ISSUE 1, 2018

communicator

change

In this issue:

EMA®

Table of Contents

Get Your *communicator* Electronically

Communicator magazine is available in electronic format. Contact us at **marketing@ema-inc.com** if you prefer to receive a PDF of the magazine via email. Interested in both formats? Contact us, and we will send both to your attention.

As an innovative management and technology consulting firm, EMA develops solutions in anticipation of changing market needs and brings new business concepts to its clients, which include utilities and government organizations.

With offices throughout the United States and Canada, EMA is headquartered in St. Paul, MN, and has provided clients with solutions since 1975.

Your comments are always welcome at marketing@ema-inc.com.

Terry Brueck	President/CEO
Elissa Lindberg	Design, Layout, & Graphics
Lisa Steidl	Editor
Caroline Whaley	Writer

EMA, Inc.
2355 Highway 36 West, Suite 200
St. Paul, MN 55113-3819
651.639.5600

marketing@ema-inc.com
ema-inc.com

Taming Turbulence

Lynne Powers
Vice President

Is your utility poised to manage disruptive changes?

Today industries are witnessing major shifts at an exponential rate. Retail is shifting from large brick and mortar stores to online shopping. The banking industry has dramatically shifted to online services and mobile application capabilities. And personal communication has shifted from landlines and basic cell phones to smartphones that allow us to take photos, stream videos, and stay connected around the clock. Some of these transformations, like the general pace of new technology, work force transitions, and cyber threats create intense demands on utility leadership.

How will utilities respond to the challenge of disruptive changes? This issue of Communicator features expert commentary on issues facing utility management, focused through a change management lens. Sharon Peters discusses the impact of the changing workforce (page 7), perhaps one of the most disruptive changes the utility industry will experience in the next decade. With a large percentage of baby boomers in the workforce and a tremendous increase in retirements, utilities will need to focus on identifying skill gaps, actively engage in succession planning, and develop employees. Ed Tirakian highlights the impending changes enabled by new technologies (page 10) such as predictive analytics, the "internet of things," machine learning, and artificial intelligence. Bob Reilly provides insight on one of the most challenging issues for utility CIOs: protecting the utility from cyber threats (page 15). Due in part to persistent high-profile breaches, security has emerged as the number one priority for IT management. EMA understands that meeting the challenge of these disruptive changes is not possible without planning for the human side of change. Leslie Willett Black, EMA's change management expert, explains how true change happens through individual effort and not only at an organizational level (page 3).

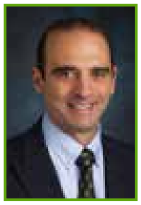
EMA has been assisting utilities manage change for more than 40 years and we are excited to help utilities meet the challenge of these disruptive changes. These are challenging but exciting times!

Contributors to this Issue

(Listed in order of article appearance)

Leslie Willett Black
Senior Consultant

Sharon Peters
Director



Ed Tirakian
Principal Consultant

Bob Reilly
Principal Consultant

Have your technology and process improvement projects delivered the desired results? Whether it's processes, job roles, reporting structures, systems, or performance measures, large-scale utility projects require people to adopt change. Ad hoc communication and training alone may not produce the intended outcome.

Leslie Willett Black, EMA's change management expert, articulates the paradox of change. "Change is both simple and complex. Simple, because people are typically not opposed to change. We adapt every day to changing circumstances; if a road is closed, we follow the signs and take an alternative route. Complex, in that each person's barriers to change are unique and everyone moves through these perceived barriers at different paces. The trouble begins when we are missing the facts and tools needed to change. The fear of the unknown takes over, creating resistance, frustration, and anger. "

Leslie believes two critical components are missing: linking staff with leadership's vision, and a plan to support staff members through the natural process of adopting change. What's needed are change leadership skills and a systematic approach to managing the people side of change. This is where change management comes in.

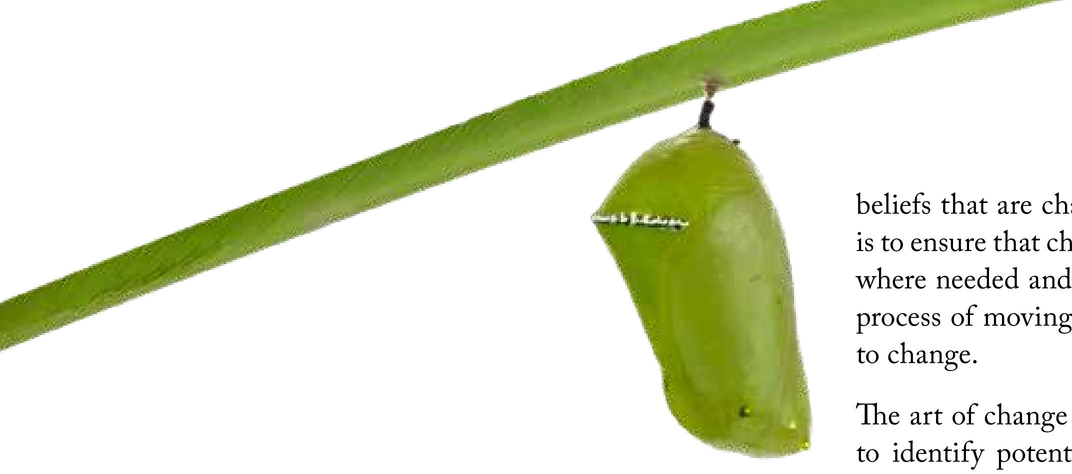
Sustained Improvement Is Impossible Without Change Management

by Leslie Willett Black

What is change management? Change management is a scalable methodology focused on planning the people side of a change initiative. It employs a systemic application of tools and methodologies mobilizing people to realign activities to meet the desired change outcomes.

But what does that mean?

Every utility project involving major system or process changes requires people to change how they do their jobs. The people side of this change is often associated with uncomfortable emotions and behavioral resistance. Ignoring or denying human change factors creates drama and resistance in a project, and ultimately impacts the success of the initiative. Change management provides a structured approach to addressing human change factors.

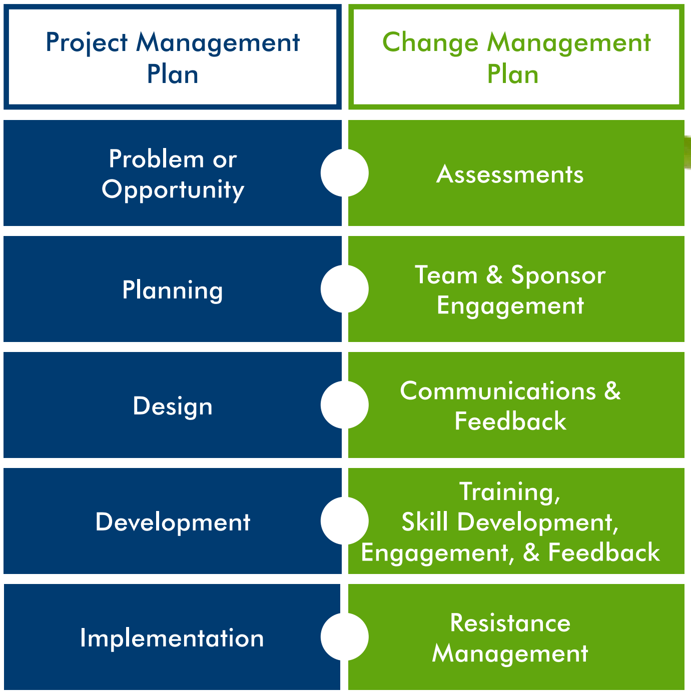


Integrating Change and Project Management

Just like a traditional project management plan, a change management plan includes activities and measurable outcomes. The project management plan focuses on the technical side of change, while a change management plan focuses on the needs of the people who are key to successfully implementing and sustaining the change.

We can summarize change management into a few key categories like leadership, communication, training, and sustainability. It is the translation of all the nuances and sub-texts within each of these categories, however, that impacts the results and return on investment.

The change management plan identifies and categorizes the change impact, taking multiple factors into consideration to assess the change impact in each group. These include processes, systems, reporting structures, performance measures, compensation, job role, critical behaviors, location, tools, and any attitudes or cultural beliefs that are challenged with the change. The purpose is to ensure that change management activities are focused where needed and to the degree required to facilitate the process of moving people through their personal barriers to change.



Project Management Plan	Change Management Plan
Problem or Opportunity	Assessments
Planning	Team & Sponsor Engagement
Design	Communications & Feedback
Development	Training, Skill Development, Engagement, & Feedback
Implementation	Resistance Management

Figure 1: A change management plan supports and complements the project management plan.

The art of change leadership lies in strategic engagement to identify potential barriers in the areas of awareness, desire, ability, and the sustainability of the new behavior. It requires a different skill set than managing operations. Building these organizational change skills is like investing in professional development; you may not immediately see a return on these investments, but over time your organization's capacity for change will expand dramatically.

When Is a Change Management Plan Required?

So how do we decide whether a project needs a change management plan? A change management plan is vital to the success of any project that requires people to change how they work. The change management scope is proportionate to the size or impact of the change. A purely technical system upgrade, for example, requires minimal change planning compared to a new core system implementation.

Once we've decided our project requires a formal change management program, we must decide where to apply it. The change management program is applied throughout the project, engaging the groups impacted. The key

consideration is the impact of the changes on each group. The size of the group doesn't matter; sometimes the smallest group is impacted the most.

Typically, in the current state, staff members are very comfortable with the processes and what is expected from them in their daily job functions. They generally feel confident and may be considered experts because they know what they are doing and when and how to do it. It is important to understand that staff members often fear the loss of competence in their jobs. Most of them want to do a good job and want processes and tools to make that happen.

Communication is key. If staff members don't have the facts about the change, the water cooler effect kicks in to fill the gaps. Often this results in misinformation and creates unnecessary confusion and fear. Someone who doesn't have the proper tools or who doesn't know how to use the tools properly may find an undesirable work-around. If staff doesn't understand the direction management wants the change to take, a well-meaning team member might step in and provide an alternative direction. These actions are all understandable coping mechanisms, but they create chaos, rumors, resistance, and all the emotionally difficult things everyone wants to avoid on projects.

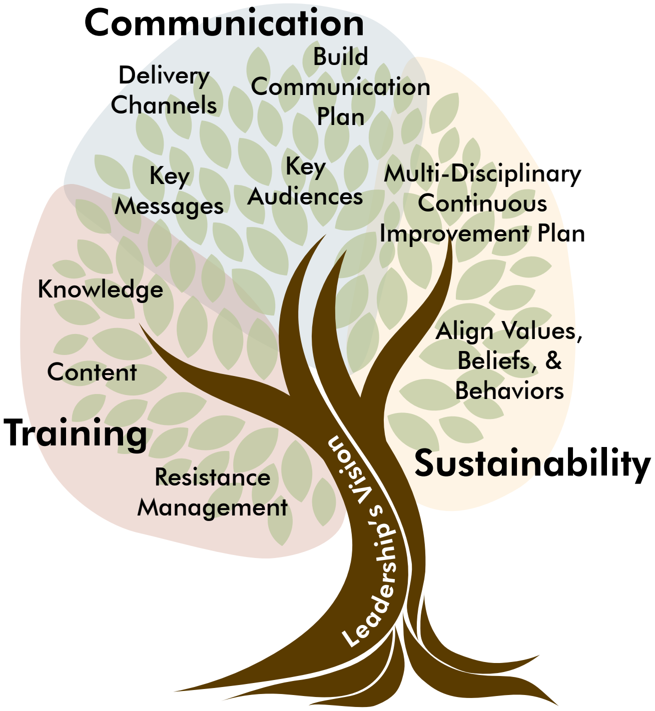


Figure 2: The change management plan's components of communication, training, and sustainability are rooted in leadership's vision for the project outcomes.

Facilitating change is like gardening. The benefits are realized after a lot of nurturing. The quality of the yield is based on the time and effort in preparing the soil, the nutrients, and the care to nurture the growth.

Change Management Plan Framework

A change management plan provides a framework to ensure everyone understands the project vision and how the project connects to leadership's strategy. When team members understand why the project is important, the desired impact, and are provided with factual updates, the barriers to change start to crumble.

A successful change management framework includes three main components to support leadership's vision: communication, training, and sustainability.

The **communication** component starts when we kick off the project and lasts through completion. Key messages are defined and delivery methodologies are aligned with the content. Content is targeted to the audience. The communication plan requires a multi-disciplinary implementation strategy. Not everyone accepts and adopts change at the same pace or interprets the message in the same way. We know that one approach doesn't work for everyone, so the plan includes monitoring, along with strategies for filling the gaps where needed.

The **training** component of the change plan extends beyond mere knowledge. It ensures staff builds confidence and proficiency in the new system or processes. A staged training approach and personal learning plans can help build comfort levels and buy-in. The faster everyone is back up to speed in their jobs, the quicker everyone feels better about the change and the sooner the desired benefits are realized.

The **sustainability** component focuses on project results and continuous improvement. There will always be some steadfast resistors. The change strategy identifies options for dealing with this resistance. A structured strategy brings a calm, clear, factual approach to the situation. Lack of planning or denial that resistance is a reality breeds frustration, bringing down even those who strongly support the project. Sustainability is built into the project, and change management plans are based on the overall project objectives. If you are expecting new outcomes, yet still measure based on the old reality, what is the incentive to change?

Facilitating change is like gardening. The benefits are realized after a lot of nurturing. The quality of the yield is based on the time and effort in preparing the soil, the nutrients, and the care to nurture the growth. The value of change management is what endures after the project ends. It can be the difference that moves a project along the continuum from good to great and from failure to success.

Change is not something that is done to you, it is something you choose to do. Everyone affected by the project's changes has a role and responsibility to engage. Employees have a personal learning plan designed to move them through their individual barriers to change; management has the additional responsibility of supporting their employees, as well as their own personal learning plans. Most importantly, leaders must understand and embrace their roles as effective change sponsors.

Remember, a project is successful when staff accepts and uses the new system or process as envisioned.

Leslie Willett Black is certified in the Prosci methodology, an internationally recognized methodology that provides a structured approach to organizational change management. Leslie integrates Prosci's body of knowledge when designing the plan to "manage the people side of change in a structured and repeatable way."

Is your utility already taking on new responsibilities? Struggling to fill critical positions? Recognizing the impacts of recent retirements? Looking for ways for your workforce to get more engaged with your technology systems?

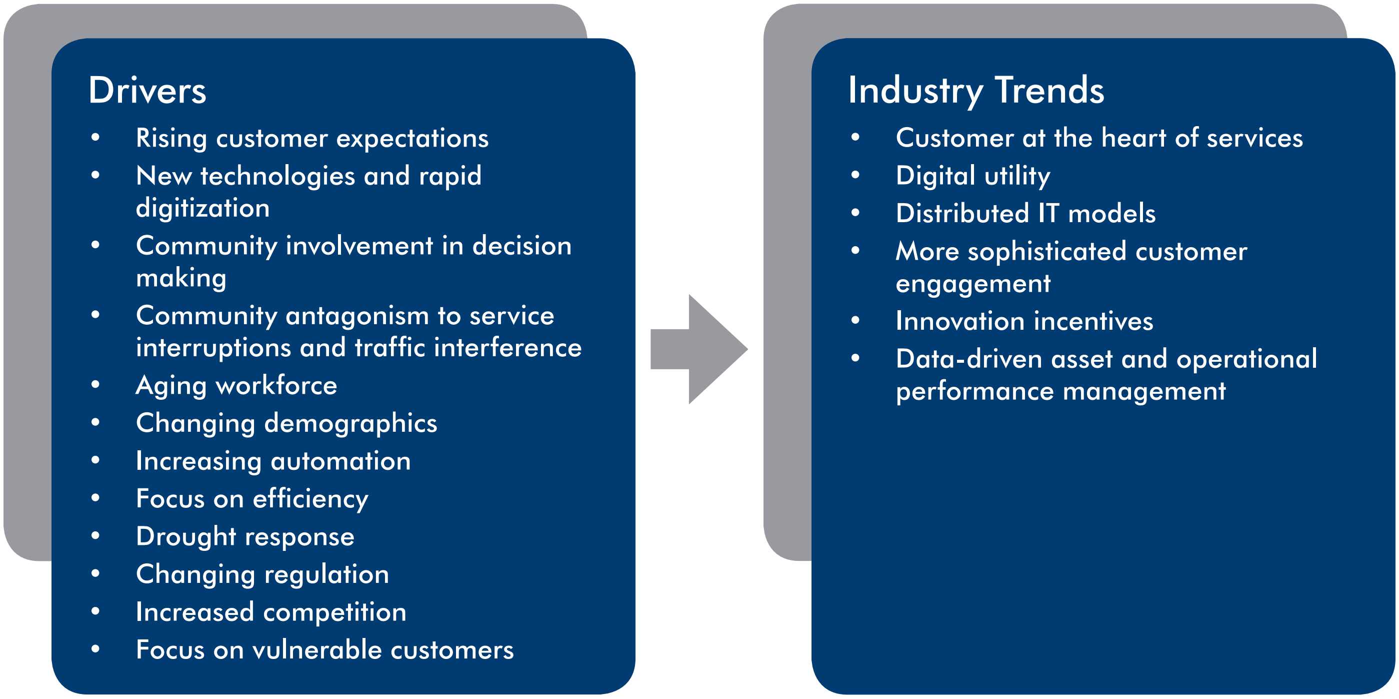
Meeting the Challenge: Preparing for a Changing Workforce

by Sharon Peters

North American utilities find themselves in the middle of a major workforce transition. Some of today's biggest concerns were identified as issues more than ten years ago, when changing demographics, impending retirements, and potential knowledge losses were seen as a perfect storm threatening water and wastewater service delivery. The Great Recession delayed and softened some of the predicted effects, but change is accelerating now that the economy has recovered.

Baby boomers are retiring. Succeeding generations are considerably smaller and want different types of career opportunities. The U.S. is close to full employment and competition for dedicated employees with strong technical and customer service skills is fierce. Some types of positions and certain markets are particularly constrained. New generations of leaders and workers are bringing different expectations and values to the workplace.

New technologies are changing how traditional utility work is done. Five years ago, it was still common to see utility workers resisting computers. Smartphones and tablets have changed those attitudes. Everyone wants to be able to interact with their phones at work the way they do at home. They want to be fully mobile and access reference information and perform data entry anywhere.



Drivers

- Rising customer expectations
- New technologies and rapid digitization
- Community involvement in decision making
- Community antagonism to service interruptions and traffic interference
- Aging workforce
- Changing demographics
- Increasing automation
- Focus on efficiency
- Drought response
- Changing regulation
- Increased competition
- Focus on vulnerable customers

Industry Trends

- Customer at the heart of services
- Digital utility
- Distributed IT models
- More sophisticated customer engagement
- Innovation incentives
- Data-driven asset and operational performance management

Figure 1: Drivers of change and industry trends (WSAA and WE&RF 2017)

Emerging Technologies Disrupting Other Industries and Expected to Impact Water and Wastewater Utilities

Emerging Technology	What is it?	What does it mean for water and wastewater?
Messaging/ chat-bots	A computer program that conducts a conversation via auditory or textual methods.	Employed by other types of utilities and cities for customer service and information acquisition, it may become a customer expectation for water.
Autonomous vehicles	Vehicles relying solely on automation.	Lower cost and improve performance of supply chain; provide access to parts of utility systems not readily accessible now at lower cost.
Augmented/ virtual reality	A technology that superimposes a computer-generated image on a user's view of the real world, thus providing a composite view/computer generated scenario that simulates a realistic experience.	Simulation of flow in plants and pipe networks; enhance customer engagement through virtual tours; complete 3D engineering design reviews; safety and operator training simulations.
Blockchain	A continuously growing list of records, called blocks, linked and secured using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data.	Peer to peer supply networks; billing and payment transactions; trusted sharing of operational and customer behavior data among utilities.
Quantum computing	A computing technique using quantum mechanical phenomena, including superposition of states. Has the potential to solve certain problems much more quickly than binary digital electronic computers based on transistors.	Asset degradation modeling; distribution system optimization; supply chain optimization; customer behavior modeling; machine learning.
Artificial intelligence	A system of devices that perceive their environments and take actions that maximize the chances of successfully achieving goals. Aspects include: reasoning, knowledge representation, planning learning, natural language processes, perception, and the ability to move and manipulate objects.	Predictive analytics to save operational costs and reduce risks through real-time optimization of assets. Better planned and executed capital projects; real-time water loss minimization; personalized customer portals.
Internet of things (IoT)	The network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these objects to connect and exchange data.	Smart meters and other equipment capable of exchanging much more information at lower costs. These can be used by a utility or by its customers to obtain enhanced information about water usage, electricity usage, operating environment factors, and equipment health.
3D printing	Processes in which material is joined or solidified under computer control to create a three-dimensional object. Also called additive manufacturing.	Produce water system assets and equipment at much lower cost than conventional methods; may increase the life of assets through use of alternative materials; can detect and repair corrosion in pipes.
Platform economies	Economic and social activity facilitated by technology frameworks. Big data, new algorithms, and cloud computing will change the nature of work and the structure of the economy.	Water and energy efficiency; disruption of traditional utility business models; changing work schedules.
True global connectivity	Personal mobile technology can connect every human being to knowledge, markets, services and communities.	Role-based dashboards, analytics and decision support available for multiple roles for both utilities and customers anywhere.

Figure 2: These emerging technologies have already begun disrupting other industries and are expected to have significant consequences for water and wastewater utilities in the coming years.

Enabler 1:
Resilience
Flexibility, agility, critical thinking

Enabler 2:
Data and Analytics
Digital literacy, internet of things

Enabler 3:
Leadership
Change management, strategic planning, learning mindset, communication, culture

Enabler 4:
Customer
Service, culture, experience, focus

Enabler 5:
Technical Skills
Network operation, engineering, risk management, general operations, knowledge management

Enabler 6:
Delivery Models
Contracting, commissioning, outsourcing, insourcing

Enabler 7:
Entrepreneurship
Innovation

Enabler 8:
Collaboration
Partnerships within the water sector, partnerships with other sectors

Figure 3: Key water utility enablers (WSAA and WE&RF 2017)

Organization structures and job roles are evolving to help the water industry adapt and new skills are needed. New roles help address new business models, new data capabilities, innovation drivers, and more interactive customer service models. Utilities are forced to consider non-traditional alternative scenarios to meet their workforce needs, including temporarily filling positions with consultants or other change agents, contracting work, combining or dividing traditional roles, and entering into shared service partnerships with other utilities.

In response to water and wastewater utility interest in the workforce transition, the Water Services Association of Australia (WSAA) and the Water Environment and Research Foundation (WE&RF) completed the "Workforce Skills of the Future" project in 2017. The central question this project investigated is how current drivers of change and industry trends (Figure 1) are affecting today's workforce and shaping the knowledge, skills, and experiences that will be needed in the workforce of the future.

As part of the project, U.S. WE&RF members were surveyed to highlight key workforce trends. Almost 70% of the utilities surveyed reported that they are extremely or very confident that they can deliver on their current business objectives with the skills and capabilities of their current workforce. Forecast more than ten years into the future, however, and that confidence level drops to 31%. Potential future gaps were identified in critical thinking, leadership and communication skills, and digital literacy and technical skills. U.S. survey respondents also identified workforce retention, emerging technologies, and increased automation as the top transformational changes most likely to affect their workforces in the next ten years.

A list of emerging technologies that are currently disrupting other industries and expected to affect water and wastewater utilities as well is provided in the table in Figure 2 (facing page), along with descriptions of potential effects.

To help water utilities adapt in a rapidly evolving work environment, the WSAA and WE&RF recommend pursuing eight key enablers (Figure 3) at the individual utility, regional, and national levels.

One thing that hasn't changed in the past decade is that planning and preparation are keys to success. Several utilities are preparing new, future-focused workforce plans or updating previous plans to focus on more flexible organizational design, user-friendly knowledge transfer, and accelerated training and career development. Other utilities are engaging with peers through regional partnerships and national conferences.

More information on the WSAA and WE&RF project can be found by selecting "Intelligent Water Systems" from the Research Areas menu on the WE&RF website at www.werf.org, or by visiting www.wsaa.asn.au/news/workforce-skills-future.

Communications Infrastruc Considerations for the Inte Digital Utility

by Ed Tirakian

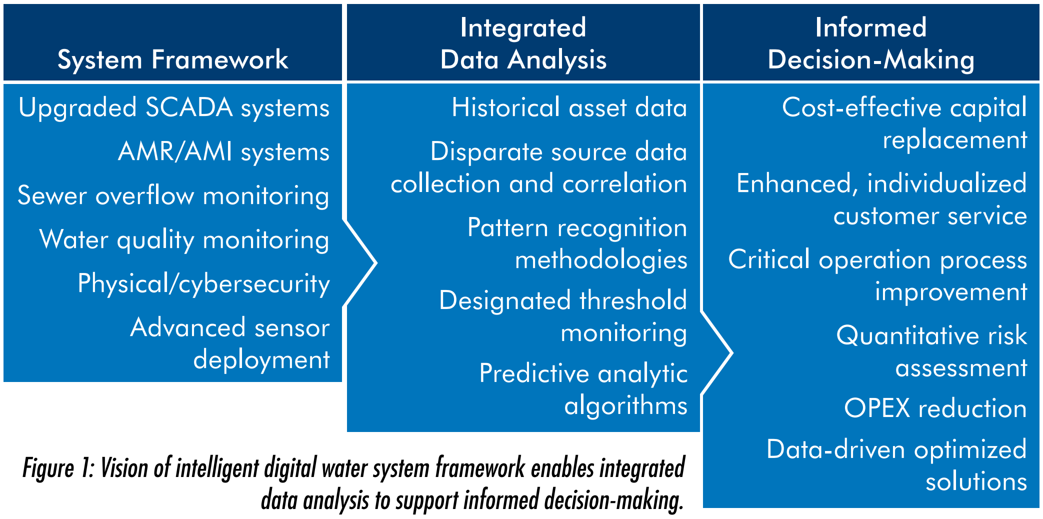
Designing solutions from a strategic and functional perspective to meet current and future needs.

Today's water utility needs increased information and insight across the organization. It requires improved operational efficiency, more responsive customer service, increased asset management insight and preparedness, resource optimization, and real-time monitoring of system and component health and performance. New and evolving digital capabilities transform organizations by enabling increased data collection and analysis, including cross-platform correlation and integration. The contemporary water utility relies on new and evolving intelligent applications and digital solutions to meet these ever-changing information needs.

Any utility embracing this information revolution needs a base framework for gathering and interpreting data and making informed decisions. An intelligent digital water utility platform sits at the core of this framework. Intelligent water systems enable integrated data analysis, which leads to initiatives focused on informed decision-making, which in turn provides the ability to drive effective, optimized solutions. This concept is illustrated in Figure 1.

Utilities' communications infrastructures face increased capability, performance, and functionality demands in this new digital environment. The underlying communications architecture is key to enabling this new digital water utility.

A digital water utility uses smarter intelligent applications to monitor meter readings, water distribution control (SCADA), water quality, and sewer levels and flows. The communications infrastructure must support regulatory compliance, connect to smart city applications such as street lighting control in a secure manner, and be sustainable in the long-term.



System Framework

Upgraded SCADA systems
AMR/AMI systems
Sewer overflow monitoring
Water quality monitoring
Physical/cybersecurity
Advanced sensor deployment

Integrated Data Analysis

Historical asset data
Disparate source data collection and correlation
Pattern recognition methodologies
Designated threshold monitoring
Predictive analytic algorithms

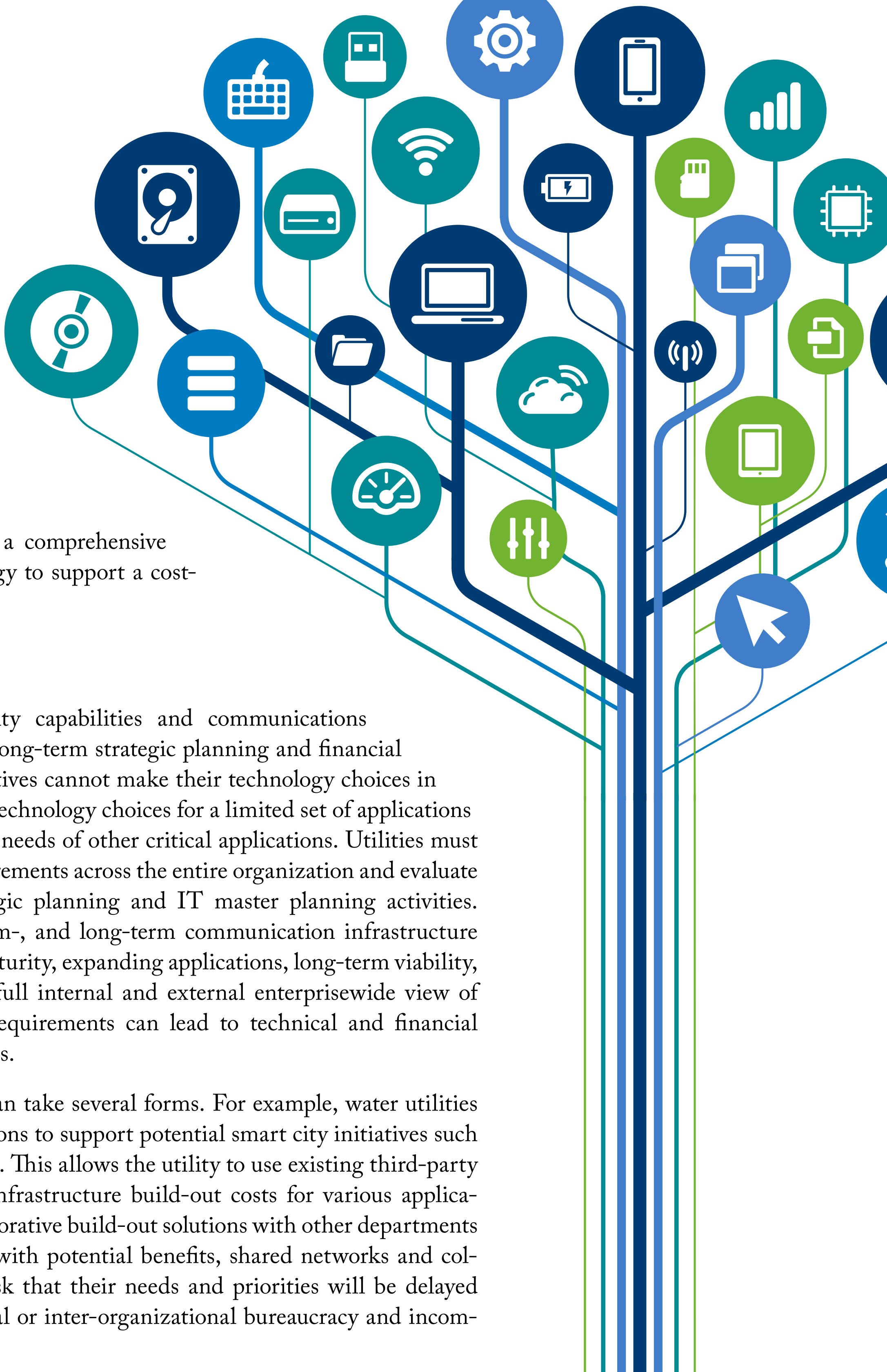
Informed Decision-Making

Cost-effective capital replacement
Enhanced, individualized customer service
Critical operation process improvement
Quantitative risk assessment
OPEX reduction
Data-driven optimized solutions

Figure 1: Vision of intelligent digital water system framework enables integrated data analysis to support informed decision-making.

Monitoring system water quality and managing system pressure across the distribution network in real time will require advanced data collection and connectivity capabilities. These considerations require utilities to look at their infrastructure from three critical perspectives: strategic/financial, technical, and technological.

cture
elligent



Utilities with this vision must have a comprehensive communications infrastructure strategy to support a cost-effective implementation (Figure 2).

Strategic/Financial

Utilities must examine digital utility capabilities and communications infrastructure alternatives through a long-term strategic planning and financial lens. Individual departments or initiatives cannot make their technology choices in a vacuum. The designs that optimize technology choices for a limited set of applications have the potential to compromise the needs of other critical applications. Utilities must consider overall communication requirements across the entire organization and evaluate these needs during high-level strategic planning and IT master planning activities. Utilities must analyze short-, medium-, and long-term communication infrastructure options considering costs, security, maturity, expanding applications, long-term viability, and other factors. Failing to take a full internal and external enterprisewide view of the communications infrastructure requirements can lead to technical and financial shortcomings in the deployed solutions.

Capitalizing on the enterprise view can take several forms. For example, water utilities can explore shared infrastructure options to support potential smart city initiatives such as streetlights and traffic management. This allows the utility to use existing third-party networks to avoid or reduce initial infrastructure build-out costs for various applications. Utilities can also consider collaborative build-out solutions with other departments and municipal organizations. Along with potential benefits, shared networks and collaborative efforts increase utilities' risk that their needs and priorities will be delayed or compromised by inter-departmental or inter-organizational bureaucracy and incompatible priorities.

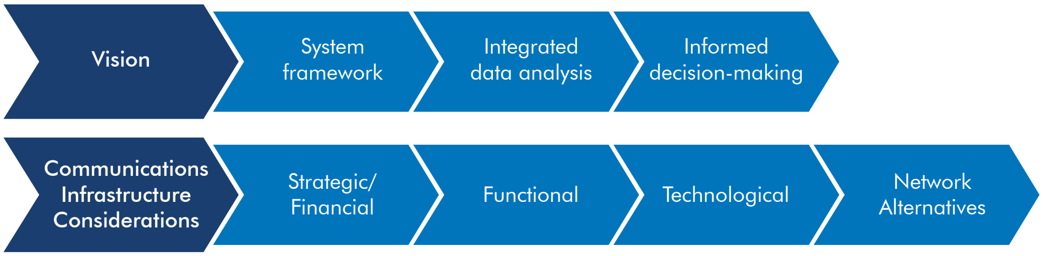


Figure 2: A communications infrastructure strategy is necessary to affordably implement the intelligent utility vision of informed decision-making.

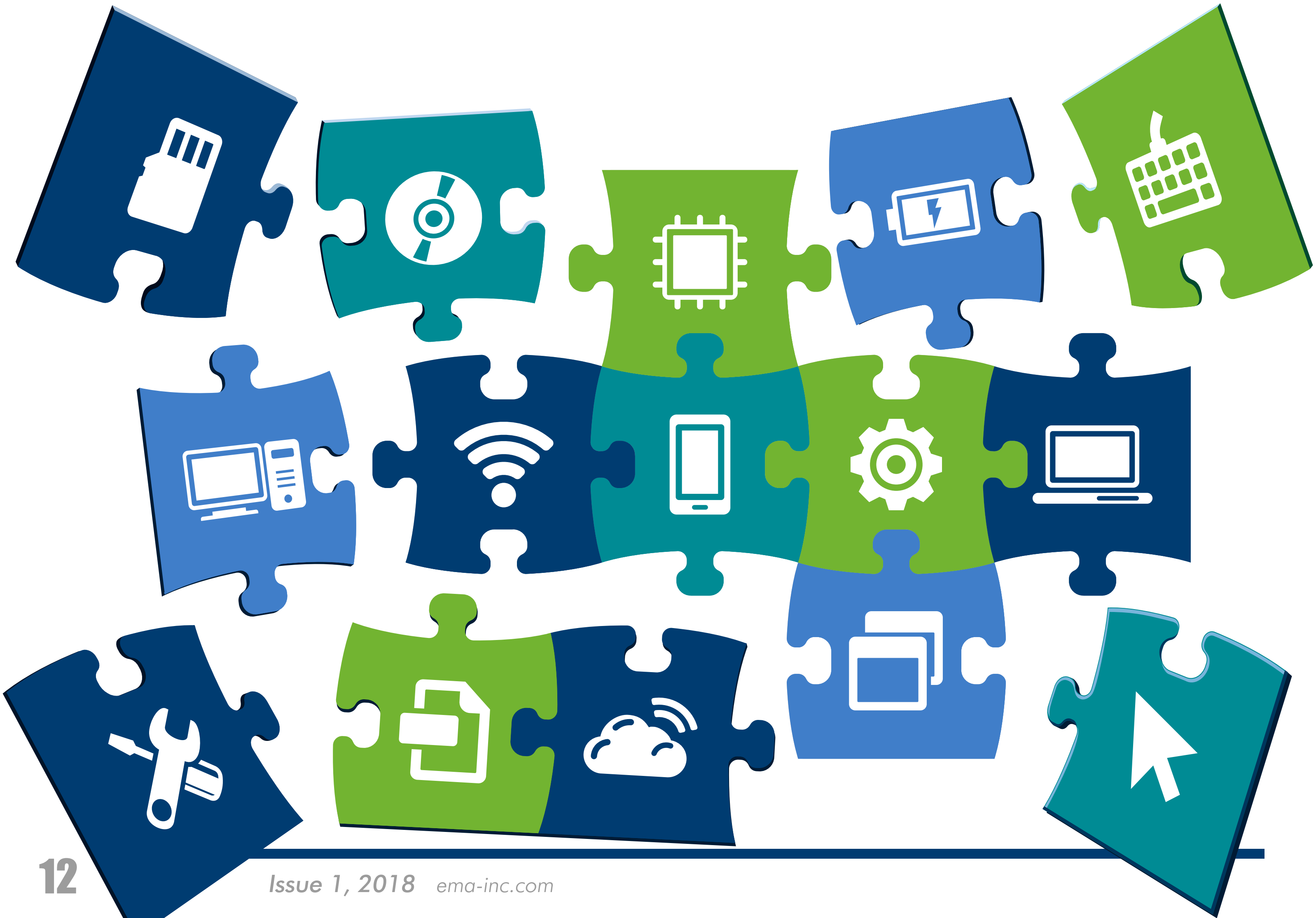
Functional

Utilities must consider their applications and functional requirements when evaluating their digital capabilities and communication infrastructure design needs. Will the functions require secure and real-time, low-latency-capable communications, like SCADA for control? Is this need networkwide, or only for certain applications and functions? Or do less secure and potentially latent systems (or those missing data reporting) for monitoring only or device reading/control functions (AMI, street lights, WQ sensors) meet the technical requirements? Before considering any individual projects and technology choices, utilities must thoroughly analyze application drivers and the technical characteristics necessary to meet requirements. Otherwise, they risk selecting a communication architecture that fails to meet long-term strategic and functional objectives.

Technological

The modern utility's critical communications infrastructure includes multiple platforms, applications, and technologies. These include SCADA networks, fire and security networks, metering networks, and mobile field-worker support in addition to general communications such as telephone, WiFi, internet, and intranet. Remote acoustic monitoring, pressure management, and other new applications will place increasing demands on these networks. Underlying communications infrastructure must have the capacity and flexibility to sustainably support these applications as diverse connectivity requirements place competing demands on water utilities' core communications architecture.

Utilities taking on technology transformations and upgrades must choose between numerous options, carefully evaluating the pros and cons. Potential synergy



and support from other departments further complicate network needs. City officials may find a bewildering assortment of technologies in use. For example, how many radio licenses are needed: SCADA, AMI, snowplows, buses, police, fire, and others?

Network Alternatives

AMR/AMI

AMR/AMI has been part of the utility landscape for several years. The leading solutions vendors have enhanced their two-way capabilities since their introduction and can now support very high (above 98.5 percent) read success rates (RSR) and OTA (over-the-air) remote firmware download capabilities for even large-scale systems (more than 100,000 meters).

AMI systems' technological maturity, security, scalability, and network capacity have changed rapidly to provide more flexibility and functionality. This flexibility allows water utilities to not only deploy AMI for smart meters, but also enables additional water system benefits and supportability for new "internet of things"/smart city applications that can improve the return on investment. These additional benefits such as pressure monitoring, system analytics, and distribution management come with ever present security concerns.

Most AMI vendor solutions are proprietary for virtually all enhanced applications. Water utilities may be able to select an AMI vendor and meter vendor independently and still be assured of basic meter reading functionality. However, if they wish to enable advanced functions, such as wireless leak detection, continuous flow, and pressure management via the AMI system, there are serious limitations. Utilities wanting to leverage these capabilities within the same communications infrastructure are usually limited to devices supplied by the AMI vendor. Acoustic leak detection capabilities are available for utilities that are not enabled via the AMI network. However, if a utility wishes to communicate to acoustic leak detection devices through the AMI networks, these devices are most likely proprietary to that AMI vendor.

Many of the internet of things/smart city applications are built on open standards such as LoRa or Wi-SUN (more on this further down in the article). To communicate with existing and emerging internet of things standards, many AMI vendors are developing gateway devices that can utilize the proprietary AMI network back to the head-end but can communicate with LoRa, Wi-SUN, or narrowband internet of things protocol devices in the field.

> Utilities' communications infrastructures face increased capability, performance, and functionality demands in this new digital environment. The underlying communications architecture is key to enabling this new digital water utility.

Cellular

Cellular is a ubiquitous and mature public communications infrastructure option. With the latest architecture offerings, leading providers such as Verizon and AT&T are pushing into internet of things/smart city applications with the deployment of the latest generation of cellular architecture. The historical issue with cellular solutions for utilities has been that the long-term operating cost per device per month was very high in comparison to AMI solutions. Emerging solutions that fall into the narrowband internet of things category such as CAT-M1 show some promise in reducing this cost, but many questions still exist. Long-term technology and pricing stability and guarantees for service levels are still issues for large utilities. Certain vendors are increasing proprietary protections on advanced smart metering solutions for cutting edge capabilities, limiting customer cellular solution choices.

Some AMI vendors do provide solutions that use cellular networks for meter connectivity to augment their proprietary networks in certain applications. The financial viability of some uses of cellular connectivity could increase as major solution providers reduce costs per device per month. As AMI meter vendors allow features such as leak detection on an open network, financial viability could improve further. The latest 4G and 5G capabilities and changing cellular device price curves leave open further questions regarding capability and compatibility between cellular infrastructure and meter vendors' proprietary architectures.

LoRaWAN solutions are typically laid out in a star topology, where Wi-SUN solutions are more applicable to mesh technologies.

Many open questions remain regarding technology maturity and scalability for these large and demanding infrastructure requirements. Can they support critical operations and service requirements for high-volume, sensitive applications across multiple organizations?

More information on LoRaWAN and Wi-SUN can be found at www.lora-alliance.org and www.wi-sun.org.

Internet of things solutions (LoRa/Wi-SUN/RPMA/NB-IoT)

Smart cities are using the internet of things to help manage everything from streetlights, traffic management, and parking, to environmental and air quality sensors and gunshot detection. Next-generation internet of things vendors support an increasing number of applications. These providers are positioning open networks based on standards such as LoRaWAN (Long Range Wide Area Network) and RPMA (Random Phase Multiple Access), both LPWAN (Low Power Wide Area Network) specifications, and Wi-SUN (Wireless Smart Ubiquitous Network). The viability of these solutions and standards is emerging and expanding for water utility applications such as monitoring of remote pump sites, irrigation management, consumption monitoring, and meter reading.

SCADA

Well-established and sophisticated SCADA networks support the control and monitoring of water utilities' critical infrastructure. To safeguard SCADA network integrity, the underlying physical layer for communications must be reliable, stable, and secure. Increasing demands for bandwidth and a transition to Ethernet impact communications network system design choices, such as the choice of medium – fiber, DSL, cellular, private wireless, etc. SCADA networks have been in place for a long time. Some applications rely on older systems and analog circuits that may not be supported in the near future. Utilities have several infrastructure options as they analyze and evaluate how to design necessary upgrades.

Cloud computing

More and more smart cities and smart water utilities are choosing to host applications in the cloud. With this trend toward distributed computing, utilities need to understand cost, performance, and other trade-offs of different hosting options, along with cybersecurity ramifications. It is imperative that disparate devices remain secure and access is limited to only service personnel with the appropriate credentials. Utilities must identify, evaluate, and determine the best hosting option for their cloud-based applications. What impacts do IaaS (Internet as a Service), PaaS (Platform as a Service), and Infrastructure SaaS (Software as a Service) have on cost and performance considerations? What are cybersecurity considerations? How can solution providers ensure that disparate devices remain secure and can be accessed only by appropriate utility/municipality personnel with responsibility for a specific class of equipment?

The new applications, technologies, developments, and standards enable transformation to a modern digital utility. They also raise many questions regarding the forward-thinking water utility's communications infrastructure strategy, implementation, and optimization. Utilities need solutions that offer high reliability, low power consumption, security, scalability, available spectrum, reasonable operating costs, and ease of deployment. Utilities must understand the costs, benefits, and ramifications of the host of options available.

The Five Deadly Sins of SCADA/PCS Cybersecurity

by Bob Reilly

This article is the third and final installment in our series on the Five Deadly Sins of SCADA and Process Control Systems Cybersecurity (Communicator 2016, Issue 1 and 2017, Issue 1). We've already addressed deadly sins two and three: allowing web browsing to the internet from SCADA/PCS and allowing direct access to the internet from SCADA/PCS. In this article we examine deadly sins one, four, and five, and recommend strategies and alternatives to mitigate their risks without impeding productivity. The remaining sins are:

Sin 1: Do you allow direct external access into your SCADA/PCS?

Direct access to your SCADA/PCS usually means there is no separation between your business network and your SCADA/PCS network. Although not uncommon in the water sector, this is a major security vulnerability. The risks associated with this kind of design are many of the things that you may hear about on the news such as ransomware, phishing, bitlockers, or, even worse, the ability of an attacker to control your network without your knowledge. This is because the business network and the SCADA/PCS reside on the same physical network with no separation. Any kind of successful attack on the business network can easily affect the SCADA/PCS network.

Figure 1 below represents a simple network where there is no separation between the two networks.

How do you know if you are safe from direct external access to your SCADA/PCS? If employees have unfettered access from your business network or remotely to the SCADA/PCS network, you are in violation of this rule and your network is at risk. A vulnerability scan of all your systems will tell you if this is a current problem on either network.

The first step in running a vulnerability scan is to talk with your information technology department, system integrator, or your technology contractor. Determine all the different access points into your SCADA network, including contractors, wired, wireless, and remote. Any

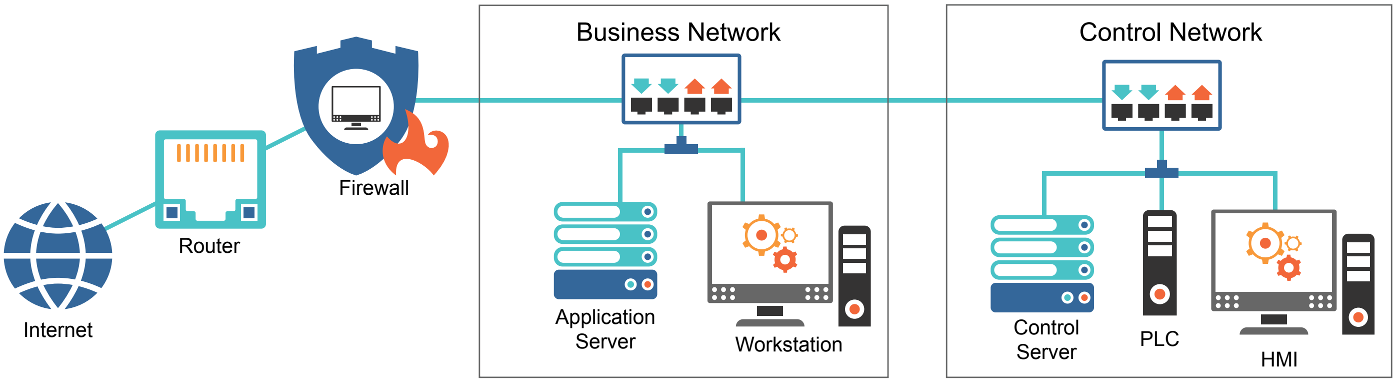


Figure 1: Direct external access

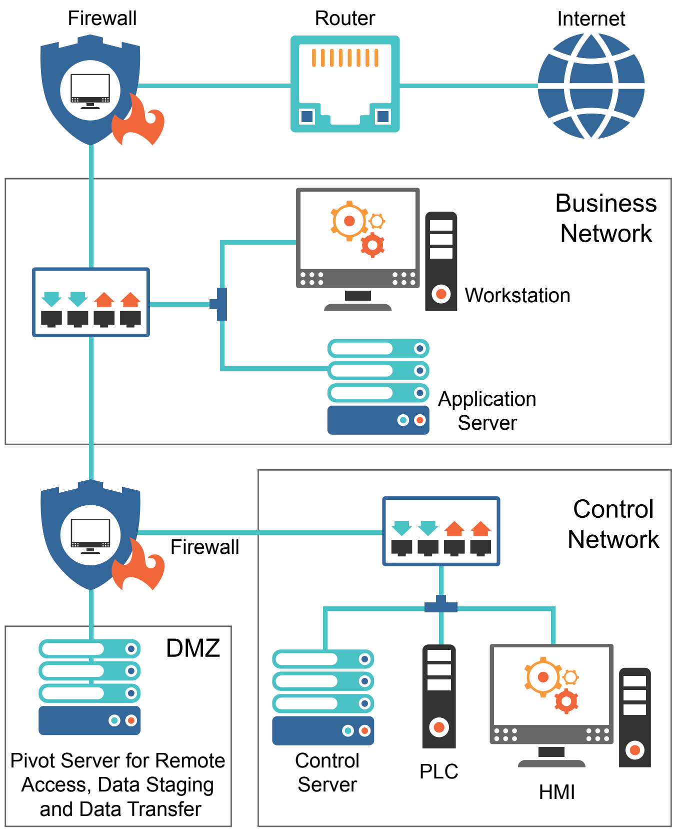


Figure 2: No direct external access

access point is a potential vulnerability and should be treated as path for potential attackers.

Ensure you have a **stateful packet inspection firewall** between your business and SCADA networks. Stateful packet inspection firewalls perform a deeper inspection of traffic as it passes through to ensure packets are compliant with policies and don't contain malware. If you already have one in place, make sure all access ports between the two networks are closed. You can check this via a penetration test against your firewall. This may require bringing in outside expertise. If your information technology department or contractors says you are secure, don't take them at their word; have them prove it to you. To do this, at a minimum you should run vulnerability scans and firewall penetration tests. Make sure proper precautions are in place on both the business network and the SCADA/PCS network. Creating a firewall between the two networks is a must. If this is something that a utility cannot do or is unwilling to do, then the two networks should be "air gapped," or physically separated.

Figure 2 shows what a secure, or potentially secure, network looks like. The firewall between the business network and the SCADA/PCS network blocks all traffic between them. Staging servers and pivot servers, located in the demilitarized zone (DMZ), control access to the SCADA/PCS network and its data. You should control any data access needs between the SCADA/PCS and the business network through a pivot server. A pivot server is a physical system located in the DMZ that acts as a secure traffic cop between the two networks. Any kind of remote access or data exchange should be limited to this location. A pivot server can be locked down to limit access to allow specific functionality only to users that have properly authenticated and have the appropriate rights. See Sin 4 for more information.

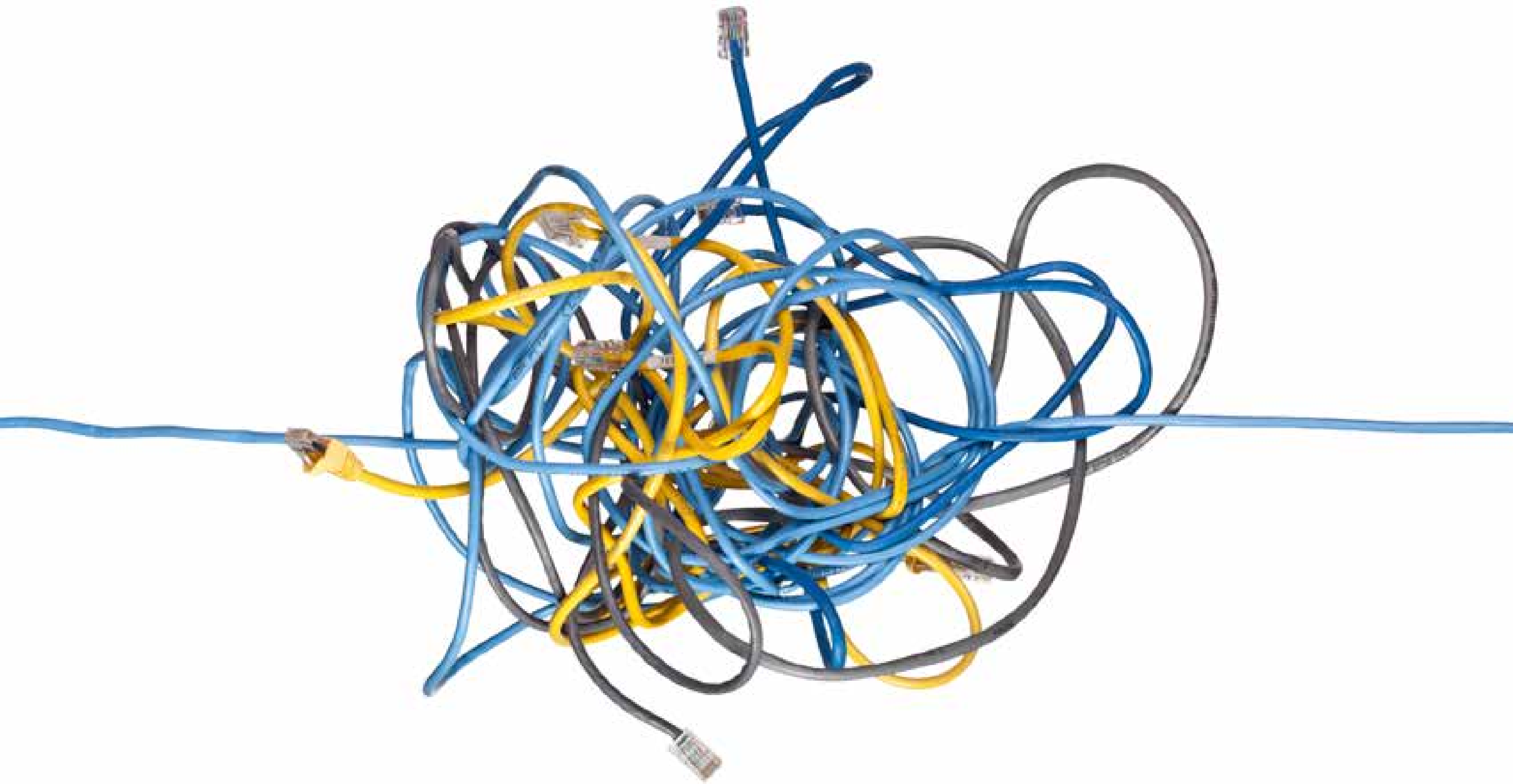
Sin 4: Do you allow SCADA/PCS laptops to be used outside of SCADA/PCS?

Many SCADA/PCS networks allow access by multiple portable devices, either for remote access or programming of programmable logic controllers (PLCs), remote terminal units (RTUs), or other equipment. These can be laptops, tablets, or even mobile smartphones. This sin manifests itself through usage of these devices outside of their intended purpose, whether on other networks or even for personal use. If you find you are using SCADA/PCS devices outside of the SCADA/PCS network, you are creating an unnecessary vulnerability.

Laptops or any mobile device set up to use on the SCADA/PCS network should be purpose-built for that task as well as **hardened** and physically controlled. Hardening is a process of securing devices to perform a certain task and locking them down from performing other tasks. Hardened devices will typically have unnecessary ports, such as FTP and HTTP, closed.

You should use multiple methods including MAC (media access control) filtering, two-factor authentication, and mobile device management to control access from remote devices to the SCADA/PCS network.

- Filtering by MAC address is not a foolproof access control method, but it can be used along with other methods to secure systems. MAC filtering is a security method to allow only specific device addresses access to the network.
- Two-factor authentication for remote access devices is an authentication method whereby users must utilize at least two of the following three methods for access:
    - Something you know – usually a password, PIN, or a passphrase



  - Something you have – usually a physical token or a text message
  - Something you are – usually a biometric such as a fingerprint
- Mobile device management (MDM) is a third-party application that is installed on mobile devices where granular policies can be set to update, monitor, and control the devices.

These are all strategies that can be incorporated into a security program to increase the overall security posture of the organization. Any one of these methods, used alone, will lower the risk of attack. Incorporating multiple methods will reduce your exposure even further.

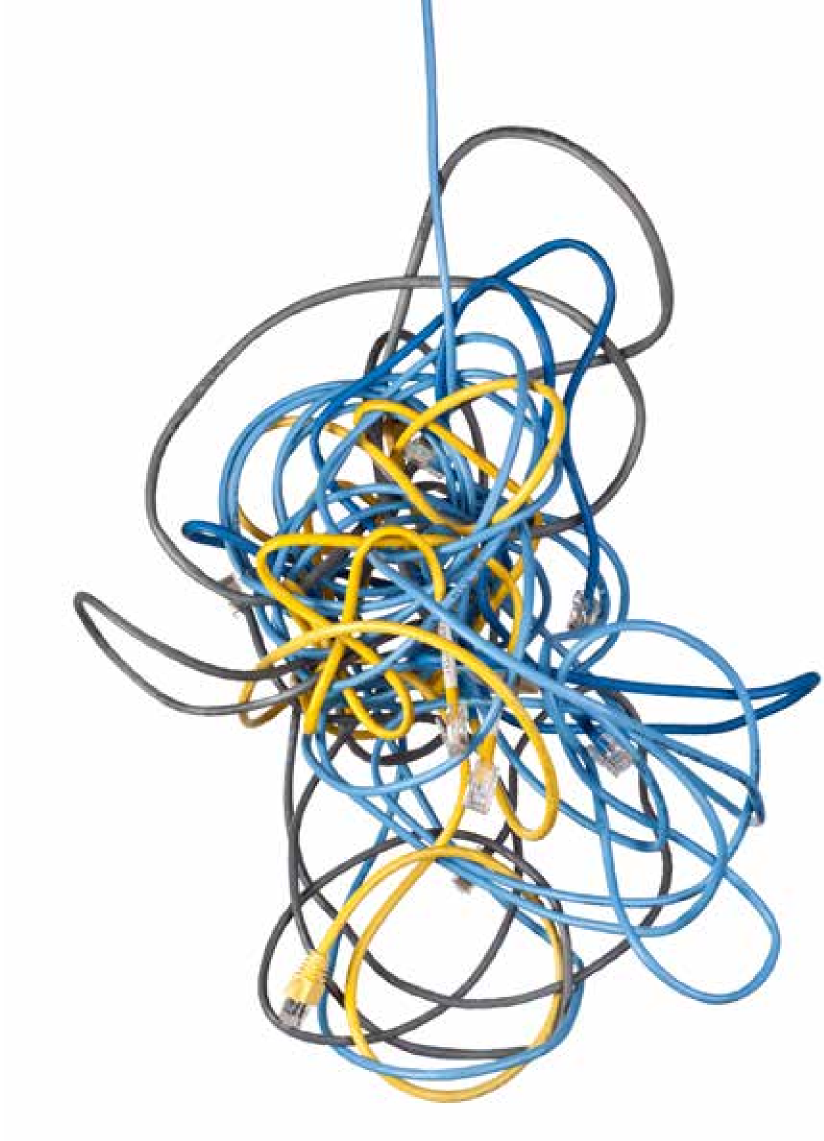
A pivot server, as shown in Figure 2, can be used for remote access from the business network or a remote location. Pivot servers should be set up to provide virtual desktop access to the SCADA/PCS network, meaning devices are never actually connected to the control network. There are many types of virtual connections that work well for this type of connection, including VMware Horizon, Microsoft Remote Desktop Services, and Citrix Xen. These systems can be controlled at many levels including at the user, application, and even at the port level.

Prior to allowing remote access, organizations should have a security program in place that includes proper log management and monitoring, intrusion prevention, and even ensuring that their policies are in place and up to date. The National Institute of Standards and Technology (NIST) recommends that critical infrastructure organizations have continuous monitoring of logs. A utility must also monitor intrusion prevention and detection at the SCADA/PCS gateway. Many utility organizations either incorporate on-site log monitoring systems that can parse log data known as a SIEM (Security Incident and Event Management), or utilize off-site log monitoring companies, known as a managed service security provider or MSSP.

Policies for the security around a SCADA/PCS are critical pieces of the overall puzzle. The latest AWWA Cyber Security Evaluation Tool lists 21 policies and plans that organizations should have in place to manage their security and their security program. Utilities cannot stop at creating this program; they must monitor and maintain it as well. In order to maintain a state of constant preparedness for the newest threats, utilities must have defined periodic reviews of this program.

Sin 5: Do you allow contractor or other outside laptops into SCADA/PCS?

If you are letting contractors bring in outside laptops or devices, or allowing them unmonitored remote access, you are guilty of Sin 5. Contractors will often bring in their own devices, connect to PLCs, and even move data between systems using a USB device.



Are you monitoring this access, either remotely or when they are on-site? Are you allowing devices not owned by the utility local access to your SCADA/PCS network?

The utility, not the contractor, should control contractor access, and all on-site and remote access should be monitored. Prior to any contractor connection to a utility SCADA/PCS network, the utility should have a defined change management plan. All production changes should be tested in a test environment and have a backout plan. A backout plan is a documented list of the steps needed to restore a system to its original state. This change management plan would be required as part of the vendor access policy. This policy will define these requirements and access will not be allowed without a signed agreement.

Utilities should control contractor remote access similarly to remote access for employees, except with even more restrictions. This access should be activated by the utility and staff should monitor the access to ensure that the contractor follows the approved change. Many of the remote access systems defined in Sin 4 allow monitoring and some have built in recording of sessions as well. This is a good idea in case any issues arise from a change.

Remote access by contractor devices should be controlled at the gateway or firewall through several methods. As discussed in Sin 4, all devices that access or can potentially access the SCADA/PCS network should first perform a two-factor authentication. Since the contractors' laptops are not owned or controlled by the utility, outside contractor devices should be placed in a quarantine where they can undergo a suitability screening. These screenings can be automated and controlled based on the potential vulnerabilities the device may introduce. The utility may choose to quarantine access to a limited access area based on the results or deny access altogether. These decisions should be documented in a policy and reviewed on a regular basis.

On-site access by contractors should be monitored as well. Staff knowledgeable of the SCADA/PCS network should escort and monitor contractors' access. If the changes are previously documented, tested, and approved by the utility, there should be little chance of a major disruption in operations.

Many contractors will use USB drives to move programs or data to and from systems. In order to avoid contractors' use of personal USB drives, the utility should have secure, encrypted USB drives that can be used when this is the only option available. Utility staff should manage and control the use of these USB devices to avoid unknowns being introduced onto the production network.

Don't stop what you're doing now, but make sure your cybersecurity improvements address these issues as priorities.

Utilities should work to create or improve their current security posture as well as their security program. A documented security program with hard deadlines for areas such as policy review, vulnerability scans, and even periodic cybersecurity assessments is a step in the right direction.

This program should incorporate all your policies and plans including incident management and disaster recovery. Not only should you have a set periodic review of all policies, but you should have a set schedule for auditing and testing of both your incident management and your disaster recovery plan. These tests should be performed, documented, and improved on a regular basis.

The bad practices mentioned in this article are not impossible to do securely, but a layered security model using the concept of defense in-depth is the best practice approach. Bring increased attention to cybersecurity. Allowing these practices presents very real and immediate threats to your system.

Recap and Next Steps

We've reviewed the five deadly sins of SCADA and Process Control Systems cybersecurity:

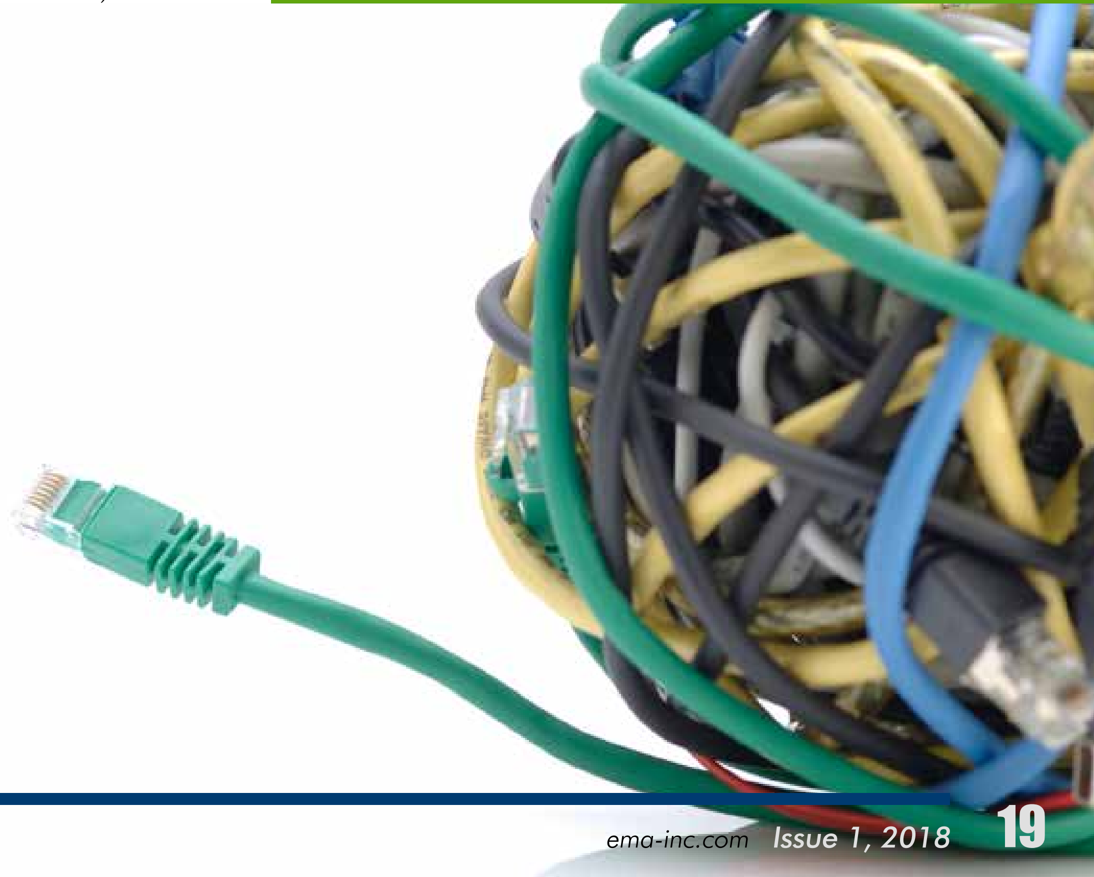
1. Allowing direct external access into your SCADA/PCS
2. Allowing web browsing to the internet from SCADA/PCS
3. Allowing direct access to the internet from SCADA/PCS
4. Allowing SCADA/PCS laptops to be used outside of SCADA/PCS
5. Allowing outside laptops into SCADA/PCS

Consider the five sins an opportunity for a defense in-depth approach. The more layers of defense, the better chance of having the proper countermeasure in place to thwart an attack. If you are just starting down this road, come up with a plan of measures that will need to be in place and begin a process of prioritization. The defenses that create the best bang for your buck should be implemented first. Policies and plans will help to guide some of these decisions based on the risk that an organization is willing to accept. A cybersecurity plan is really a roadmap to continually lower current risks while actively planning for future risks.

For more information, visit the NIST website to review special publication 800-82 Rev 2 and/or try using the AWWA Cybersecurity Guidance and tool to quickly assess your current security posture.

csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

www.awwa.org/resources-tools/water-and-wastewater-utility-management/cybersecurity-guidance.aspx



EMA, Inc.
2355 Highway 36 West, Suite 200
St. Paul, MN 55113-3819

**CHANGE
SERVICE
REQUESTED**

Join EMA at the Following Conferences

AWWA Annual Conference and Exhibition (ACE)

Las Vegas, NV • June 11 - 14, 2018

EMA PRESENTATIONS

- Communications and Cybersecurity for Intelligent Water Networks
  Bob Daly (EMA) and Mary Smith (Water Research Foundation)
- Utility Communications Technology Options – What are the important considerations for a smart water/ smart city infrastructure?
  Moderated by Ed Tirakian (EMA)
- When is AMI More Than Just New Technology?
  Terry Brueck and Mark Germscheid (EMA), Glen Gerads and Marie Asgian (Minneapolis Water Treatment & Distribution Services)

WEFTEC

New Orleans, LA • September 29 - October 3, 2018

EMA PRESENTATIONS

- Columbia, SC Operations: Empowered Employees and Increased Efficiency through Workforce Planning
  Jack Geisenhoff (EMA) and Joseph Jaco (Columbia Water)