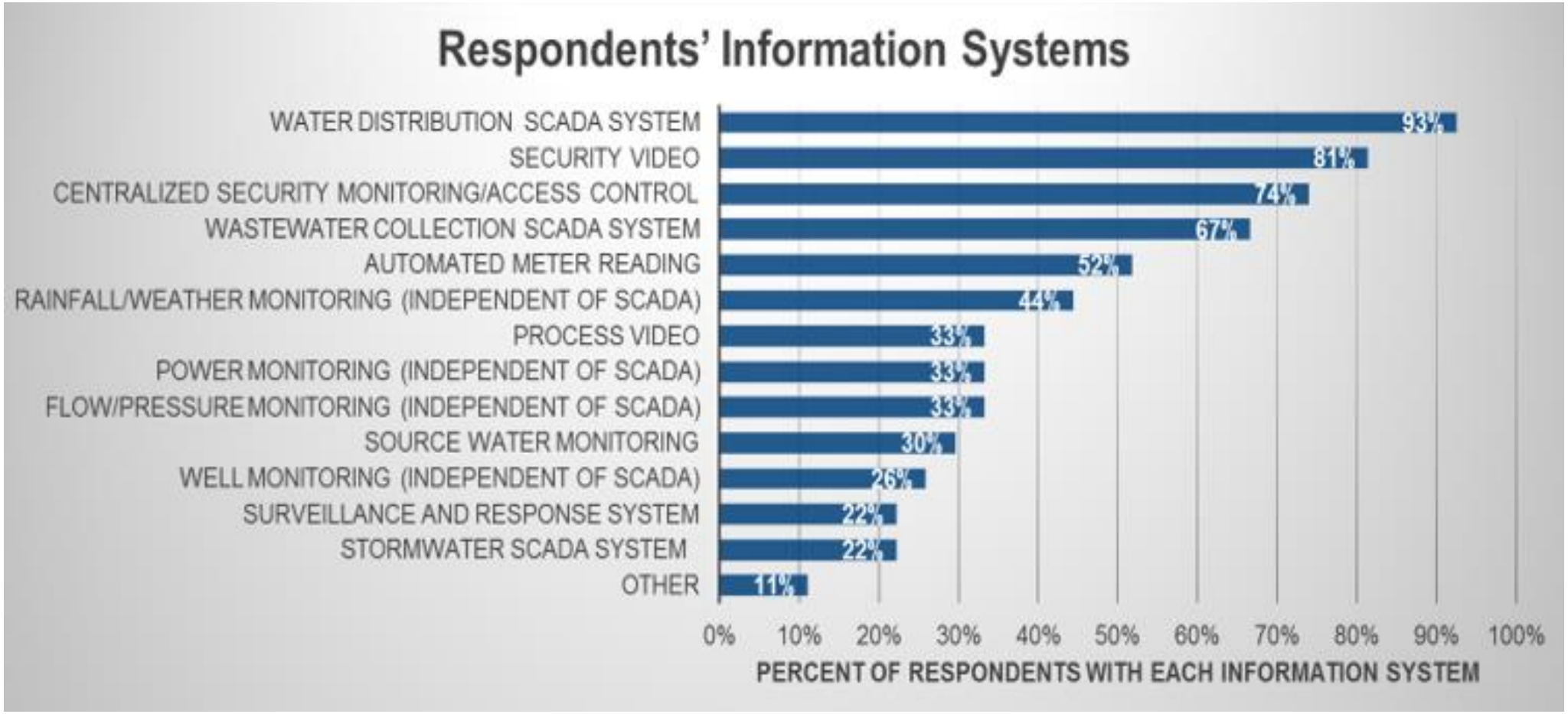
Utility Survey Findings

Who Were the Survey Respondents?



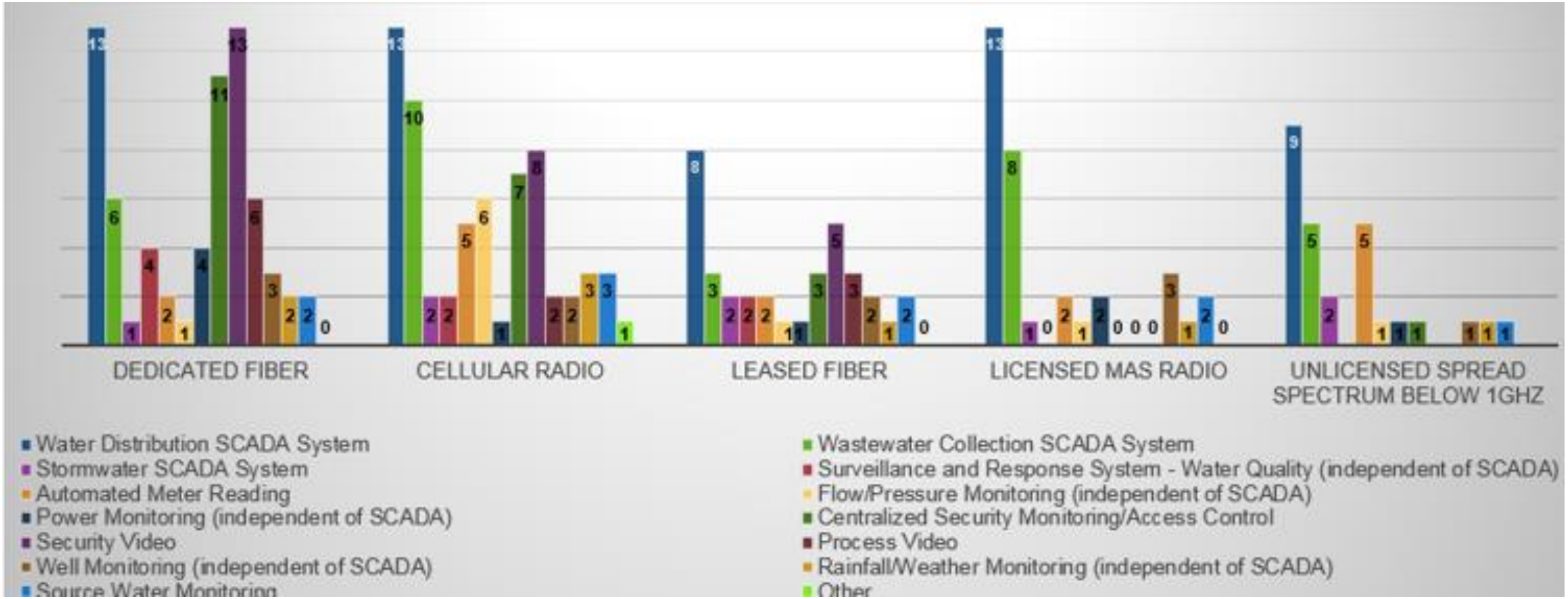
Source: WRF Project # 04760

Most Popular IWS Information Systems



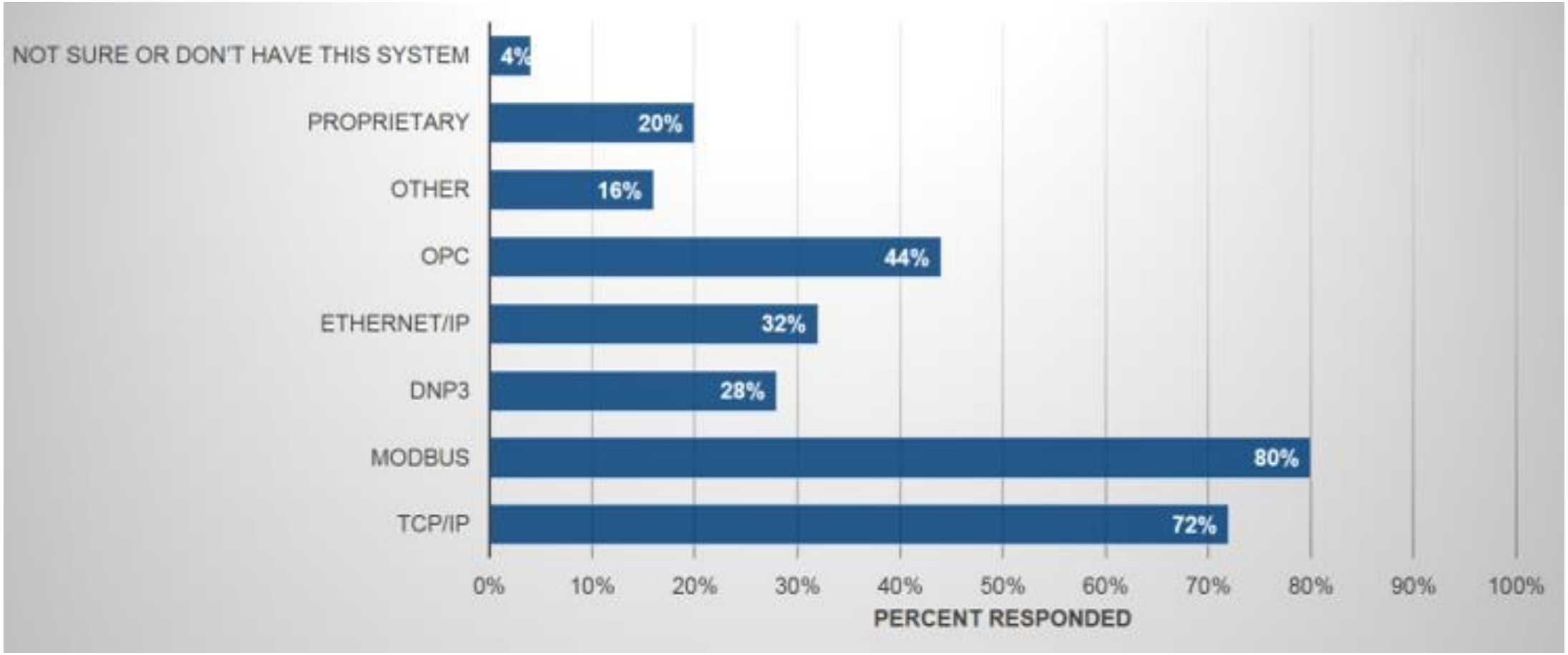
Source: WRF Project # 04760

Most Popular Means of Communications



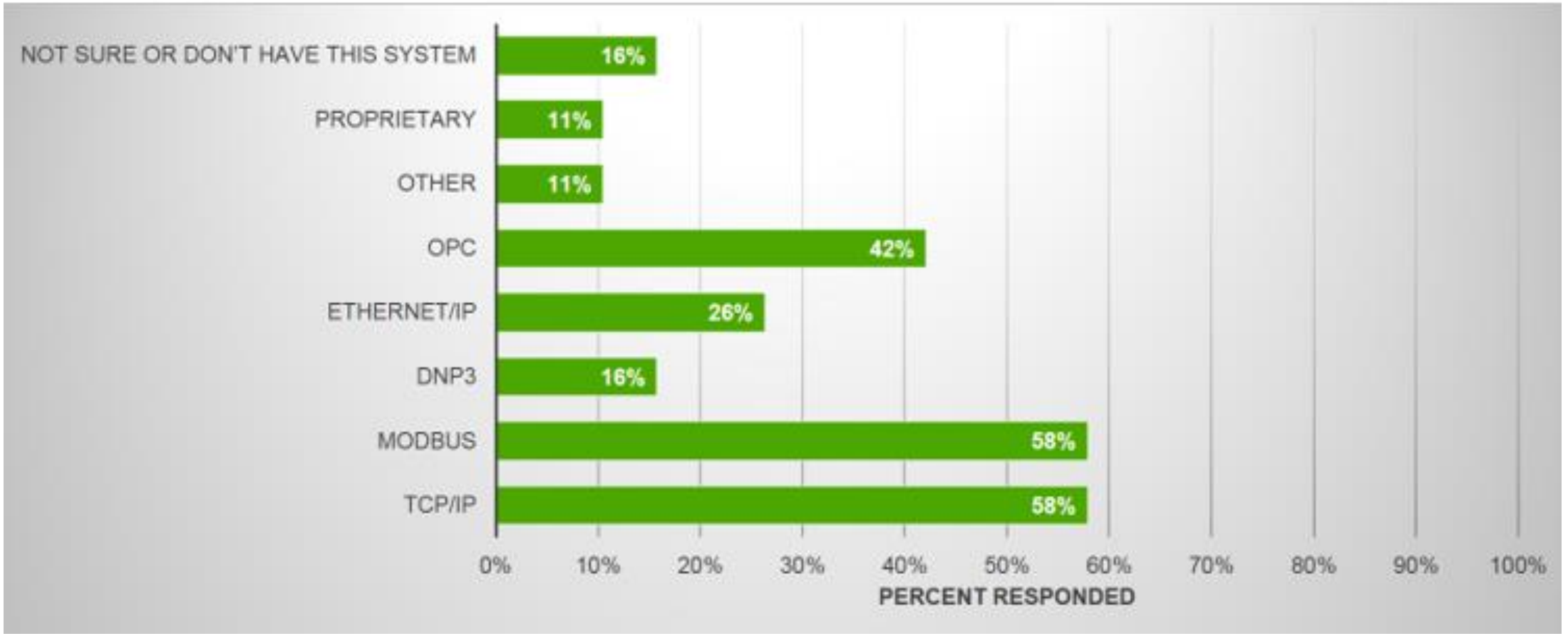
Source: WRF Project # 04760

Distribution SCADA Protocols



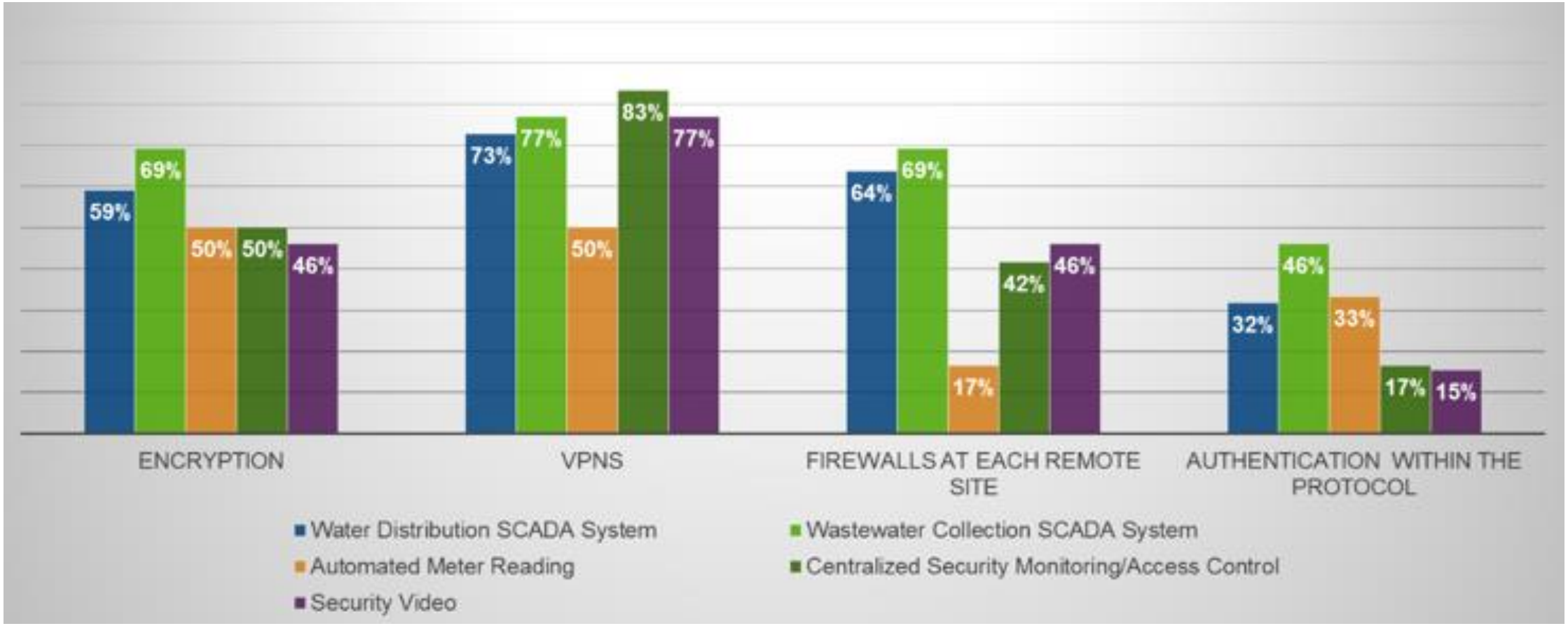
Source: WRF Project # 04760

Collection System SCADA Protocols



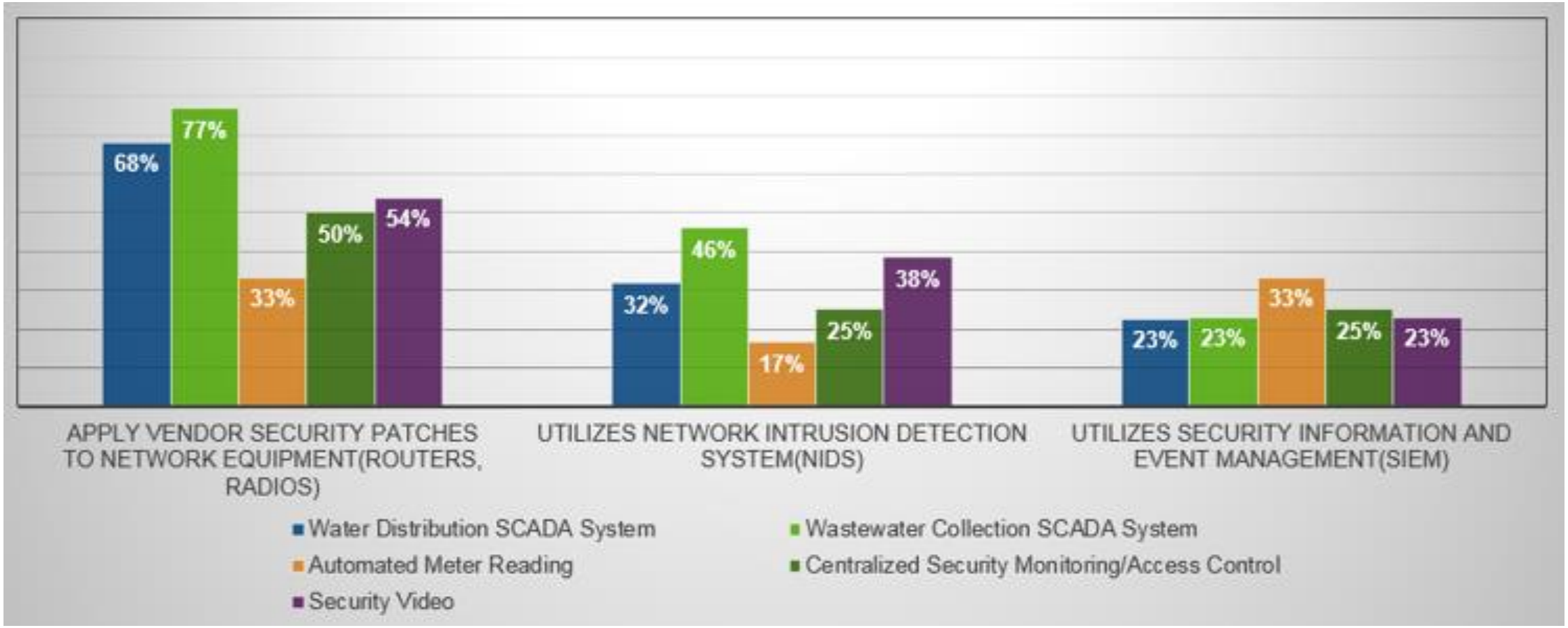
Source: WRF Project # 04760

Use of Security Technologies



Source: WRF Project # 04760

Use of Security Technologies



Source: WRF Project # 04760

What Survey Revealed about Security

- Reduced participation in answering security questions
- Room for improvement
  - Approx. 66% have formal cybersecurity policies and procedures
  - Approx. 50% have had independent cybersecurity testing done in the past 2 years
  - Approx. 25% are using Security Information and Event Management systems

Section 3

Considerations for IWS Communications and Security

Introduction to Considerations Matrix Tool

- Concept developed during UAP/PAC workshop
- Excel sheet for each of the most popular information systems
- Each sheet shows, for the 5 most popular communication methodologies:
  - General considerations
  - Cybersecurity considerations
  - General observations concerning capital and O&M Costs
  - General and security considerations for the most popular protocols

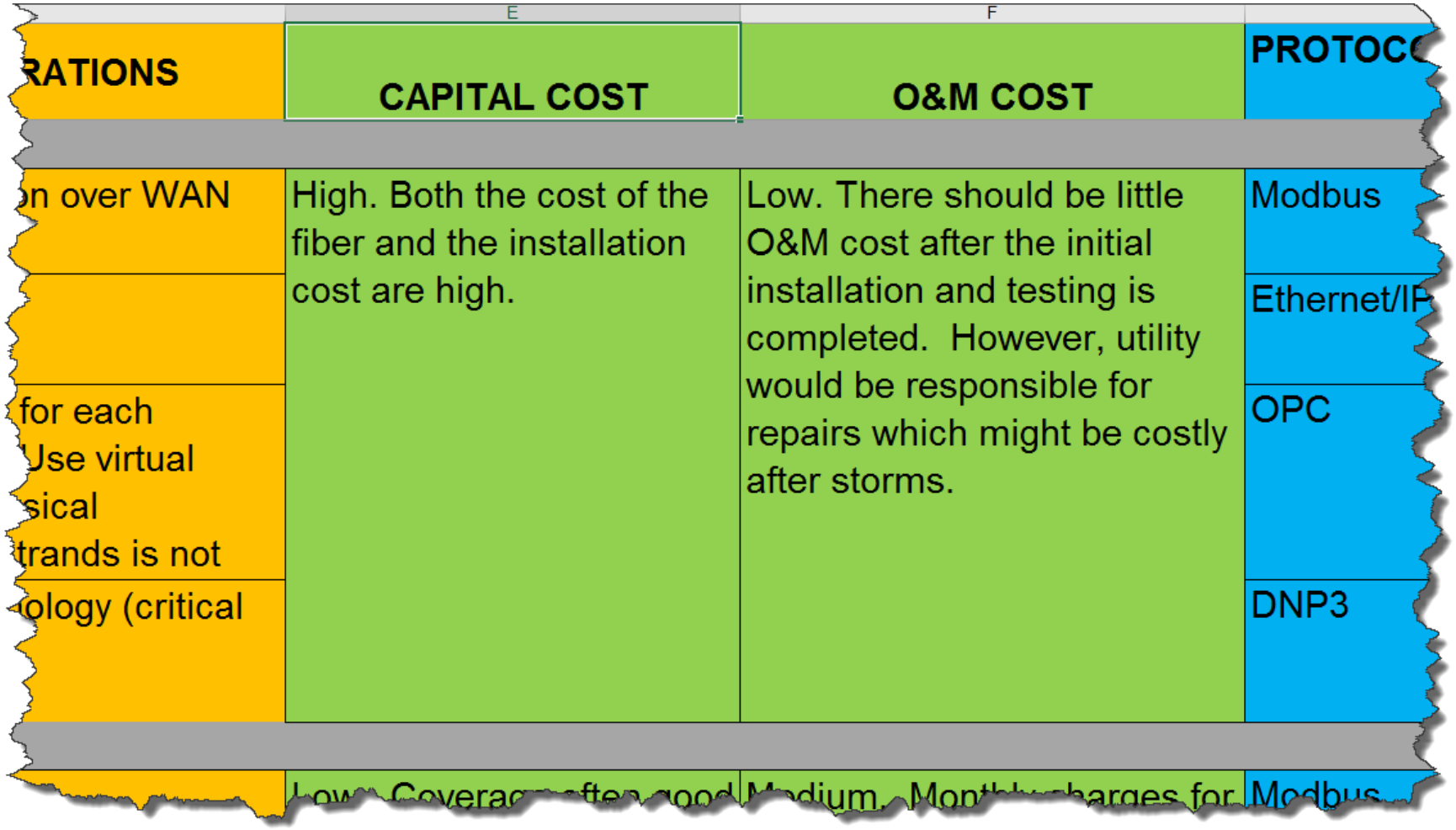
Introduction to Considerations Matrix Tool (Cont.)

- AMI/AMR sheet is focused on Field Area Networks (FANs)
- Security Video provides general and security considerations for protocol/codecs (communication/compression methods)

Considerations Matrix for Distribution SCADA

INFORMATION SYSTEM	COMMUNICATION METHODOLOGY	GENERAL CONSIDERATIONS	CYBER CONSIDERATIONS	
Distribution SCADA System				
	Dedicated Fiber	•Reliable	•Authentication/ Encryption over WAN	High. fiber cost
		•Large bandwidth	•Firewall capabilities	
		•May be shared with other information systems.	•Have dedicated strands for each communication system. Use virtual network technology if physical separation on separate strands is not possible.	
		•QOS and SLAs very important to guarantee required bandwidth if fiber is shared.	•Intrusion detection technology (critical sites)	
		•Life-cycle (don't control	•Authentication measures	Low

Considerations Matrix (Continued)



	E	F	
RATIONS	CAPITAL COST	O&M COST	PROTOCC
on over WAN	High. Both the cost of the fiber and the installation cost are high.	Low. There should be little O&M cost after the initial installation and testing is completed. However, utility would be responsible for repairs which might be costly after storms.	Modbus
			Ethernet/IP
for each Use virtual sical trands is not			OPC
ology (critical			DNP3
	Low. Coverac ften good	Medium. Monthly harges for	Modbus

Considerations Matrix (Continued)

COST	PROTOCOLS	PROTOCOL CONSIDERATIONS	PROTOCOL SECURITY CONSIDERATIONS
uld be little the initial testing is wever, utility nsible for ight be costly	Modbus	•Number of data types is limited to those understood in the 1970s, Large binary objects are not supported. •Master/Slave protocol. Does not support peer to peer. •Time-Stamped data must be custom programmed, outside of protocol •Modbus TCP would be used or serial encapsulated in TCP. •Open Protocol, vendor neutral.	Modbus protocols do not have authentication or encryption included as part of the protocol itself. Authentication and encryption should be added outside of the protocol as a recommended cybersecurity practice. Bandwidth with fiber is large enough to support additional overhead for authentication and encryption measures. Encapsulate the protocol within a secure transport protocol like TLS
	Ethernet/IP	•Utilizes the Common	Segmentation and perimeter security. Use authentication

Section 4

Emerging Technologies

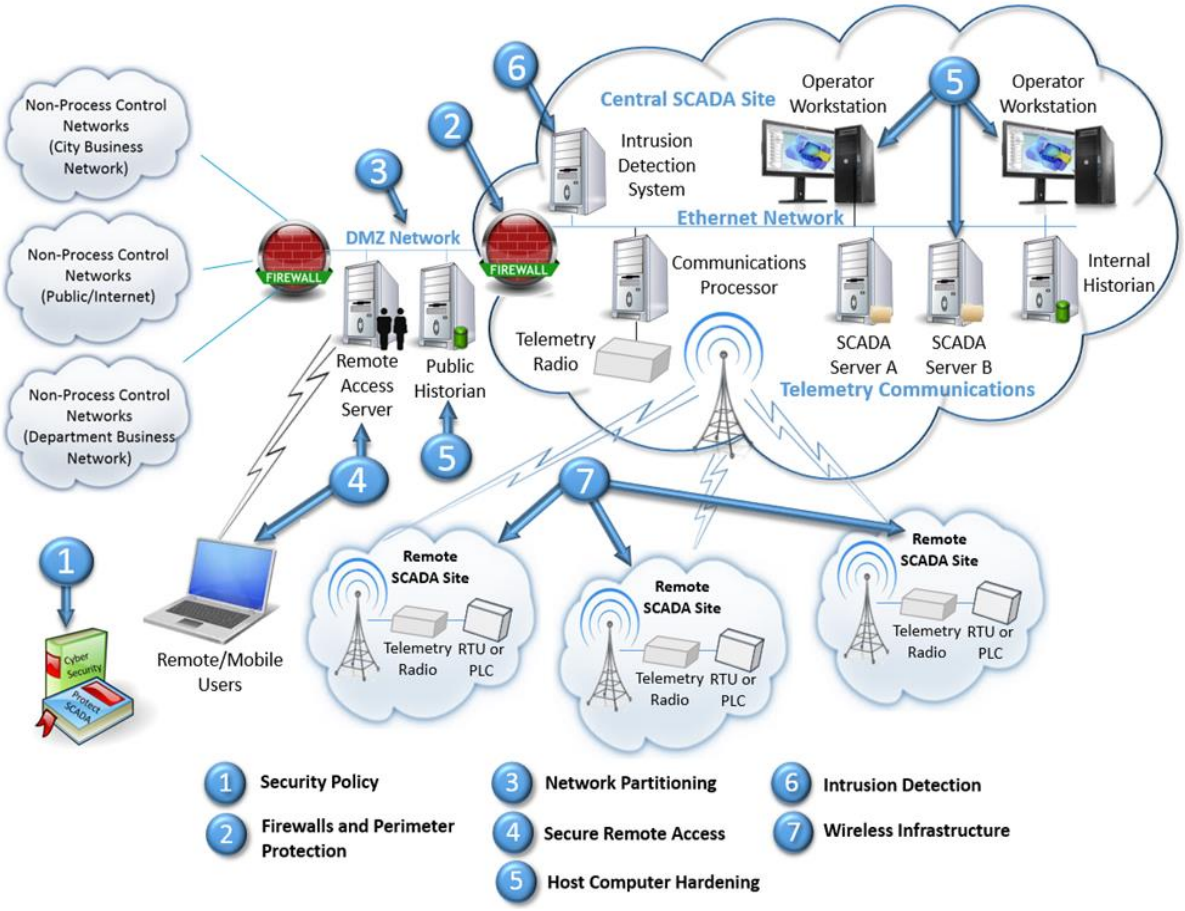
Emerging Communication Technologies

- Low Power Wide Area Networks (LPWANs)
  - Wide coverage to distributed devices using small packets at regular intervals, often battery powered
  - Examples:
    - LoRa - 900 MHz ISM, low downlink bandwidth challenge
    - RPMA – 2.5 GHz ISM, increased downlink bandwidth over LoRa
    - LTE-CatM1 – cellular LTE technology, use cellular providers
    - NB-IoT – cellular LTE technology, complementary to CatM1

- WiMAX
  - Higher bandwidth, but higher power requirement
  - Licensed spectrum

Emerging Security Technologies

- Inventory Technologies
  - Passive discovery tools
  - Hybrid Tools working with ICS vendor applications detect changes
- Threat Detection
  - Network inspection
  - Use AI to flag abnormal communications
- Industrial firewalls
  - Understand industrial protocols
  - Provide higher level of filtering capability

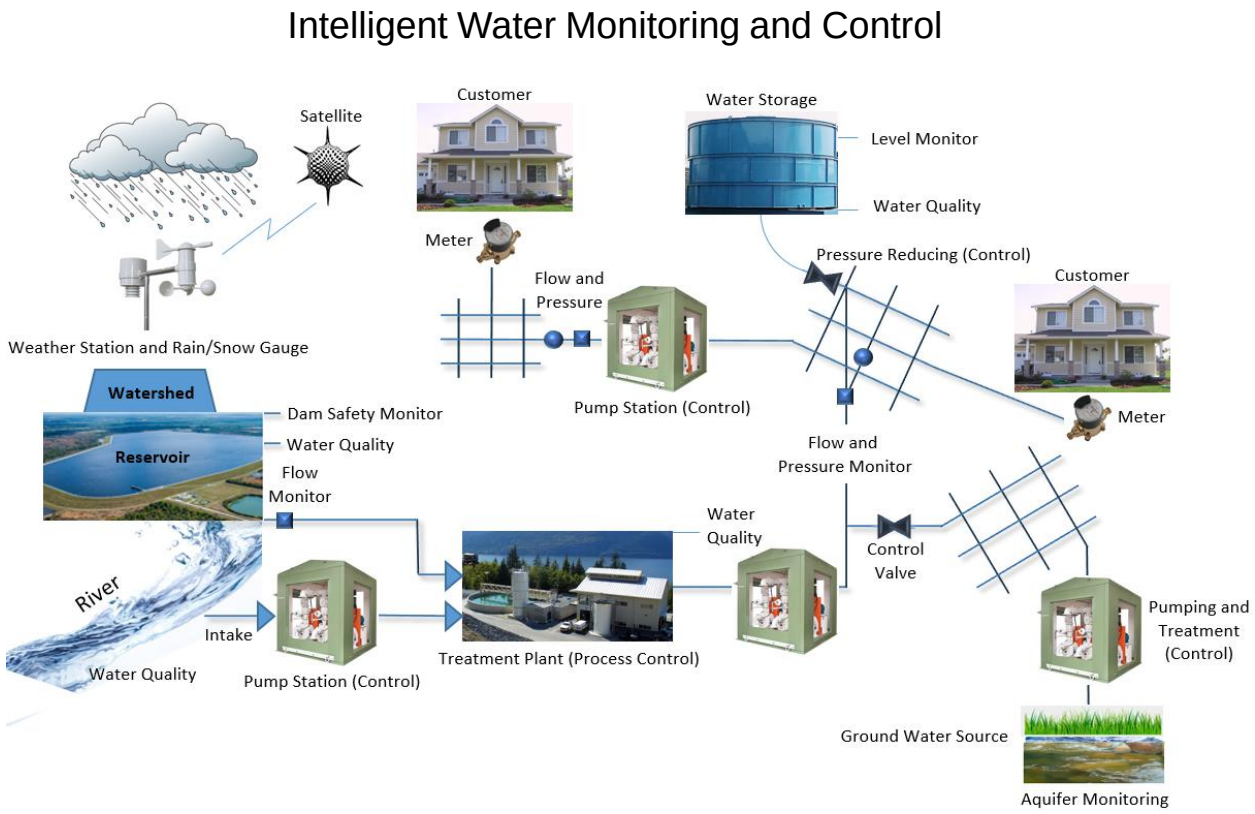


Section 5

Conclusions

Conclusions

- Survey revealed the most popular IWS information systems, communications technologies and protocols
- There is room for security improvements
- Utilities should consider risks associated with use of older communications with older protocols
- The considerations matrix provides guidance when selecting communication methods and protocols
- Utilities have an increasing range of communications options as new technologies emerge



Questions?

Bob Daly, EMA Mary Smith, WRF

Bob: bdaly@ema-inc.com

Mary: msmith@waterrf.org