Security for Field Area Networks: IT and OT Perspectives

zpryme

Sponsored by

cisco

Security for Field Area Networks: IT and OT Perspectives

With the rise of technologies such as distribution automation and advanced metering, field area networks (FANs) have gained considerable momentum because of their prominent role in grid modernization initiatives. With the world rapidly heading toward 20 billion connected devices, FANs are an essential tool for utilities looking to capture real-time asset and IoT application data. The value of FANs and the utility modernization imperatives to securely deploy and operate multiservice networks will only continue to increase as they provide the core flexible foundation for future grid applications—from distributed power generation and energy storage to electric vehicle charging to microgrids.

As recent attacks in the utility space have demonstrated, security among this growing set of distributed assets and sensors is incredibly important, and both operational technology (OT) and information technology (IT) will play key roles in managing secure communications networks. This paper explores how utilities are approaching and incorporating FAN security and network planning for the 21st century connected grid. Furthermore, Zpryme considers the current state of IT and OT responsibility in FAN security. Zpryme surveyed 100 IT and OT professionals from utilities to understand their perspectives on FAN security.

Key Findings

- 60% of respondents report cyber-attacks focusing on both IT and OT infrastructure.
- Only 37% of utilities say that IT and OT personnel are working Very Well or Extremely Well.
- Only 26% of utilities feel Very Prepared for FAN security.
- The top three areas of security concerns relating to FANs are SCADA systems (83%), Distributed Automation (79%), and AMI Meters (76%).

Based on this survey data and research with utility representatives involved in FAN planning, this paper provides:

- A snapshot view of the industry's current state of FAN security
- Guiding principles and considerations for successful OT/IT FAN security collaboration

Demographics

- Utility type:
  IOU (33%), municipal (30%), cooperative (26%), and district/federal (10%)
- Services provided:
  Electric (53%), water (16%), gas (15%), wastewater (7%), solid waste (5%)
- Headquarter location:
  Midwest (22%), southeast (22%), northwest (16%), southwest (15%), international (11%), mountain (8%), northeast (7%)
- Annual revenue:
  Below US$100M (27%), US$100M to $500M (24%), US$1B to $5B (19%), US$500M to $1B (17%), over US$5B (13%)
- Organization focus:
  Operational technology (51%), information technology (35%), risk and compliance (8%), security (7%)

The Growing Importance of FAN Security

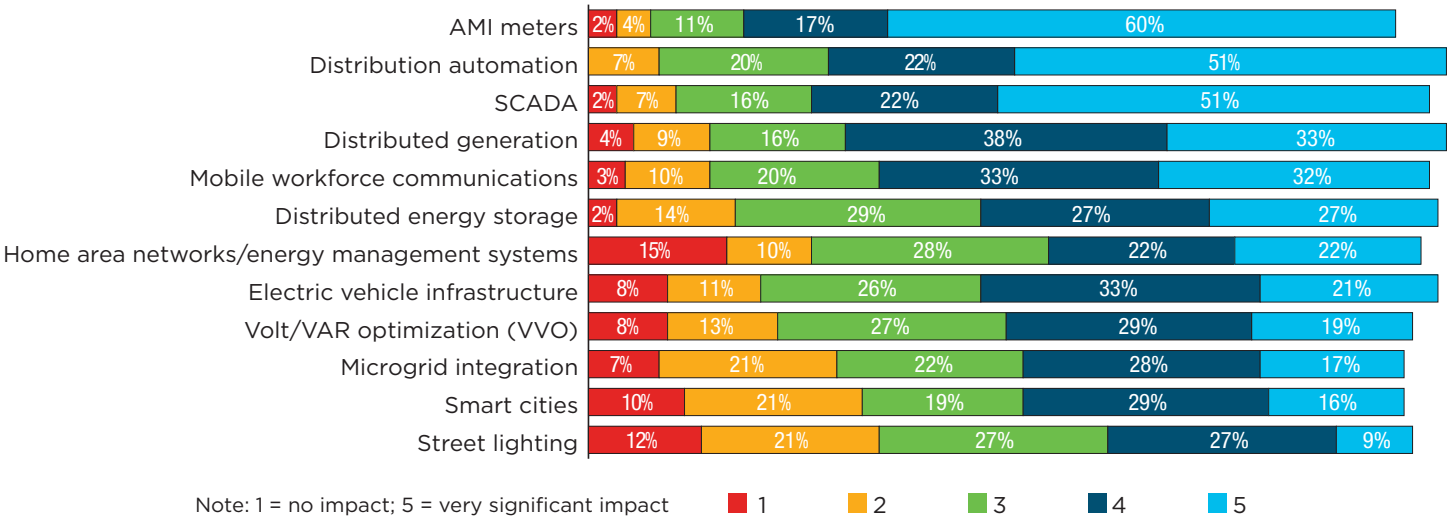
It has been a full decade since the North American Electric Reliability Corporation- Critical Infrastructure Protection (NERC-CIP) first took effect, and the evolution from uncertain acceptance to rapid deployment of security protocols and technologies has been staggering. Globally, similar security standards like NIST and ISO/ IEC have developed to address cyber security imperatives.

> FANs have become the go-to communication tool for utilities to connect the central network with assets, personnel, and devices in the field.

However, even as utilities have methodically worked to protect critical infrastructure, the pace of technological change and security risks has quickened. The rapid transformation of the grid from a single directional system transmitting and distributing power to customers, to a multi-directional network has necessitated a shift in communication infrastructure.

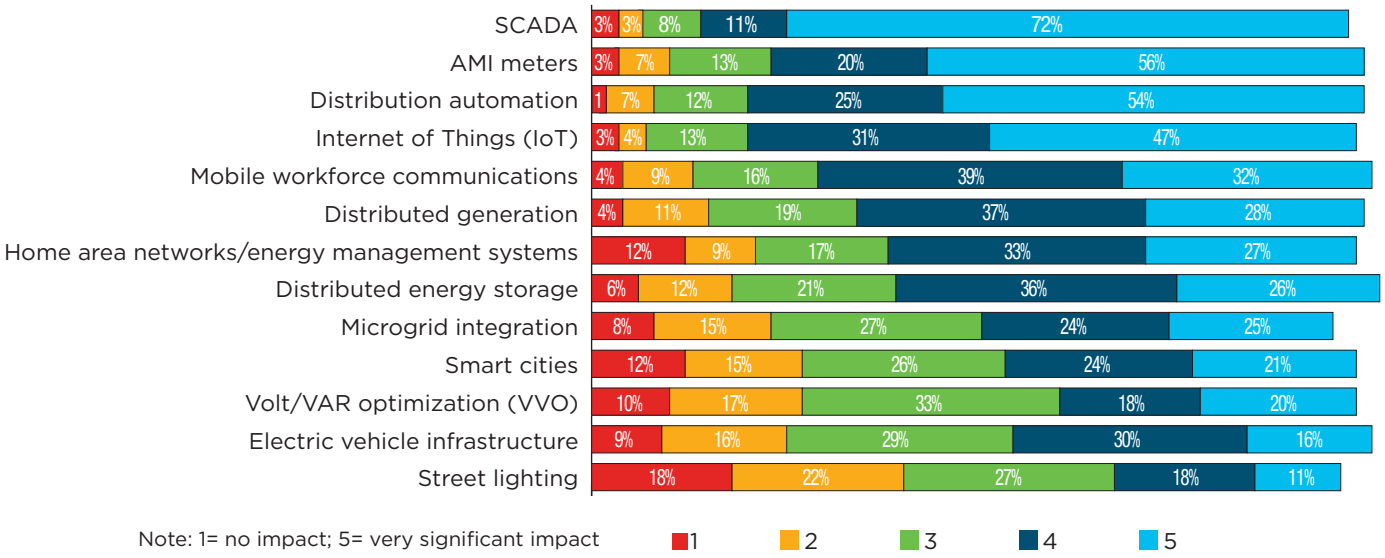
FANs have become the go-to communication tool for utilities to connect the central network with assets, personnel, and devices in the field. Over the next three to five years, utilities recognize the enormous impact FANs will have on the IT and OT business model. Foundational systems to the smart grid like AMI meters and SCADA systems (this is true across the full range of power, water, solid waste, and other utilities services) will become increasingly dependent on reliable FANs. These networks allow for lightning fast collection, analysis and communication of data from AMI meters, and SCADA systems underpin the smart grid. Consequently, utility leaders recognize the importance of FANs in the Interoperability of distributed generation, energy storage, industrial IoT and technology integration in the next 3-5 years.

Figure 1: Impact on utility's FANs in the next 3 to 5 years



The smart grid requires FANs to be highly reliable, scalable, flexible, mobile, and secure. With the growing number of connected devices, the large geographic coverage area, and need for real-time monitoring of asset performance, utilities have relied heavily on wireless technology like cellular, broadband point-to-multipoint, and wireless mesh networks to power FANs. As with all networks, wireless technology comes with vulnerability to cyber-attacks. Recognizing the importance of SCADA and AMI systems, it is not surprising that 83% (SCADA) and 76% (AMI) of utility respondents express concerns over their respective security. Concern for the FANs and smart grid security is also widespread across the diverse and growing set of energy functions, services and applications in today's utility. Distributed Automation (79%), IoT applications (77%), mobile workforce management (71%), distributed generation (65%), Energy Management systems (60%), and distributed energy storage (62%) all elicit significant security concerns from respondents. The awareness of security risks, by utilities is just the first step to resolving this issue. IT teams need to get OT buy in when deploying software solutions for FAN security management. Without this coordinated approach, key OT systems like SCADA and Distributed Automation will be more susceptible to a security breach.

Figure 2: Application Security concern

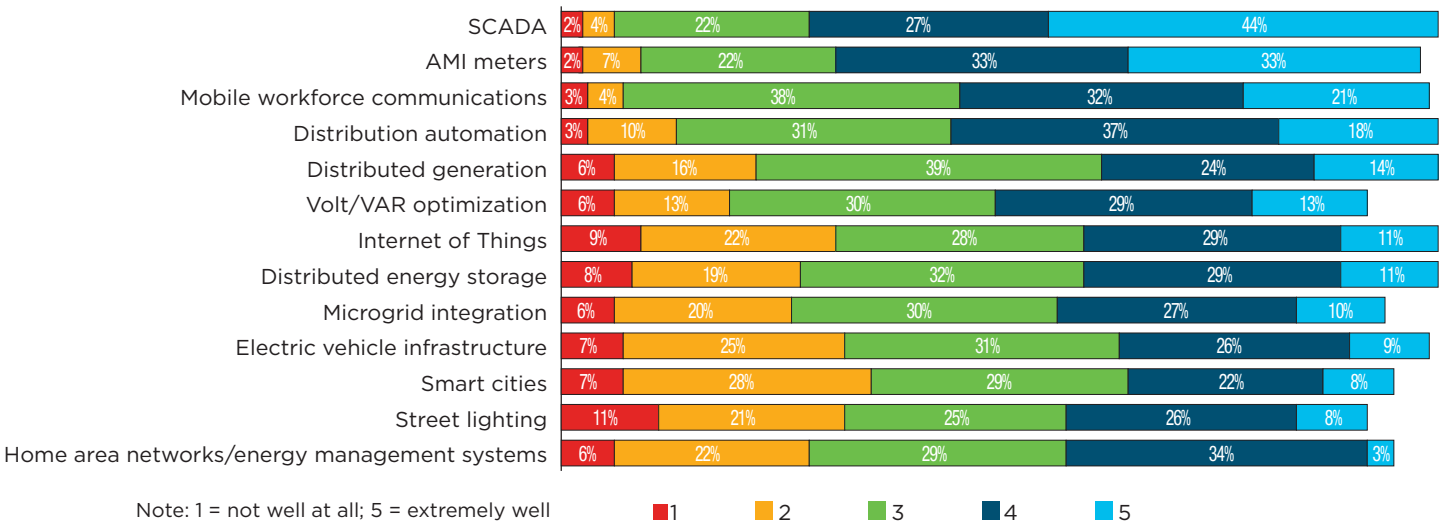


Fewer than 50% of respondents feel significant confidence that critical systems are sufficiently protected from security threats.

Perhaps even more concerning, is the general outlook on vendors' abilities to currently assist utilities in managing FAN security concerns. Fewer than 50% of respondents feel significant confidence that critical systems like distributed generation (38%), Volt/VAR optimization (42%), electric vehicle integration (35%), and micro-grid integration (37%) are sufficiently protected from security threats. The perception of security for key customer-facing systems like IoT applications (40%) and Home Energy Management systems (37%) is also particularly low.

The current dichotomy between the recognition of FAN security being essential and current lack of confidence in the ability to address those security concerns is striking. Understanding the current approach utilities are taking in deploying FAN security is essential for closing that gap.

Figure 3: Vendor community ability to address security concerns today



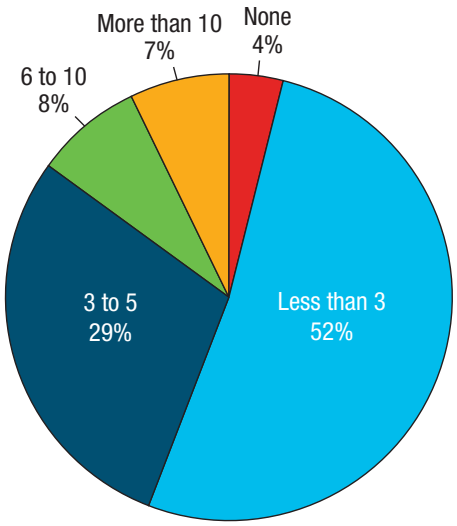
Utility Approaches to FAN Security

There is not a one size fits all approach to FAN security at this point. Digital strategy for cybersecurity is evolving across the grid. NERC-CIP was and continues to be a major driver in the North American experience – with similar mandates and regulations in play around the globe and considerable variation by state and region. On the OT side, security drivers are highly dependent on the individual organization's processes and requirements. Regulators have not caught up to making FAN security a defined standard. That said, utility OT and IT practitioners do share the universal requirement to be vigilant in assessing and constantly evolving security. Do they have the best available solutions and best practices in place for protection, detection, and real-time response?

There are several common steps that most utilities are taking. Many utilities require encryption of all wireless communication, which protects against the manipulation or theft of sensitive data. Not all encryption is created equal, and advanced cyber hackers using AI assisted algorithms are a threat to old-school mechanisms. Advanced utilities will increasingly incorporate public key infrastructure (PKI), key rotation algorithms, and certificate management to proactively protect FANs against vulnerabilities associated with static, pre-shared keys.

In addition to advanced encryption, another recommendation of NERC-CIP is creating a firewall to extend security around the perimeter of a FAN. Firewalls can then permit essential SCADA and AMI meter communication to operate in the network while blocking unauthorized traffic to penetrate the grid network. Just as with encryption keys, there are advanced firewall capabilities that actively monitor suspicious traffic patterns associated with hacking. Intrusion detection and prevention can identify intrusion patterns and either automatically block a suspected hacker or alert the network operator. And increasingly with industrial IoT, that visibility and control must extend to the edge of the network and to thousands, if not millions, of end points.

Figure 4: Number of utility FANs



While approaches to FAN deployment and the level of sophistication of FAN security currently varies, it is clear from our survey that the number of field area networks utilities have deployed are significant. 44% of utilities have already deployed 3 or more FANs across their grid and asset base. IT and OT teams need to be conscientious of the reality that as more FANs are deployed across the system, the complexity of adequately addressing the security threat landscape expands accordingly.

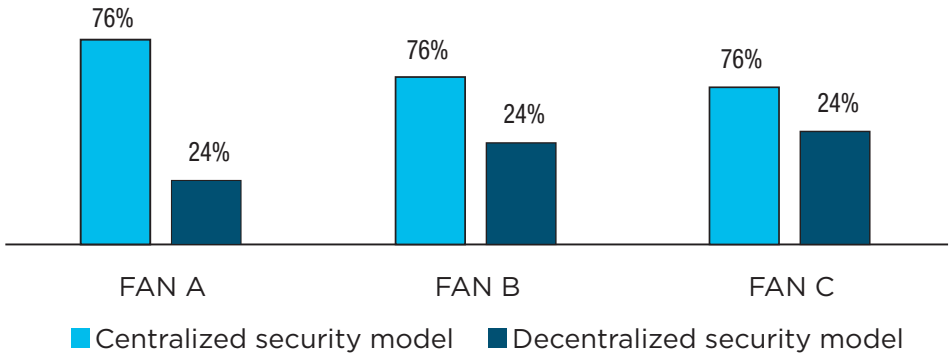
Learning from leading utilities who have actively deployed FANs over the past few years will be essential for long-term grid security. Most utilities are still looking to develop new field area networks, and AMI meters, SCADA, distributed automation, distributed generation, energy management systems, and mobile workforce communications were the main priorities for deployment. IT and OT teams will need to develop strategic best practices for identifying vendor solutions and internal processes to harden the grid against security threats. Zpryme addresses these principles, and gives specific recommendations later in this paper.

Figure 5: Priority of FANs

FAN A	FAN B	FAN C
• AMI meters	• Distribution automation	• Mobile workforce communications
• SCADA	• AMI meters	• SCADA
• Distribution automation	• SCADA	• AMI meters
• Home area networks/ energy management systems	• Mobile workforce communications	• Distributed energy storage
• Distributed generation	• Internet of Things (IoT)	• Electric vehicle infrastructure

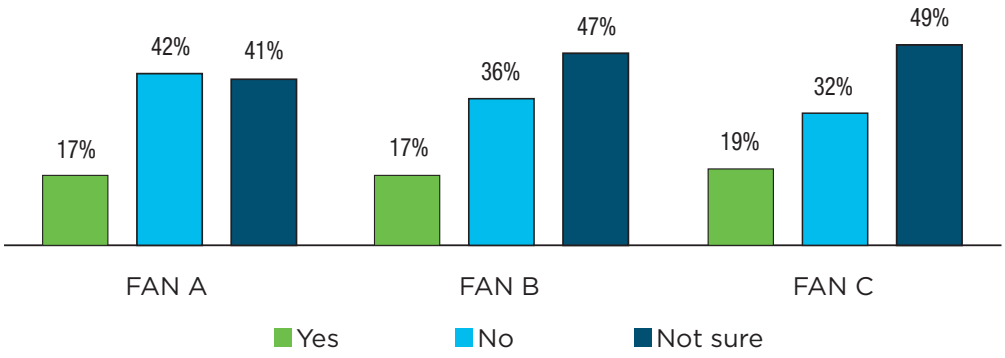
Regardless of the type of system deployment, one of the most common concerns facing utilities is how to balance the security of a central control network with the flexibility and speed associated with distributed FAN security. Currently, utilities are favoring the centralized approach, which traditionally has ensured that a single, protected database and source of truth is used to authenticate users and devices. However, technology shifts are opening the possibility that a distributed security model can provide reduced system vulnerability, greater resiliency, and network flexibility to improve asset operations throughout the grid. Our research shows utilities are successfully leveraging FANs for next generation digital utility operations –integrating new sources of energy and offering innovative services for new revenue streams, prosumer demands, and new customer experiences. The FAN's ability to utilize a single, IP-based network for multiple services inherently involves multiple subsets of IT staff and diverse operational owners from different parts of the utility organization. With the emerging technology, each can take greater responsibility for their respective role of provisioning, securing and managing the network devices, and data resulting in efficiencies and cost savings while offering methods of IT-OT collaboration for better security. Leading utilities are achieving distributed management and security and aspiring to zero-touch provisioning of routers and other devices, and real-time performance monitoring and troubleshooting.

Figure 6: Security model of FANs



As the grid becomes a more complex system that must integrate distributed generation and reliably balance customer energy needs, a decentralized security model begins to make more sense. Complexity in the grid requires multi-layer management to provide embedded communication and distributed intelligence at the edge. In this system, new security standards will focus on security to each end-point and improving interoperability in mesh networks. Grid speed and reliability must never come at the expense of security, but advanced network management monitors all system traffic for suspicious patterns and prevents unauthorized access.

Figure 7: Consideration of distributed security model for FANs



Zpryme found that utilities feel adequately prepared for current FAN security needs and trust the current security systems. This confidence should be tempered by an understanding that threats are continuously evolving, and a vigilant enterprise-wide approach is necessary to stay ahead of hackers. Utilities have benefited from a greater regulatory emphasis in the wake of successful hacking of generation, transmission, and distribution networks globally. Furthermore, utility security leaders have kept close watch of data breaches in other industries. Despite IT and OT utility leaders' best efforts, traditional approaches to FAN security will not protect the grid forever. Innovation, collaboration, and the consistent drum-beat for higher standards are needed to stay one-step ahead of threats. "Somewhat prepared" cannot be good enough. End to end security must be in place for the FAN to respond to threats and breaches. A well-prepared utility will have a plan for before, during, and after a breach. Before a breach occurs, IT teams must be vigilant to harden and monitor systems to block threats or discover them early on. During a breach, IT and OT operators will have to move quickly to detect what has been affected and defend the overall network infrastructure. It is critical that utilities move quickly to quarantine systems and mitigate potential damage. Finally, a post-mortem is required to remediate any damage and harden the system against future attacks.

Figure 8: Trust in security of FANs

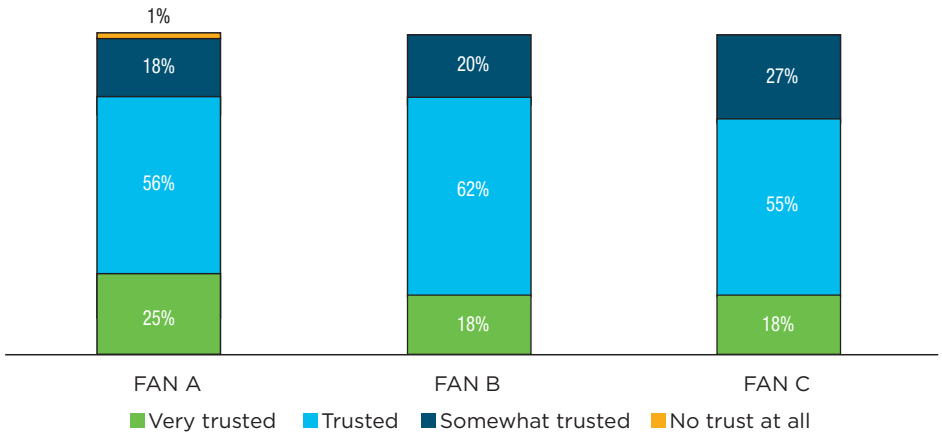
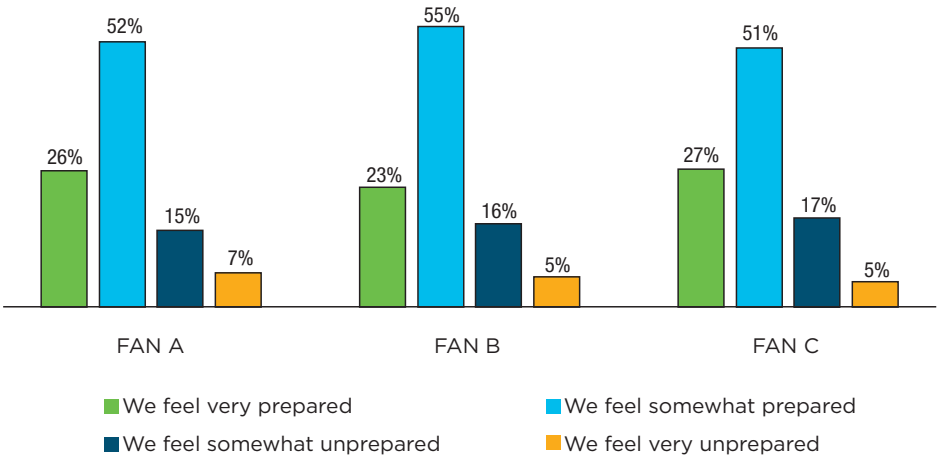


Figure 9: Preparedness for security needs of FANs



Organizational Strategy and Systemic Challenges to FAN Security

FAN security requires an organizational response that prioritizes three strategic pillars across IT and OT business units.

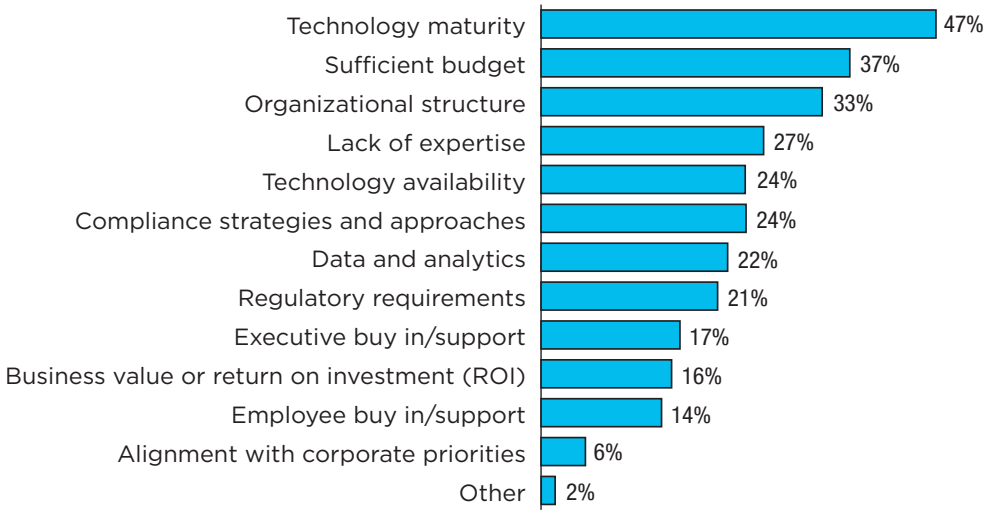
1: The first pillar is device and platform access control. Technology systems must ensure that security is designed into every end-point on the grid. Furthermore, dynamic authentication for every user, device, and application that accesses a field area network must be controlled. As FANs become more prevalent, the need to control them and to access and move the data those systems produce at the grid edge will require a holistic approach of central and distributed security based on device and platform control.

2: The second pillar is absolute data security and confidentiality for every smart meter, IoT, distributed automation, and distributed generation device. This requires communications technology that deploys multiple layers of encryption.

3: The third pillar of effective FAN security is advanced threat detection. Having well-established policies for managing grid operations will allow for threat detection technologies to monitor discrete systems for abnormal communication patterns and automatically block suspicious activity.

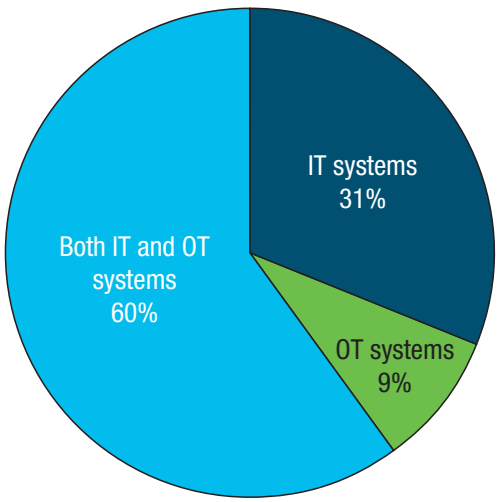
These principles provide an organizational framework for utilities to approach FAN security, but Zpryme found that many utilities are still asking, "How much security is enough?" Utility data, IoT, analytics and automation are creating opportunities and challenges. In this era of the smart grid and digitization, leaders must routinely ask, "how are we monitoring the data flowing through the grid? How are we inspecting the data flowing through the network?". Thoroughly answering these questions necessitates heightened collaboration between IT and OT in order to lead with a real strategy for FAN security.

Figure 10: Top 3 challenges for FAN security Note: % of respondents who selected an answer option in his or her "top 3"



Utilities of all sizes struggle to answer those fundamental strategic questions. As CTOs and COOs develop long-term plans for FAN security, two major categories cause the biggest challenges. The first is technology based: technological maturity, technological availability, and adequate analytics. Grappling with a rapidly changing technological landscape that presents new threats on a seemingly daily basis can seem particularly daunting. Ultimately, the organizational category is the biggest roadblock facing utilities. Developing a sufficient budget, overcoming a lack of expertise, developing a compliance strategy, and outlining an effective organizational structure will lead to competent decisions around technology deployment. Utilities must proactively form trusted advisor relationships with a range of flexible partners and technology vendors. The best utility vendor relationships will be technology and process driven. Vendors that offer integrated networking, security, and data management expertise to uniquely arm utility leaders to bridge IT and OT perspectives are key to secure digital transformation, to simultaneously address both technical and operational control requirements, and to meet the differing decision criteria. With both parties at the table, modular security solutions can be set in motion now while equipping the organization to expand security elements as needed for the future. The utility is more empowered to efficiently and cost effectively expand and adeptly turn off and on security elements with the flexibility required to transform and thrive with the new digital utility model.

Figure 11: Current focus of cyber-attacks



Making those competent decisions requires an understanding and acknowledgment that cyber-attacks menace both IT and OT FAN systems. Utilities are increasingly moving to a model where IT and OT personnel share the responsibility for FAN security. But, there are structural impediments to some utilities making this leap.

That common barrier and frustration with the legacy siloed security approach is reflected in a recent comment from one utility representative: "As a municipal utility, my agency is integrated into the city government for IT Services. OT services are a utility responsibility. Close coordination is needed and rapidly evolving threats are a challenge for a governance structure with weeks to months' procurement cycle and decision-making process."

Figure 12: Overall responsibility for FAN security

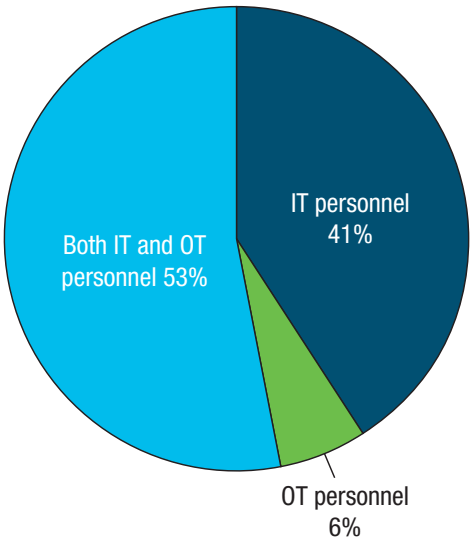


Figure 13: Responsibility for FAN budget decisions

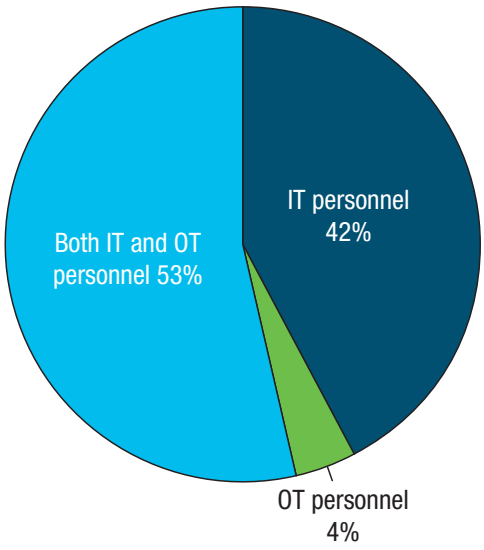
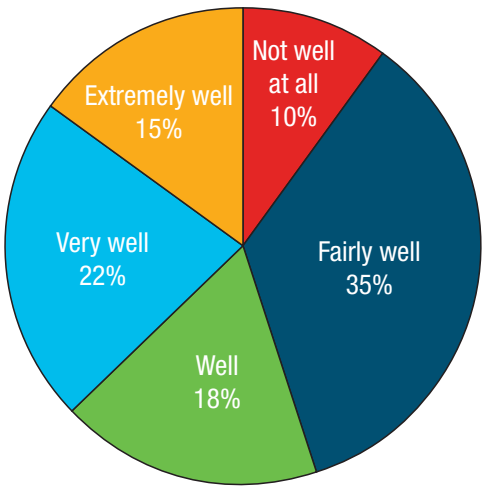
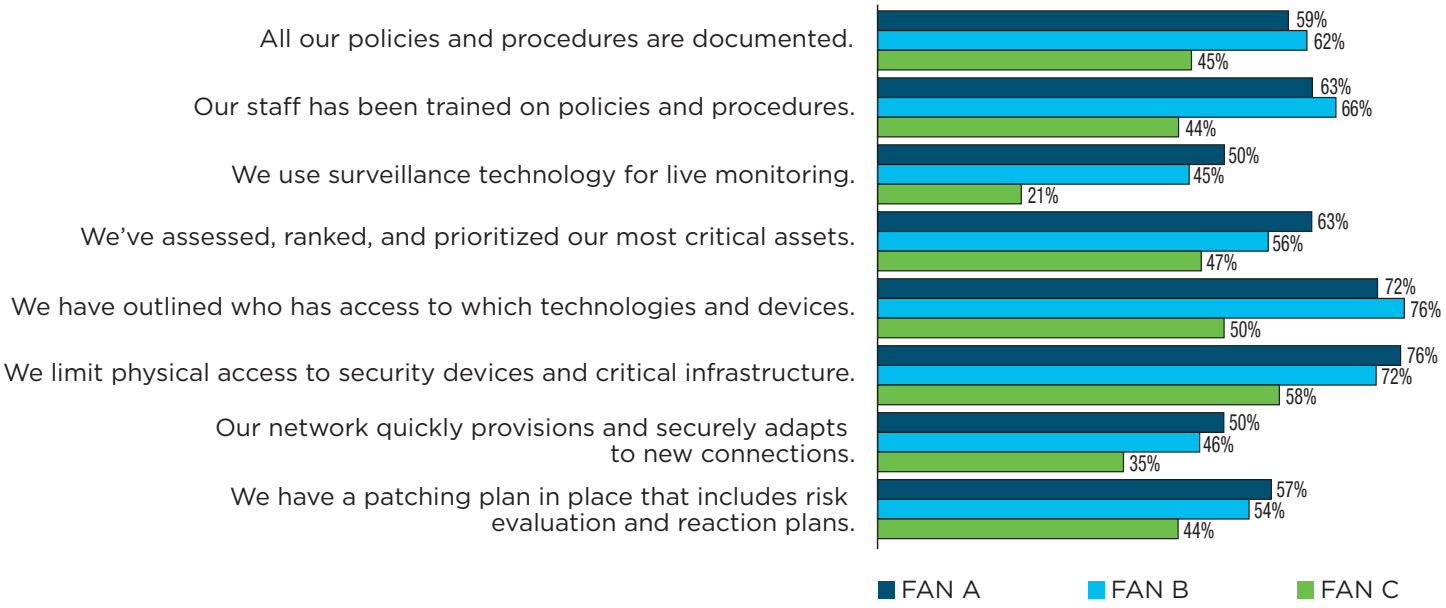


Figure 14: Efforts of IT and OT personnel working together on FAN security



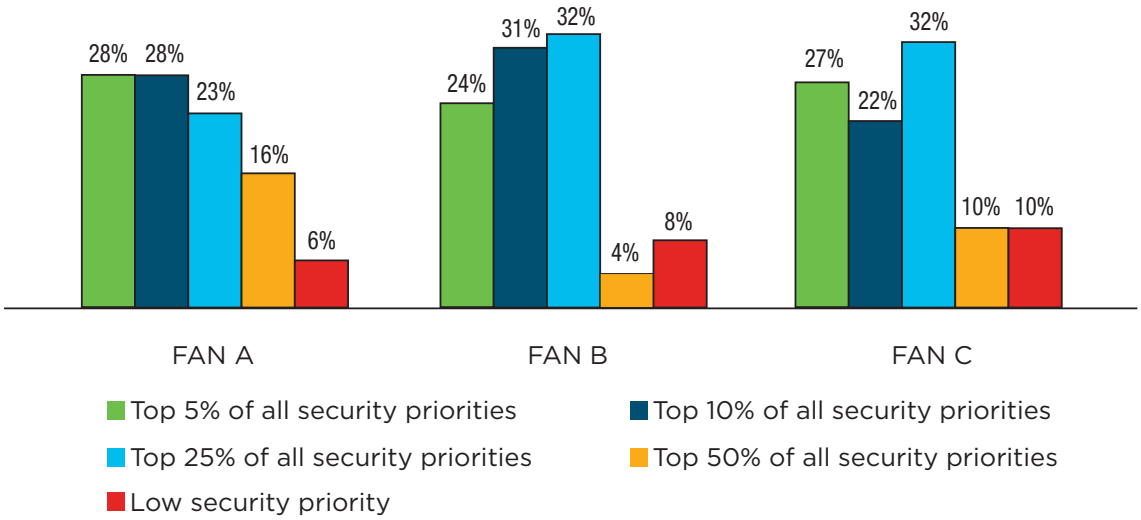
Even those utilities that recognize the importance of joint decision making still have room for growth. Only 37% of utilities rate their coordination efforts as working together Extremely Well or Very Well.

Figure 15: Procedural, physical and electronic security efforts for FANs *Note: % of respondents who agree with the statement



Despite these sobering numbers, there are still some significant positives to take away. Utilities are prioritizing FANs as a significant area of attention. The vast majority of utilities rank their FAN systems in the top 25% of all security priorities. This prioritization will ultimately lead to more comprehensive policies and a technology stack that dynamically provides security throughout the grid.

Figure 16: Security priority of FANs



Conclusion

Field area networks have become an essential communication system to improve performance throughout the grid. As the grid becomes more complex, FANs will form the foundational backbone connecting essential systems like AMI meters, SCADA, distributed automation, and distributed generation. However, because FANs rely on a variety of wireless communication technologies, they are increasingly vulnerable to physical and cyber-attacks. For a utility and today's advanced grid, it's much more than saying, "we need to ensure we stay in compliance and to shore up security for a single network." Utilities need to have a living and evolving end-to-end strategy to secure the current state of the utility systems and simultaneously prepare to secure tomorrow's critical infrastructure. Zpryme recommends five key steps a utility should take to ensure FAN security:

Recommendations

1. Develop a coordinated strategy across the enterprise that is based on the three pillars: access control, data security, and advanced threat detection.
2. Develop a coordination plan and responsibility matrix between IT and OT departments within the utility.
3. Identify and engage a technology partner that prioritizes FAN and grid security.
4. Develop a threat prevention plan that is focused around access control, data security and consistent monitoring.
5. Develop a crisis management plan for before, during and after a security breach. This will allow the utility and technology partner to respond more effectively during a cyber security event.

They must embrace managing a proliferation of utilities applications and the data movement from machine to machine dialogue, machine learning and distributed edge computing capabilities. And utilities must focus on complete visibility into how they are protecting and defending against the potential of attacks on both legacy and next generation systems. The challenge at hand is to ensure that enterprise-caliber end-to-end security is truly integrated into flexible and resilient grid solutions across the FAN infrastructure.

Utilities must develop processes and seek out technology partners committed to open standards based on the three principles of FAN security: device and platform control, data security, and threat detection.

As utility leaders know all too well, there's no such thing as absolute static security – so IT and OT leaders must be prepared by the moment for a coordinated response with the right technology and tools to take pointed action when intrusions and attacks happen. They must prepare now for how to respond together. Utilities must develop processes and seek out technology partners committed to open standards based on the three principles of FAN security: device and platform control, data security, and threat detection. The processes must account for collaborative IT and OT multi-layered management. The technology solutions should focus on embedding security to every node throughout the grid and distributed intelligence that promotes resiliency.

FAN security must include real-time monitoring of everything occurring across a mesh cellular or other network activity while delivering insights on troubleshooting and recommended actions that break down siloes for managing the utility at a higher and more aligned level. FANs represent the connective tissue that binds the smart grid together, consequently ensuring their security must be of the highest priority.

For more information on how you can strengthen your Field Area Network security, contact Cisco at:
http://www.cisco.com/go/utilities

With Cisco, you can digitally transform utility operations – from headquarters to substations to critical systems and diverse IoT sensors in the field at the edge of the network; from production to transmission; and from distribution to the meter. Utilities are modernizing and securing networks and communications, automating industrial controls, improving data management and visibility for real-time decision making and utilities value. Cisco expertise can help you eliminate information silos and securely connect machines, assets, and people for agile and resilient operations. With our innovative and flexible solutions, utilities are delivering the grid of the future today – with a strong network foundation that is interoperable, open, and standards-based for:

Field Area Networks (FAN): Enables pervasive monitoring and control of energy distribution networks. (AMI, DA, DER, Quality of Service, Workforce Automation, Streetlighting, Direct Load Control, and more)

Substation Automation: Modernizes the grid with multiapplication networks for reliability, compliance, protection, remote diagnostics / maintenance. Provides multiservice network framework for optimized intra-substation communications.

Utility WAN: Enables deployment of next-generation MPLS teleprotection and SCADA converged IP communications networks. Migrates critical system control infrastructure to the IP world.

Distribution Automation (DA): Reduces costs with intelligent distribution across the grid to substations and meters. Scalable network management achieves distribution feeder efficiency and reliability with end-to-end security.

Grid Security: Detects / prevents internal and external attacks on control systems. Manages access, improves cyber and physical security to meet regulatory requirements and improve incident response.

Mobile Workforce: Improves worker productivity and the customer experience with router, mobility, and wireless innovations. Connects fleet, assets, and field workers with a secure, mobile, and intelligent enterprise network.