THE FUTURE OF SMART CITIES: CYBER-PHYSICAL INFRASTRUCTURE RISK

August, 2015

NATIONAL PROTECTION AND PROGRAMS DIRECTORATE

OFFICE OF CYBER AND INFRASTRUCTURE ANALYSIS

This page intentionally left blank

EXECUTIVE SUMMARY

The Department of Homeland Security's Office of Cyber and Infrastructure Analysis (DHS/OCIA) produces Infrastructure Risk Assessments to provide an assessment of emerging risks to critical infrastructure.[1,2] This report addresses how the adoption of and increased reliance on smart technologies may create or increase risks for Smart Cities. This report focuses on the Transportation Systems Sector, the Electricity Subsector within the Energy Sector, and the Water and Wastewater Systems Sector.

As technology pervades into our everyday lives, once simple devices have become smarter and more interconnected to the world around us. This technology is transforming our cities into what are now referred to as "Smart-Cities". Smart Cities have been defined as urban centers that integrate cyber-physical technologies and infrastructure to create environmental and economic efficiency while improving the overall quality of life.[3] The goal of these new cities is to create a higher quality of life, a more mobile life and an overall increased efficient use of available resources. Some examples of Smart-City technologies are interconnected power grids reducing power waste, smarter transportation resulting in increased traffic management, and smarter infrastructures that reduce hazards and increase efficiency.

This interconnectedness of devices introduces cyber-physical technologies that connect cyber systems to physical systems, thereby removing the barrier between the cyber and physical worlds. Some cyber-physical systems are integrated at the design stage unlike more traditional legacy systems; a full-fledged cyber-physical system is typically designed as a network of interacting elements with physical input and output instead of as standalone devices. Smart City, in everyday use, is inclusive of terms such as 'digital city' or 'connected cities'. Cyber-physical innovations feature prominently in Smart Cities, particularly as cyber-physical technologies are increasingly added to existing infrastructure and built into newly constructed infrastructure. Removing the cyber-physical barriers in an urban environment presents a host of opportunities for increased efficiencies and greater convenience, but the greater connectivity also expands the potential attack surface for malicious actors. In addition to physical incidents creating physical consequences, exploited cyber vulnerabilities can result in physical consequences, as well.

The vulnerabilities and attack classes (such as distributed denial of service, malware, and phishing attacks) to most logical technologies such as computers and servers have been researched over the decades and years and are well understood by security researchers. Although the specifics of the attacks and potential consequences can vary with each type of attack the basic structures and general mitigations for these attacks are known. The same can be said of the vulnerabilities and mitigation factors for physical infrastructure. However, with the introduction of Smart Cities and cyber-physical innovations the vulnerabilities, resulting mitigating factors, and potential consequences for these new technologies are still unclear. As these new cyber-physical devices are introduced to the World the vulnerabilities, risks, threats, and consequences will be better understood. This report summarizes the insights from a technology-informed futures analysis—including a critical look at potential future vulnerabilities as a result of these cyber-physical infrastructure systems become pervasive in Smart Cities. The goal is to help Federal, State and local analysts and planners incorporate anticipatory thinking into Smart City design and continued critical infrastructure protection efforts relating to this new technology. The analysis focuses on specific cyber-physical technologies that represent key aspects of the future of Smart City infrastructure (Table 1).

[1] Risk is defined as the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. It is often thought of as a function of threat, vulnerability, and consequence, where threat and vulnerability are components of likelihood (U.S. Department of Homeland Security Risk Steering Committee, DHS Risk Lexicon, Washington, D.C.: U.S. Department of Homeland Security, 2010).
[2] Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. (DHS, "What Is Critical Infrastructure?" http://www.dhs.gov/what-critical-infrastructure, accessed, August 18, 2014).
[3] In addition, a smart city "gathers data from smart devices and sensors embedded in its roadways, power grids, buildings, and other assets. It shares that data via a smart communications system that is typically a combination of wired and wireless. It then uses smart software to create valuable information and digitally enhanced services." (Smart Cities Council, "Vision," http://smartcitiescouncil.com/category-vision, accessed February 4, 2015).

TABLE 1— KEY SMART TECHNOLOGIES

Sector	Cyber-Physical Technologies Examined
Transportation Systems Sector	Autonomous Vehicles Positive Train Control Intelligent Transportation Systems Vehicle-to-Vehicle and Vehicle-to-Infrastructure
Electricity Subsector	Smart Power-Generation Plants Smart Distribution and Transmission Advanced Metering Infrastructure
Water and Wastewater Systems Sector	Smart Water Treatment Smart Water Distribution Smart Water Storage

ANALYSIS

The efficiencies and security challenges that come with Smart City transformation will vary by geographic location, infrastructure sector, and the information technology (IT) systems of each city, requiring cities to take a close look at their unique characteristics as they upgrade their systems. At a high level, three themes cut across the security considerations that come with integrating cyber-physical systems into city infrastructure: changing seams, inconsistent adoption, and increased automation. These themes emerged from the assessment of dynamics shaping future cyber-physical infrastructure—detailed in this report—and the themes provide a framework for considering the implications of future challenges that today's planners will face.

Changing Seams – Seams—such as those that exist between rural and urban, legacy and new infrastructure components, or business networks and control system networks—are moving or disappearing as systems are upgraded and networked. The physical and virtual seams between infrastructure components, and sectors, are becoming increasingly permeable as cyber and physical systems become networked and remotely accessible. Increased connectivity, faster speeds, and multi-directional data flows diversify access points into critical infrastructure, changing and stretching the borders that Smart Cities must secure.

Inconsistent Adoption – Critical infrastructure will evolve at different rates because of factors such as resource availability, user preferences (e.g., consumer purchases of autonomous vehicles, utility operators' use of "smart" technologies), or scale and accessibility (e.g., the size of water-distribution networks being upgraded). The inevitable inconsistency of cities' technology migration will introduce security challenges to government, industry stakeholders, and the people living with these technologies. For example, as areas merge older and newer infrastructure, local "blind-spots" may exist in areas where older equipment remains dominant but lacks the same ability as newer equipment to report operational status, problems, or efficiency opportunities. Such inconsistent adaptation poses challenges to developing consistent security policies for cities at different stages of—or with different approaches to—Smart City development.[4]

[4] At the same time, standardization—as opposed to diversity—can also lead to a level of uniformity that creates additional challenges. Any standards-based approach should ensure that adherence to standards—e.g., taking the approach that checking the boxes is all that is necessary—does not replace sound engineering judgment.

Increased Automation – Cyber-physical infrastructure can migrate control from people to algorithm-based systems, introducing a level of security and resilience into a system by mitigating any potential human errors. However, in addition to mitigating some risks, removing human interaction with the system, potentially introduces some new security challenges, including, but not limited to, issues associated with:

- Increasing the number of system access points and, therefore, potential attack vectors;
- Skill atrophy;
- Loss of visibility into all parts of a system;
- Cascading failures; necessary changes in emergency response plans (e.g., humans will not be present in areas of the system they once were);
- Unanticipated permutations of automated functioning; or
- Unintentional elimination of manual overrides.

OPPORTUNITIES FOR DHS

State and local governments, in partnership with industry, will largely drive the evolution of cyber-physical infrastructure in Smart Cities. DHS can contribute to this stakeholder community to help it anticipate and plan for potential risk, and to influence the overall security environment in which these technologies will exist. DHS can assist in the development of standards and regulations, helping to ensure consistency across sectors and geographic areas. Strategic communication and engagement may influence a more secure evolution of cyber-physical infrastructure as Smart Cities adopt technologies at varying rates. DHS can also facilitate or direct Federal assistance to State and local governments.

Table of Contents

Table of Tables

SCOPE

This report addresses the question: How might vulnerabilities in Smart City cyber-physical infrastructure be exploited to create significant damage to the economy, public health and safety, or national security? The three sectors explored in this report are the Transportation Systems Sector, the Electricity Subsector within the Energy Sector, and the Water and Wastewater Systems Sector.

The analysis in this report is based on specific cyber-physical technologies relating to the Transportation Systems, Energy, and Water and Wastewater sectors. OCIA has collaborated with industry experts to select these technologies, from a wide range of current and emerging technologies based on the following criteria:

- Likelihood of adoption by cities within the next 5 – 10 years.
- The potential to have transformational impact on the growth and trajectory of Smart Cities.
- The potential direct impact on public safety and national security.

The technologies are not intended to be an exhaustive list; instead, they represent cyber-physical trends that characterize key aspects of the future of Smart Cities.

This report identifies future pathways for potential disruptions and makes technology-specific observations for each sector analyzed for this study. Furthermore, this report discusses the nature of future vulnerabilities and to better understand how they might be exploited in ways that lead to physical consequences. The pathways are not identified as a likely future or suggest where the risks may be highest.

The technology-specific observations synthesize findings across the pathways to highlight potential vulnerabilities that, if unaddressed, may increase the risk profile of a technology or infrastructure sector in a Smart City. These observations are categorized into the three high-level themes—changing seams, inconsistent adaptation, and increased automation—that transcend the security challenges associated with the evolution of cyber-physical systems in Smart Cities.

The report concludes with Opportunities for DHS, which detail areas where DHS can assist its partners to anticipate and mitigate risk, and influence the overall security environment in which these technologies will exist. These opportunities fall into three categories of "levers" available to DHS: standards and regulations, communication and engagement, and Federal assistance.

INTRODUCTION

Many U.S. cities are experiencing substantial population growth, and State and local governments are struggling to keep up with congestion, pollution, and the increased demands being placed on aging and failing infrastructure. Municipal governments are increasingly looking to address these concerns by networking various infrastructure smart technologies of the city, which can support increased automation and responsiveness. In doing so, cities will become "Smart Cities"—urban centers that integrate cyber-physical technologies and infrastructure to create environmental and economic efficiency while improving the overall quality of life.[5] This transformation will significantly affect a city's critical infrastructure, which is increasingly composed of cyber-physical systems.

Traditionally, infrastructure in cities involved a series of standalone components; cyber-physical systems involve a series of electronically networked physical elements, including embedded sensors, computation devices, communication technology, and actuators. Cyber-physical systems can capture a vast amount of data produced in a city to identify and implement new efficiencies. In addition to collecting data and suggesting more efficient processes, these systems can also automatically control and manipulate physical infrastructure to implement changes. By developing a "system of systems," a Smart City can integrate short- and long-term efficiencies.

Although Smart Cities and the implementation of cyber-physical systems into critical infrastructure networks bring a host of much-needed benefits, they also introduce a new set of risks to public safety and, potentially, national security. Historically, cyber and physical systems have operated fairly independently of one another. The impact of a cyber-system disruption was contained within the cyber domain, and a physical disruption was contained in the physical domain. Cyber-physical infrastructure directly links or, at the design level, integrates both domains. In addition to physical incidents creating physical consequences, exploited cyber vulnerabilities can result in physical consequences. In general, the vulnerabilities for cyber and physical infrastructures—as separate systems—are well known by system administrators. The existence of vulnerabilities does not guarantee adverse impacts on a system or component. Since the concept of cyber-physical infrastructure is new, the impact of the exploitation of a vulnerability may be understood but the risk and consequence to the infrastructure and its connected components is not fully understood as system administrators have not had substantial time to evaluate and improve security based on actual events.

Increasing the challenge for security research is the rapid evolution of key technologies underpinning Smart Cities and the wide variability in the pace and scale of technology adoption and implementation by Federal, State, and local municipalities. The confluence of rapid technology evolution and the unknown trajectory of its adoption create even greater future uncertainty for those responsible for security and risk management at all levels of government and the private sector.

To address that uncertainty, this report takes a technology-informed approach to futures analysis that draws on an assessment of "knowns and unknowns," and a diverse research base to generate multiple hypotheses for how technological innovations could affect critical infrastructure protection. Based on 30 subject matter expert interviews (see Appendix A for a list of experts) and expansive open-source research, pathways emerged that are both specific and broad enough to elicit crosscutting insights about the nature of cyber-physical vulnerabilities.

Although the technology-specific observations in this report do not delve into extensive discussion of standards, regulations, or practices in development or in use today (i.e., voluntary cybersecurity guidance documents), readers can measure their own security posture in light of these future considerations and available guidance identified by the Electricity Journal and the National Institute of Standards and Technology.[6] In combination with such guidance, the insights in this report provide Federal, State, and local analysts and planners with the resources they need to incorporate anticipatory thinking into Smart City design and continued critical infrastructure

[5] For examples of such cybersecurity guidance, see (1) Hawk, Carol and Akhlesh Kaushiva, "Cybersecurity and the Smarter Grid," The Electricity Journal, October 2014, Vol. 27, Issue 8, p. 84–95 and (2) National Institute of Standards and Technology, The Smart Grid Interoperability Panel Cyber Security Working Group, "Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security," September 2010, http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf, accessed February 4, 2015.

[6] For examples of such cybersecurity guidance, see (1) Hawk, Carol and Akhlesh Kaushiva, "Cybersecurity and the Smarter Grid," The Electricity Journal, October 2014, Vol. 27, Issue 8, p. 84–95 and (2) National Institute of Standards and Technology, The Smart Grid Interoperability Panel Cyber Security Working Group, "Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security," September 2010, http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf, accessed February 4, 2015.

protection efforts. Critically assessing potential future vulnerabilities and associated attack vectors as these infrastructure systems are being developed and implemented will help those responsible for Smart City security stay ahead of, and potentially mitigate, the particularly complex risks associated with the rapid evolution of cyber-physical infrastructure.

FUTURE PATHWAYS

The following four pathways explore plausible answers to the following question: How might vulnerabilities in Smart City cyber-physical transportation infrastructure be exploited to create significant damage to the economy, public health and safety, or national security? Each pathway includes:

- Examples of specific attack or accident vectors
- A discussion of the technology vulnerabilities that could be exploited
- Disruptions and consequences that would warrant regional- or national-level attention

TECHNOLOGY-SPECIFIC OBSERVATIONS

The associated potential vulnerabilities to future Smart City infrastructure technologies will be highlighted in the following sections. In some cases, these vulnerabilities are inherent to the technology itself, and they will change as a technology proliferates in a city. At a high level, these vulnerabilities are associated with three themes that cut across the security considerations that come with integrating cyber-physical systems into Smart City infrastructure.

Changing Seams – Seams—such as those that exist between rural and urban, legacy and new infrastructure components, or business networks and control system networks—are moving or disappearing as systems are upgraded and networked. The physical and virtual seams between infrastructure components, and sectors, are becoming increasingly permeable as cyber and physical systems become networked and remotely accessible. Increased connectivity, faster speeds, and multi-directional data flows diversify access points into critical infrastructure, changing and stretching the borders that Smart Cities must secure.

Inconsistent Adoption – Critical infrastructure will evolve at different rates because of factors such as resource availability, user preferences (e.g., consumer purchases of autonomous vehicles, utility operators' use of "smart" technologies), or scale and accessibility (e.g., the size of water-distribution networks being upgraded). The inevitable inconsistency of cities' technology migration will introduce security challenges to Government, industry stakeholders, and the people living with these technologies. For example, as areas merge older and newer infrastructure, local "blind-spots" may exist in areas where older equipment remains dominant but lacks the same ability as newer equipment to report operational status, problems, or efficiency opportunities. More broadly, such inconsistent adaptation poses challenges to developing consistent security policies for cities at different stages of—or with different approaches to—Smart City development.[7]

Increased Automation – Cyber-physical infrastructure can migrate control from people to algorithm-based systems. The process of removing or limiting human interaction with the system or increased automation, introduces new potential security challenges, including, but not limited to, issues associated with:

- Increasing the number of system access points and, therefore, potential attack vectors;
- Skill atrophy;
- Loss of visibility into all parts of a system;
- Cascading failures;
- Necessary changes in emergency response plans (e.g., humans will not be present in areas of the system they once were);

[7] At the same time, standardization—as opposed to diversity—can also lead to a level of uniformity that creates additional challenges. Any standards-based approach should ensure that adherence to standards—e.g., taking the approach that checking the boxes is all that is necessary—does not replace sound engineering judgment.

- Unanticipated permutations of automated functioning; or
- Unintentional elimination of manual overrides.

The sections below detail observations regarding these technology-specific vulnerabilities and how they can evolve along with Smart City transportation systems.

TRANSPORTATION IN SMART CITIES

This section focuses on the future dynamics of cyber-physical infrastructure in Smart Cities within the Transportation Systems Sector, providing Sector-level inquiries emphasizing security and resilience. In addition to the general security risks inherent in transportation networks, Smart City transportation systems bring a unique set of security challenges, including the:

- Sheer scale and complexity of transportation networks in major cities, including the difficulty of securing mobile device connectivity to transportation networks and distinguishing legitimate mobile device queries from anomalies.
- Large number of system access points stemming from the presence of networked technology across large systems, raising the cost and difficulty of properly securing each system device. This number includes hardwired access points—many of which may be located in remote areas—and wireless access points.
- Burden of ensuring smooth interface, communication, and security among multiple interdependent systems, including sensors, computers, fare collection systems, financial systems, emergency systems, ventilation systems, automated devices, power relays, etc.
- Demand for nonstop access to real-time data that Smart City transportation systems require, and the related costs associated with maintenance and service downtime.
- Logistical and security hurdles of physically accommodating enormous volumes of passengers and freight, along with the reality that security breaches could result in public safety risks.

Five cyber-physical technologies that will be part of future Smart City transportation systems are autonomous vehicles, positive train control (PTC), intelligent transportation systems (ITS), and vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) technologies.

AUTONOMOUS VEHICLES

Autonomous vehicle technology enables automobiles to understand the environments in which they operate and execute safe and efficient commands based on this understanding. Autonomous vehicles can assume decision-making and operational tasks, enabling drivers to become passengers, entirely disengaged from the demands of driving. Autonomous vehicles can steer, select optimal speeds, avoid obstacles, choose efficient routes, park themselves, and warn passengers of imminent danger. The majority of autonomous vehicles in development use a deliberative architecture, meaning they are capable of making decisions entirely based on onboard technology—though many are capable of also incorporating external inputs when beneficial. To gather the data necessary for operation, autonomous vehicles use a variety of sensors. Light detection and ranging (LIDAR) technology uses light pulses to identify lane and road markings and boundaries. Global positioning system (GPS) devices gather specific geographic data to inform route selection and other location-based decision-making, often in combination with onboard tachometers, altimeters, and gyroscopes. Video cameras track other vehicles and pedestrians while capturing information on traffic lights and road signs. Radar sensors similarly track other vehicles. Ultrasonic sensors support parking by capturing data on objects in close proximity to autonomous vehicles, including curbs and other cars. A central onboard computer processes inputs from these sensors and issues commands to a car's steering, acceleration, braking, and signaling systems.

Some automobile manufacturers, urban planners, and policy makers envision a future in which vehicles take complete control of the driving process, and such implementation of autonomous vehicles will likely happen incrementally, with an increasing number of tasks being automated over time.[8]

[8] Monitor 360 Interview with a Smart City Expert, June 25, 2014; Monitor 360 Interview with an Autonomous Vehicle Expert, August 7, 2014.

PATHWAY 1: AUTONOMOUS VEHICLE SYSTEM MALFUNCTION

Sample Vector 1: A malicious actor hijacks one or more autonomous vehicles.

Autonomous vehicles are vulnerable to remotely executed attacks because of the amount of control a central computing system holds over various physical components and their ability to communicate with nearby vehicles and infrastructure. By gaining remote access to an autonomous vehicle's central computer, a malicious actor could control the braking, steering, and acceleration of a car, or prompt onboard sensors to react to non-existent events. To maximize danger to passengers, the malicious actor could also surreptitiously insert software into a vehicle's central computer so that it is programmed to take dangerous actions when a certain condition is met—e.g., when a car is traveling above 70 miles per-hour. Alternatively, a malicious actor could use malware to gain control of multiple vehicles simultaneously without their owners' knowledge. With a critical mass of infected vehicles, that actor could execute preprogrammed commands to tamper with sensors or execute specific dangerous commands.[10]

In 2014, two security experts demonstrated the ability to remotely access and control vehicle functions, including braking, steering, and engine power. Although this attack exploited a Bluetooth vulnerability, the experts also highlighted the possibility of using cellular connections and in-car applications as additional attack vectors.[9]

- Unlike personal computers or mobile phones, which have become common to patch through a simple download, installing system updates or security patches for a car may be expensive and complicated at the early stages of this technology's development.[11] Some vehicles are currently able to receive updates that are pushed out remotely and known as "push updates," but this capability is not widespread. Other options currently available to car manufacturers are: to direct drivers to schedule a service appointment at a dealership, or send a piece of hardware—a flash drive for example—and allow drivers to install updates themselves.[12] Both options will be costly for car manufacturers and will rely on customer initiative. Failure to follow update instructions could leave many vulnerable cars on the road.[13] Although car manufacturers may extensively use Bluetooth or other wireless connections to automate updates in the future, autonomous vehicles without the ability to receive "push" updates will remain vulnerable to missed or delayed software updates during initial rollout.[14]
- Full autonomy requires networking automobile elements originally designed to be standalone features, increasing the complexity of in-car networks and the number of potential weak points in the system. For example, a newly networked tire pressure-monitoring sensor or entertainment system could provide a low-security vector to access central computer systems.[15]
- Autonomous vehicles will likely incorporate Web-access technology designed to allow passengers to access the Internet while travelling, greatly increasing a vehicle's attack surface.[16] The growing presence of cellular and Bluetooth technology in modern cars also increases the risk of remote attacks on autonomous vehicles. These vulnerabilities could allow malicious actors to access the vital computing functions of an autonomous vehicle.[17] Although car manufacturers will potentially adapt their security systems as onboard computers become increasingly pervasive and powerful, weak spots and security vulnerabilities will likely persist that will have to continuously updated and patched to address these vulnerabilities. Like desktop computer systems, it is near impossible to anticipate all potential attacks or

[9] Anderson, James et al, "Autonomous Vehicle Technology: A Guide for Policymakers," Rand Corporation, http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR443-1/RAND_RR443-1.pdf, accessed December 6, 2014.
[10] Miller, Charlie and Christopher Valasek, "A Survey of Remote Automotive Attack Surfaces. Presentation at Blackhat Conference, August 6, 2014.
[11] Anderson, James et al, "Autonomous Vehicle Technology: A Guide for Policymakers," Rand Corporation, http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR443-1/RAND_RR443-1.pdf, accessed December 6, 2014.
[12] bid.
[13] Monitor 360 Interview with a Vehicle Hacker, July 30, 2014; Michael Mimoso, "Car Hacking Enters Remote Exploitation Phase." http://threatpost.com/car-hacking-enters-remote-exploitation-phase/107626, accessed November 19, 2014.
[14] Monitor 360 Interview with a Vehicle Communications Expert, July 31, 2014.
[15] Rouf, Ishtiaq et al, "Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study." http://www.cse.sc.edu/~wyxu/papers/TPMS2010.pdf, accessed November 11, 2014.
[16] Mimoso, Michael, "Car Hacking Enters Remote Exploitation Phase." http://threatpost.com/car-hacking-enters-remote-exploitation-phase/107626, accessed November 19, 2014.
[17] Monitor 360 Interview with a Cyber-Physical Security Expert, July 24, 2014.

to test autonomous vehicle computers for all possible bugs.[18] As a result, autonomous vehicles are likely to experience the same challenges as traditional computer systems.

Isolated or infrequent attacks would not necessarily affect transportation safety as a whole, but a sophisticated and focused attack could warrant regional- or national-level attention. Malicious actors able to control one or more autonomous vehicles could cause considerable danger and physical damage by engineering collisions with other vehicles or cause a vehicle to crash. By focusing these attacks on fast-moving vehicles, vehicles carrying hazardous materials, or crashing vehicles into city infrastructure such as bridges and tunnels, the potential loss of life could be significant. Likewise, using widely disseminated malware—spread through attacks on a large number of individual cars over time or through a vulnerability intentionally inserted in a software update—could expand the potential for loss of life. Multiple actors working together could also target a larger group of vehicles to greater effect. Not all damage caused by these attacks is necessarily physical; even a small-scale disruption might undermine consumer confidence, cause panic, or, depending on government response, lower public trust.[19]

Sample Vector 2: A malicious actor disrupts an autonomous vehicle's sensor devices.

Autonomous vehicles depend on a series of external inputs—such as stop lights, road signs, and awareness of other vehicles—making an attack on their sensor systems a relatively easy and inexpensive way to affect a large number of these vehicles. Although it would be difficult to orchestrate numerous autonomous vehicles to attack one specific target this type of attack (e.g., a collision targeting a specific building), it could be successful in causing mass confusion resulting in creating dangerous driving conditions with potential for loss of life.[21] Disrupting sensors for this type of attack could be accomplished by placing a signal-jamming device in a high-traffic area—e.g., on a freeway light post—or by affixing it to a conventional car, drone, or other vehicle. A trend towards "sensor fusion"—using multiple types of sensors—mitigates some risk by creating redundancies.

In 2013, a truck driver with a $100 GPS jammer attached to his truck accidentally jammed a satellite network at Newark Airport as he drove by the airport's perimeter. In this instance, the disruption was accidental.[20]

- Standard methods of cybersecurity protection, such as complex cryptography and sophisticated security standards, would do little to prevent an attack on an autonomous vehicle's sensors.[22] The risk of such an attack comes from the susceptibility of onboard sensors to external inputs, not from flaws in onboard cybersecurity. GPS devices are one example of autonomous vehicle sensors vulnerable to signal jamming, as they are largely unable to distinguish normal inputs from potentially disruptive inputs (such as those coming from a jamming device).[23]
- Though illegal, GPS jammers are readily available online and can also be custom built using online instructions and a basic understanding of electrical engineering.[24] LIDAR sensors are also vulnerable to outside interference. Although signal-blocking devices for autonomous vehicles would most likely need to be custom built for this purpose, the associate attack strategy is fairly straightforward—requiring only that a signal jammer be in the vicinity of a target device.
- Unlike GPS and other radio wave jamming devices, there are no Federal laws prohibiting LIDAR or other laser-based jamming devices, and only a few States have outlawed them.[25] In addition, almost anyone who can afford the relatively inexpensive disruption devices—costing as little as $150—could execute this type of attack, as little specialized knowledge is necessary to disrupt autonomous vehicles in this way.[26]

---

[18] Ullman, Ellen, "Errant Code? It's not just a Bug," The New York Times, August 8, 2012; Townsend, Anthony, "Smart Cities: Big Data, Civic Hackers, and the Quest for a new Utopia." New York: W.W Norton & Company, 2013.
[19] Monitor 360 Interview with an Urban Futurist June 28, 2014; Monitor 360 Interview with a Smart City Expert, June 25, 2014.
[20] Gibbons, Glenn, "FCC Fines Operator of GPS Jammer That Affected Newark Airport GBAS," http://www.insidegnss.com/node/3676, accessed November 19, 2014.
[21] Monitor 360 Interview with an Autonomous Vehicle Expert, August 7, 2014.
[22] Monitor 360 Interview with a Vehicle Communications Expert, July 31, 2014.
[23] Although not discussed extensively here, sensor spoofing is an additional consideration beyond jamming. The wrong information that stems from spoofing can lead to separate consequences than the lack of information related to jamming.
[24] Monitor 360 Interview with an Autonomous Vehicle Expert, August 7, 2014; Monitor 360 Interview with a Transportation Scholar, August 7, 2014.
[25] Federal Communications Commission, "GPS, Wi-Fi, and Cell Phone Jammers," http://transition.fcc.gov/eb/jammerenforcement/jamfaq.pdf, accessed December 6 2014; "Florida Needs to Ban Radar Detectors," Orland Sentinel, January 27, 2011.
[26] Law Enforcement Services, LLC, "Understanding Police Traffic RADAR & LIDAR," http://www.lawenforcementservices.biz/Law_Enforcement_Services,_LLC/RADAR_-_LIDAR_TRAINING_files/Radar%20-%20Lidar%20Jammers.pdf, accessed July 10, 2015.

Employed at scale or in strategically significant locations, signal disruption for autonomous vehicles could pose a potential threat to public safety. Although autonomous vehicles will enter a safety-mode upon recognizing errors—coming to a safe stop or returning vehicle control to a human driver—such incidents would still lead to congestion and unsafe conditions. The more sensor devices that have been compromised, the more haphazard these actions will become, potentially leading to traffic inefficiency, car accidents, or panic.[28] Although such incidents are unlikely to cause widespread loss of life, signal disruption attacks could undermine confidence in cyber-physical technology and create logistical challenges for transportation and city administrators. The severity of the consequences would increase if the attack were orchestrated to be widespread and in high-speed areas, or if the attack were targeted around tunnels or major transportation hubs.

Attacks, system errors, and product recalls affect public confidence. Negative impressions of Toyota rose from 17 to 41 percent following a 2009 recall.[27]

AUTONOMOUS VEHICLE TECHNOLOGY-SPECIFIC OBSERVATIONS

Changing Seams

- Unlike computers and mobile phones, autonomous vehicles may be difficult to supply with software updates and security patches for technical and logistical reasons (i.e., the technology is complex and the connectivity needed to support updates may be inconsistent; some updates may require consumers to bring vehicles to a physical location). These challenges will compound as the volume of autonomous vehicles increases.
- Ensuring security for the number of car technologies that are designed for discrete purposes—from tire pressure gauges to navigation to heating and cooling—is considerably more difficult than for technologies that were designed to operate as a single integrated system.

Inconsistent Adoption

- Variety in the types of autonomous vehicles being built—including potential technology variations that competitors deploy to distinguish themselves—has the potential to increase vulnerabilities associated with vehicle interoperability.
- As autonomous vehicle use increases in cities, it will be difficult to identify autonomous vehicles that have been compromised—and are under the control of—by malicious actors.
- Global diversity among autonomous vehicle manufacturers will increase the potential for inconsistent cybersecurity and, therefore, opportunities for malicious actors to introduce viruses, malicious code, or other exploits into the system.
- During periods where city roads have a mix of autonomous and non-autonomous vehicles, safe and efficient autonomous vehicle functionality will require more complex capabilities as autonomous vehicles will have to account accurately for other autonomous vehicles, semi-autonomous vehicles, and non-autonomous vehicles.

Increased Automation

- The automation that comes with autonomous vehicles requires the use of a wide variety of sensors, including LIDAR, GPS, radar, and video cameras, all of which add potential vulnerabilities and attack vectors to autonomous vehicles.

[27] Kelly, Anne Marie, "Has Toyota's Image Recovered from the Brand's Recall Crisis?" http://www.forbes.com/sites/annemariekelly/2012/03/05/has-toyotas-image-recovered-from-the-brands-recall-crisis/, accessed December 8, 2014.
[28] Edwards, Jim, "Here's The Most Obvious, Terrifying Flaw In Google's Self-Driving Car Prototype: The 'Panic Button,'" http://www.businessinsider.com/flaw-in-googles-self-driving-car-prototype-the-panic-button-2014-5, accessed December 6, 2014.

POSITIVE TRAIN CONTROL

Positive Train Control (PTC) is a system of remote sensors and automated control devices primarily designed to stop or slow a train automatically to prevent dangerous situations. Through wired and wireless connections and automated acceleration and deceleration controls, PTC is used to prevent train-to-train collisions, derailments caused by excessive speed, and unauthorized movement of trains. PTC systems typically involve four elements: onboard systems, wayside systems, a central dispatch center, and a communication system. Onboard systems are located on trains themselves and include GPS and other location systems, as well as train control systems. Wayside systems include signal crossings, track switches, and maintenance points. The communication system transmits inputs from these first two systems to the dispatch center. Track information is than transmitted from the dispatch center back to the trains and wayside infrastructure. These commands can result in suggestions for train and infrastructure operators or can be programmed to carryout operational changes automatically.

In 2008, the U.S. Congress mandated the implementation of PTC systems on most railroad networks, by December 2015. Currently, some progress has been made, but many rail agencies have indicated they do not have the necessary resources to meet the deadline, and they are uncertain if the technology and training necessary for full PTC operation will be ready.[29] The Government Accountability Office and others have recommended granting extensions on the 2015 PTC mandate, and several bills have been introduced to extend the deadline, but as of July 1, 2015 no extension has been granted.[30]

PATHWAY 2: POSITIVE TRAIN CONTROL SYSTEM FAILURES

Sample Vector 1: A malicious actor accesses and manipulates PTC systems to threaten rail safety and cause collisions or derailments.

A malicious actor could create unsafe conditions by transmitting an "all clear" signal, despite the presence of a stalled train, or by blocking transmission of a signal warning of a stalled train or upcoming sharp turns. Similarly, an actor could access PTC systems to stop trains at specific locations, leaving cargo, passengers, and crew vulnerable to hijacking or other types of attack. Such cyber-attacks could be accomplished by sending faulty signals directly to onboard PTC components to warn of danger ahead, or by manipulating wayside signals (e.g., displaying red signal lights) to stop approaching trains. Both situations could trigger automatic braking mechanisms onboard a targeted train. Alternatively, a malicious actor could block the availability of incoming track information from a dispatch center, causing a safety-override mode on affected trains that often results in an automated full stop.

In 2008, a teenager allegedly remotely accessed a tram system in Lodz, Poland, and successfully manipulated signal controls. By observing train movement patterns from public locations, he was able to change signals that caused derailments and injuries.[31]

- The inherent level of automation and controllability of PTC systems makes vulnerabilities particularly dangerous if a malicious actor can exploit them.[32] After obtaining system level access, an actor could execute a variety of commands, many of which could cause a chain of automated reactions with little or no human oversight to recognize unsafe dynamics and warning signs. Malicious actors could exploit a wide variety of system entry points, as PTC and railway systems involve a considerable amount of hardware spread over a large area, including rural and geographically remote and hard-to-access locations.
- The dispersed nature of PTC systems allows threat actors the ability to also conduct attacks, by connecting to the device both physically and remotely, and to bypass secured dispatch or command

[29] Boardman, Joe, "Train safety takes money, cooperation." http://www.usatoday.com/story/opinion/2013/12/16/derail-amtrak-railways-safety-column/4002855/, accessed November 15, 2014; Monitor 360 Interview with a Transportation Scholar, August 7, 2014.
[30] Government Accountability Office, "Actions Have been taken to Enhance Security, but the Federal Strategy can be Strengthened and Security Efforts Better Monitored." http://www.gao.gov/products/GAO-09-243, accessed November 3, 2014; S.650, Railroad Safety and Positive Train Control Extension Act, https://www.govtrack.us/congress/bills/114/s650, accessed July 13, 2015; S.1006, A Bill to Incentivize Early Adoption of Positive Train Control, and For Other Purposes, https://www.govtrack.us/congress/bills/114/s1006 , accessed July 13, 2015.
[31] Grant, Ian, "Schoolboy hacker derails Poland's tram network," http://www.computerweekly.com/news/2240084537/Schoolboy-hacker-derails-Polands-tram-network, accessed December 6, 2014.
[32] Monitor 360 Interview with a Cyber-Physical Systems Expert, July 28, 2014.

centers.[33] A threat actor that gains system level access could potentially surreptitiously control or stop a train.

At a minimum, PTC disruptions or errors in the system could potentially result in dangerous speeds and the increased potential for collision and derailment. A more focused attack could result in national-level security repercussions. Targeting crowded passenger trains (e.g., colliding two passenger trains at high speeds or near crowded platforms) or trains carrying dangerous chemicals or explosive materials (e.g., Toxic Inhalation Hazard cargo such as chlorine gas), could lead to loss of life or economic damage.[34]

Sample Vector 2: Interoperability failures lead to significant system errors.

Many railroad companies share portions of the same tracks, creating a diverse, inter-connected system in which different sections of track are controlled by different companies. As each company is responsible for implementing its own PTC system, interoperability is crucial to minimize unsafe conditions. The Legislation mandating the implementation of PTC technology includes a requirement that all PTC systems are interoperable among the different rail lines compounding the issue of complying with the mandated deadline.[36] The technology required to allow PTC interoperability across different railroad systems—different railroad systems must be able to communicate to each other, and trains must be able to operate on multiple railroad systems—is still in development, making it difficult to install PTC systems that guarantees future interoperability. In addition, although most railroad companies have sought interoperability agreements with other companies in their railroad classification, there is little transparency regarding how much attention intra-class interoperability is receiving.[37] Ensuring interoperability that allows for future technologies and uncertainties is also challenging. Similarly, inconsistent implementation and poor maintenance could cause problems and system errors. Even with a focus on testing and failsafe mechanisms, computer systems inevitably experience some degree of bugs, glitches, and errors, and even a single bug can lead to catastrophic consequences. For example, in 2006 a bug in San Francisco's BART transportation system caused three rail lines to shut down over 7 hours. Nobody was injured, but estimates put the economic cost of similar shutdowns at $1 billion.[38] As networked PTC systems grow, so will their complexity, making controllability to prevent errors all the more challenging.

In June 2009, a Washington, DC Metro system train crashed into a stopped train, resulting in nine fatalities and 52 injuries. The cause was deemed to be a faulty track circuit, which failed to register and relay the presence of the stopped train back to the dispatch center. Not recognizing the presence of a stopped train, the dispatch center indicated that other trains in the area should proceed as normal, resulting in the crash. The National Transportation Safety Board indicated that the Washington Metropolitan Area Transit Authority (WMATA) failed to conduct proper maintenance, and the manufacturer of the track circuit failed to provide a maintenance plan to WMATA.[35]

Errors in PTC systems could have regional-level consequences, most likely in the form of delays, which would inflict a secondary effect on the National economy. Interoperability problems leading to malfunctions are less likely but could also cause collisions or unsafe speeds. Any system error resulting in a train collision, particularly involving fatalities, could increase public fear of rail travel, although accidents from system errors are unlikely to have the same negative psychological impact as a directed attack on PTC systems.[39]

---

[33] Monitor 360 Interview with a Transportation Scholar, August 7, 2014.
[34] Branscomb, Lewis et al, "Rail Transportation of Toxic Inhalation Hazards," http://www.hks.harvard.edu/m-rcbg/rpp/Working%20papers/Rail%20Transportation%20of%20TIH.pdf, accessed December 8, 2014.
[35] "Collision of Two Washington Metropolitan Area Transit Authority Metrorail Trains Near Fort Totten Station." http://www.ntsb.gov/doclib/reports/2010/RAR1002.pdf, accessed November 18, 2014.
[36] The Rail Safety Improvement Act of 2008 and "Freight Railroads Assert FCC-Required Antenna Review Lengthening Delays in Installing Positive Train Control." https://www.aar.org/newsandevents/Press-Releases/Pages/Freight-Railroads-Assert-FCC-Required-Antenna-Review-Lengthening-Delays-in-Installing-Positive-Train-Control.aspx, accessed November 9, 2014.
[37] Stagl, Jeff, "Railroads Set Positive Train Control Development & Interoperability Strategies to Meet 2015 Mandate." http://www.progressiverailroading.com/ptc/article/Railroads-Set-Positive-Train-Contol-PTC-Development-amp-Interoperability-Strategies-to-Meet-2015-Mandate--18969, accessed October 7, 2014.
[38] Townsend, Anthony, "Smart Cities: Big Data, Civic Hackers, and the Quest for a new Utopia." New York: W.W Norton & Company, 2013.
[39] Monitor 360 Interview with a Transportation Scholar, August 7, 2014.

POSITIVE TRAIN CONTROL TECHNOLOGY-SPECIFIC OBSERVATIONS

Changing Seams

- As PTC-equipped rail links remote and urban areas, PTC infrastructure may establish new cyber-physical connections between remote and urban areas. In turn, vulnerabilities that a malicious actor exploits in remote areas may extend consequences to urban areas and vice versa.
- Widespread PTC introduces new, networked hardware devices throughout the rail systems. These devices—spread across urban and remote points of the system—add countless physical access points into cyber-physical rail networks, increasing the attack surface.

Inconsistent Adoption

- Increased diversity in PTC technology, specifically in radio frequency usage, will make it more difficult to secure frequencies or monitor for unauthorized usage.
- Where different PTC systems fail to interact smoothly, system errors can increase the reliance on manual control and the potential for human error, particularly if manual skills have atrophied as automation has become more prevalent.

Increased Automation

- As rail automation and efficiency increases with ubiquity, potential staff decreases could result in less human oversight, less maintenance and repair capacity, and a loss of institutional knowledge.
- The presence of networked wayside devices, such as signals and track switches, will leave even the most secured trains vulnerable to compromised wayside devices.

INTELLIGENT TRANSPORTATION SYSTEMS

An Intelligent Transportation System (ITS) is a system in which real-time data is gathered and used to inform automated decisions regarding the function of traffic-related infrastructure and hardware. These systems typically include four main elements: sensors that gather information on traffic conditions, controllers that make changes to traffic control devices (e.g., traffic lights), a central computer to analyze data and suggest system adjustments, and a communication system to link the various components. Although traffic communication networks have traditionally been hardwired, cities are increasingly looking to wireless networks for such communications. For example, an ITS-enabled intersection could have a video camera or an in-ground induction loop sensor to detect the presence of cars. These sensors would transmit data to a controller, which could then optimize the function of a traffic light for traffic conditions. Controllers can be pre-programmed to take certain actions based on inputs from local sensors or can be manually controlled from a central point. In either case, the data collected by sensors is transmitted back to a central computer, where it is analyzed and added into the broader data collection pool.

Several pilot implementation programs around the country have already proven relatively successful, including the "Midtown in Motion" program in New York City, covering a 110-block area. As the safety and efficiency benefits of these systems become apparent, it is likely that adoption rates will increase as other cities strive to follow suit.[40]

PATHWAY 3: INTELLIGENT TRANSPORTATION SYSTEM DISRUPTION

Sample Vector 1: A malicious actor accesses ITS networks during a natural or man-made disaster to create unsafe driving conditions or system congestion, trapping people in an affected area.

By targeting communications or central computing systems, a malicious actor could cause multiple traffic signaling devices to shut down or, more likely, enter a failsafe mode (e.g., a blinking red light). Alternatively, a malicious actor could target traffic signaling devices themselves, causing local and regional disruptions that increase congestion and decrease safety in specific target areas.

[40] Monitor 360 Interview with a State Transportation Administrator, August 29, 2014.

- The large number of networked devices in an ITS network creates multiple potential entry points for an actor seeking access to the system, increasing vulnerabilities to a malicious attack.[41] Traffic lights, for example, could be a relatively accessible vector for malicious actors to gain access to the broader ITS network, particularly if the traffic lights are in low-traffic and hard-to-monitor areas.
- Wireless communication networks used by ITS systems are also vulnerable to this kind of attack, partially due to the propensity of ITS administrators to route communications through existing enterprise networks. Although such routing generally provides convenience and cost benefits, shared commercial networks are often less secure. The lower security standards, visibility, and control inherent in many commercial networks, as well as the familiarity many hackers have with these systems, would make it easier for a malicious actor to observe or intercept ITS data.[43]
- ITS technology may be more vulnerable to attacks coinciding with natural or man-made disaster because of the fragility of many widely used communication nodes during such events. Wi-Fi and cellular systems frequently become overloaded and fail—or are directly damaged and fail—during crises, as evidenced by the September 11, 2001 attacks, Hurricane Katrina in 2005, and the 2011 tsunami in Japan.[44] The brittleness of these communication nodes during crises could make it easier for actors to impact driving conditions and contribute to overall congestion.

In 2014, a University of Michigan team accessed a traffic light network using readily available hardware. Once inside the system, the team quickly gained the ability to change traffic signals, alter logic commands, and disable the signal devices. Similarly, security researchers at IOActive recently highlighted the ease of accessing ITS infrastructure and the lack of attention these vulnerabilities receive from both technology vendors and local administrators.[42]

The consequences of this type of attack would largely relate to constrained vehicle flow in the targeted area, and an increase in dangerous driving conditions.[45] More specifically, congestion could prevent efficient egress in situations of immediate danger or prevent emergency personnel from providing timely assistance, leaving higher risk citizens and those with injuries more vulnerable. If an actor executed an attack to coincide with a manmade incident or natural disaster, the inability to travel by road would likely contribute to panic, loss of life, or overall danger resulting from the initial incident.

Sample Vector 2: A malicious actor tampers with ITS data integrity to lower long-term system functionality, trust, and safety.

A malicious actor could interfere with data integrity in an ITS system by targeting networked transportation infrastructure devices or by inserting inaccurate information into the system. Altering sensor data integrity could cause dissemination of faulty information to the broader system, causing the system's central computers to issue inefficient or unintentionally unsafe commands to other network devices. Although ITS systems will be able to recognize and block known faulty or clearly dangerous signals, inauthentic signals that are merely inefficient will be harder to identify. Instead of destroying devices or creating other kinds of visible damage, this tampering with data integrity could instead make subtle changes to otherwise functional systems. As a result, recognizing the presence of an attack and then identifying and blocking the source would likely be difficult, time-consuming, and expensive.[46] The inability to recognize and remove a problem quickly could amplify the impact of an attack the longer the faulty data remains

When two lanes on the George Washington Bridge were unexpectedly closed in November 2013, conservative estimates hold that the resulting traffic jam, which only lasted for several hours, cost the New York economy more than $7 million. In addition to economic costs, the resulting traffic jam prevented emergency vehicles from responding to calls and drastically lowered overall response time.[1]

[41] Monitor 360 Interview with a Vehicle and Hardware Hacker, July 30, 2014.
[42] Ghena, Branden, et al, "Green Lights Forever: Analyzing the Security of Traffic Infrastructure." https://jhalderm.com/pub/papers/traffic-woot14.pdf, accessed November 17, 2014; Cerrudo, Cesar, "Hacking US Traffic Control Systems." http://blog.ioactive.com/2014/04/hacking-us-and-uk-australia-france-etc.html, accessed November 16, 2014.
[43] Monitor 360 Interview with a Vehicle Communications Expert, July 31, 2014; Monitor 360 Interview with a Vehicle and Hardware Hacker, July 30, 2014.
[44] Townsend, Anthony, "Smart Cities: Big Data, Civic Hackers, and the Quest for a new Utopia." New York: W.W Norton & Company, 2013.
[45] Ghena, Branden, et al, "Green Lights Forever: Analyzing the Security of Traffic Infrastructure." https://jhalderm.com/pub/papers/traffic-woot14.pdf, accessed November 17, 2014.
[46] Monitor 360 Interview with a Vehicle and Hardware Hacker, July 30, 2014.

in the system. Further, the large number of authorized users necessary to operate, maintain, update, and repair ITS networks will make it difficult to monitor and identify suspicious behavior and potentially allow threat actors to disguise their actions behind standard procedures or background noise of daily operations.

Although most attacks of this nature would likely result in isolated traffic congestion and a small number of traffic accidents, there are several ways they could have more significant economic and national security consequences.[47] Executed across multiple areas of multiple cities, the effects of such an attack could cause loss of life and foster mistrust in Smart City technology. A group of malicious actors working together could manipulate incoming and outgoing ITS data in multiple intersections, onramps, toll plazas, interchanges, and other critical ITS sensor locations across a city. Prolonged red lights, a lack of metering on onramps during rush hour, or the closing of reversible lanes could cause citywide traffic congestion, potentially affecting a city's transportation grid for extended periods of time—depending on the severity of the attack. Estimates put the opportunity cost of an individual sitting in traffic—or the cost to a local economy—at roughly $17 per hour of person travel.[48] Multiple engineered traffic jams across a series of large cities along the Eastern Seaboard, for example, could negatively affect the local economy while ripple effects could cascade to the state, regional, or national level.

INTELLIGENT TRANSPORTATION SYSTEM TECHNOLOGY-SPECIFIC OBSERVATIONS

Changing Seams

- As ITS systems become more pervasive in Smart Cities, the systems will introduce new, networked devices (e.g., traffic signals, traffic signs, or standalone sensors) and expand avenues for remote access to the entire system.
- High numbers of communication links within ITS increases the attack surface and may lead to the use of existing public or commercial communication networks—many of which use commercial networks lacking robust security capabilities.

Inconsistent Adoption

- Although ITS implementation costs are likely to stabilize over time, security and maintenance will perpetually fluctuate as cities discover and adapt to new vulnerabilities and technology advancements, making change and adaptation part of the status quo.
- Once ITS systems become pervasive, they will involve a significant number of devices and components over a large area, all requiring regular maintenance and upgrades. Smaller or budget-constrained cities implementing ITS may not have the staff or resources necessary to maintain ITS systems securely.
- As ITS technology and guidelines evolve, cities will see increasing challenges in keeping the systems interoperable, secure, and efficient. Such challenges are particularly true for early ITS adopters, who may require more frequent, incremental upgrades that bring potential interoperability issues (versus later adopters, who may be better positioned to pursue larger-scale system replacements with more proven technologies).

VEHICLE-TO-VEHICLE AND VEHICLE-TO-INFRASTRUCTURE

Vehicle-to-vehicle (V2V) technology uses Dedicated Short-Range Communications—a technology that is similar to Wi-Fi and has a range of about 3,000 feet—to allow vehicles to "talk" to one another and to stationary infrastructure such as buildings and street lights.[49] Cars and trucks on a V2V network can send and receive data about their location, speed, and distance relative to other connected cars in order to alert drivers to potential dangerous situations. For example, Left Turn Assist alerts drivers when oncoming traffic creates unsafe left turn

[47] Monitor 360 Interview with an ITS Administrator, September 30, 2014.
[48] "2012 Urban Mobility Report," Texas A&M Transportation Institute. http://mobility.tamu.edu/ums/report/, accessed November 19, 2014.
[49] 3,000 feet is based on ideal conditions. There are a number of variables that affect the range of Dedicated Short-Range Communications at any given time.

situations. Intersection Movement Assist helps drivers avoid collisions in dangerous or crowded intersections.[50] Vehicle-to-infrastructure (V2I) systems allow physical infrastructure—including traffic signals and onramps—to inform vehicles of their presence, and to allow vehicles to send information to the infrastructure. For example, a stoplight could suggest a speed that would allow an approaching driver to arrive at the light as it changes to green, reducing stop and start time and overall congestion.

With strong support from Federal, State, and local government—including a 2012 "Safety Pilot" model deployment program in Ann Arbor, Michigan, in which nearly 3,000 vehicles were networked—V2V and V2I technologies are likely to become widely used within 5 – 10 years.[51] In 2014, the National Highway Traffic Safety Administration (NHTSA) announced that it was working on a new regulation to mandate V2V technologies in all cars in the near future, with the goal of promoting widespread adoption. These new regulations may take effect by 2020, by which time some experts estimate over 25 percent of cars will have V2V technologies and over 60 percent of cars will be connected.

PATHWAY 4: WIDESPREAD MALFUNCTION OF AUTOMATION SYSTEMS

Sample Vector 1: A malicious actor disrupts V2V and V2I signals to impact system functionality.

A malicious actor could interfere with safety-related data as it is communicated over V2V networks. Blocking a vehicle's data output regarding sudden braking, acceleration, lane changes, or turning would leave surrounding vehicles blind to these actions. Malicious actors could also manipulate a vehicle's computer system such that the data sent out to surrounding vehicles is based on faulty information. Alternatively, a malicious actor could disrupt V2I networks, targeting networked traffic devices or V2I relay points. Inaccurate information about upcoming road features—including lane merges, sharp turns, or dangerous conditions ahead—could severely curtail system performance and affect a larger number of networked vehicles, as faulty information would be disseminated to all cars in a given area.[52] The use of on-board sensors identifying traffic independently of the V2V network may create redundancies that lower risk.

- The involvement of multiple vendors in the design and construction of automation systems will likely introduce vulnerabilities into the technology. Automobile manufacturers are likely to outsource the design and installation of various aspects of their automation system.[53]
- The safety features these technologies provide will likely lead to atrophied vigilance and responsiveness as people become accustomed to automated controls. Unexpectedly removing the safety features provided by functioning automation systems could have a disproportionately harmful effect on safety conditions if that were to occur after drivers have been using automation systems for some time.[54]
- As mentioned previously with autonomous vehicles, when specific vulnerabilities are identified, installing system updates and security patches in V2V-enabled vehicles may be inconsistent and time-consuming depending largely on individual owners' prerogative.[55] Although vehicle manufacturers can currently "push" security updates to vehicles in an efficient way, manufacturers will need to assess repeatedly the security aspects of such "push" updates as more cellular and Wi-Fi connectivity in vehicles potentially create unanticipated network linkages between systems.[56]

The consequences of an attack against V2V and V2I signals could affect local public safety in a Smart City, although the consequences would likely be limited to traffic accidents and congestion. Manipulating onboard automation systems would require a malicious actor to maintain close proximity with target vehicles, limiting the range of any attack. Attacking a V2I device would allow malicious actors to impact a large number of vehicles at once. For

[50] Halsey, Ashley, "Communication between car computers may reduce accidents by up to 80 percent." http://www.washingtonpost.com/local/trafficandcommuting/direct-communication-between-car-computers-may-reduce-accidents-by-up-to-80-percent/2014/02/03/b55e9330-8d1a-11e3-833c-33098f9e5267_story.html, accessed November 19, 2014.
[51] Monitor 360 Interview with a Vehicle Communications Expert, July 31, 2014.
[52] bid.
[53] bid.
[54] Monitor 360 Interview with a National Highway Administrator, August 6, 2014.
[55] Monitor 360 Interview with an Autonomous Vehicle Expert, August 7, 2014; Mimoso, Michael, "Car Hacking Enters Remote Exploitation Phase," http://threatpost.com/car-hacking-enters-remote-exploitation-phase/107626, accessed November 19, 2014.
[56] Pushing software changes (especially automated control functions) to vehicles is significantly different than updating a computer or other system. Regulatory authorities will need to determine whether and how the vehicle will remain approved for operation if the software update changes the operating characteristics of the vehicle. Email from Department of Transportation, Federal Highway Administration, January 21, 2015.

example, if a networked traffic light sends a signal to networked cars in an area to indicate a traffic light suddenly turned red when it is actually green, multiple cars would be forced to brake rapidly, increasing the risk of collisions. If executed across multiple sections of high-speed areas, this type of attack could cause multiple accidents, potential loss of life, and potential economic impact.

Sample Vector 2: A malicious actor capable of disrupting V2V and V2I networks blackmails automobile owners or manufacturers.

A malicious actor could demonstrate the ability to disrupt a networked vehicle's V2V or V2I functionality on a small scale and then blackmail the vehicle's owner. Additionally, the malicious actor could threaten to manipulate the system on a larger, more publicized scale, and blackmail the vehicles' manufacturer unless a fee is paid. The consequences of this type of attack could warrant regional- or national-level attention based on the potentially large-scale economic fallout for automobile manufacturers, and the attack may negatively affect public trust and confidence in cyber-physical technology more generally. If this type of incident were to occur, automobile manufacturers may have to undergo potentially expensive security patches to fix the exploitation in question. Public knowledge of this type of incident could cause consumers to question the safety and security commitment of the manufacturers of V2V-enabled vehicles, which could slow adoption rates and cause economic damage to car companies using V2V and V2I technology.

Blackmail involving cybersecurity is not unprecedented, as hackers have previously demanded ransoms from companies including Nokia, Domino's Pizza, Evernote, and Feedly after demonstrating their ability to access encrypted files and otherwise disrupt services. Although not all victims have given in to hackers' demands, some hacks have been deemed serious enough to justify paying a ransom, as was the case in 2007 when Nokia paid a ransom of several million dollars to prevent the release of stolen encryption keys.[57]

VEHICLE-TO-VEHICLE AND VEHICLE-TO-INFRASTRUCTURE TECHNOLOGY-SPECIFIC OBSERVATIONS

Changing Seams

- As V2I systems become more pervasive, they will interact with—and perhaps become part of—simultaneously evolving cyber-physical infrastructure systems (such as ITS), requiring that system developers and city administrators continually address interoperability and security beyond initial implementation stages.
- V2I systems will leave V2I- and V2V-enabled cars vulnerable to direct attacks on the automobiles themselves and to attacks on a wide variety of infrastructure devices, which may receive less security scrutiny than automobiles.

Increased Automation

- As the driving assistance features of V2V and V2I systems become more ubiquitous, drivers are likely to increasingly rely on such features. This reliance may result in skill atrophy, eroding driver proficiency and increasing vulnerability to accidents and congestion in the event of a system failure.

[57] Farivar, Cyrus, "Nokia paid millions in ransom to stop release of signing key in 2007," http://arstechnica.com/tech-policy/2014/06/nokia-paid-millions-in-ransom-to-stop-release-of-signing-key-in-2007/, accessed November 17, 2014; and "Hackers steal Dominos Pizza customer data in Europe, ransom sought," http://www.reuters.com/article/2014/06/16/us-dominos-pizza-cybersecurity-idUSKBN0ER1TF20140616, accessed November 16, 2014; McGregor, Jay, "Feedly And Evernote Go Down As Attackers Demand Ransom." http://www.forbes.com/sites/jaymcgregor/2014/06/11/feedly-and-evernote-go-down-as-attackers-demand-ransom/, accessed November 18, 2014.

ELECTRICITY IN SMART CITIES

This section focuses on the future dynamics of cyber-physical infrastructure in Smart Cities within the Electricity Subsector of the Energy Sector, as part of a broader series of Sector-level inquiries emphasizing security and resilience. Smart City technology security challenges are likely to affect the general security risks already inherent in electricity networks. Potential sources of increased risk include:

- Advances in bottom-up innovation and distributed generation technology will complicate how electricity utility companies operate, adding new security, stability, and interoperability variables.[58]
- Smart technologies will increase the networking and automation of generation, distribution, transmission, and metering processes in the electricity grid. In addition to addressing new security vulnerabilities, avoiding interoperability problems and performance issues will be a challenge.
- Smart grids will introduce a large number of hard-to-secure physical devices with networked connectivity—many of which will interact directly with customers—expanding the attack surface and introducing hard-to-control variables.

Three cyber-physical technologies that will be part of future Smart City electricity systems are smart power generation plants, smart distribution and transmission, and advanced metering infrastructure.

SMART POWER-GENERATION PLANTS

Adoption of smart power-generation technology in large power plants is increasing, with many utility administrators seeking collaboration to set standards and increase information sharing.[59] Smart power-generation systems use an array of networked sensors and meters to gather real-time system data—from both inside a power-generation plant and from the outside system, including transmission and distribution systems. This data is transferred through communication networks to a central control point for analysis. Intelligent electronic devices—such as programmable logic controllers—and supervisory control and data acquisition (SCADA) systems then automatically respond with automatic generation control. As power-generation plants have become increasingly automated, the combination of new automated capabilities and advanced networking present opportunities to identify problems faster, reduce costs, and increase overall system efficiency. These additions, coupled with new power-generation systems designed to adjust load demand more rapidly, can improve power-generation facilities' ability to meet constantly changing energy demands accurately and rapidly.

Changing consumer demands, environmental factors, resource availability, and new power-generation strategies increase the need for faster regulation and load following. For example, increasing numbers of solar panels and wind turbines can be considered part of the smart power-generation landscape—known as distributed generation—complicating the load-balancing equation by increasing the number of generation sources. Unlike traditional electricity generation, which usually comes from a smaller number of larger facilities, distributed generation infrastructure relies on a larger number of dispersed facilities. This increases the overall number of failure points in the power-generation system, while increasing variation in available output. Conditions that are less conducive to energy generation (such as cloud cover or lack of wind) could leave customers in need of additional electricity-generation sources, putting an unanticipated strain on legacy generation facilities. Many existing generation plants are unable to increase energy production quickly and are not designed to handle a rapidly changing demand for power.[60] Although advances in energy-storage technology may help ease this burden, smart load is also a central aspect of increasing load-balancing capabilities.

[58] "Distributed generation," also sometimes known as embedded-generation technology, refers to solar, wind, and other decentralized forms of energy generation. Private individuals or organizations can install and manage distributed generation systems with limited involvement from public energy utility companies.
[59] Monitor 360 Interview with Energy System Engineer, November 3, 2014.
[60] Monitor 360 Interview with Smart Grid Expert, October 31, 2014.

PATHWAY 1: SMART POWER-GENERATION PLANT DISRUPTION

Sample Vector 1: A malicious actor gains access to SCADA systems or other control systems within a power plant to damage components and disrupt electricity delivery.

Because of the high degree of connectivity and automation in smart power-generation systems, a malicious actor able to exploit system weaknesses, might be able to take control of a large number of critical components within one or several smart power-generation plants, including boilers, turbines, pumps, and valves. Control of these components could be used to take a variety of disruptive actions such as changing the flow of steam to a turbine; underserving or overwhelming it; keeping a turbine spinning without necessary lubrication; or preventing water from reaching a cooling system. A malicious actor could also engage in harmful subterfuge, turning off SCADA and other remote capabilities to prevent remote fixes. Data manipulation could be used to hide the presence of a disruption, increasing the likelihood of resulting breakage or wider system impact. Data manipulation could also be used to deliver false data readouts, prompting operators or administrators to take inefficient or dangerous actions.[61] These attacks could be launched by anyone with access to these systems, including unauthorized access by insiders or hackers.

A malicious actor could also conduct attacks using malicious software. By using infected hardware, emails, or transmission vectors, a malicious actor could introduce malware that is designed to change various parameters in smart power-generation systems, with the goal of breaking machinery. Actors could design malware to locate and manipulate specific hardware devices or software systems, wait to execute an attack at a pre-determined time, and seek opportunities to propagate further.

- Many power-generation plants use decades-old technology and infrastructure, with purpose-built networks and control systems. As these systems were not designed to be networked into a broader system—from either a security or functionality perspective—the introduction of networked and cyber-physical systems brings new security challenges.[62] Many of these traditionally isolated systems with limited or one-way communication capabilities, such as SCADA systems, are now connected to two-way communication technology. Both the lack of native cybersecurity features and the difficulty of adding comprehensive cybersecurity features into pre-existing hardware increase vulnerability to cyber-attacks.[63] A malicious actor with access to a highly networked power-generation plant would have control over many more system functions than in a traditional plant.
- The desire for grid efficiency and transparency leads many power companies to connect long-segregated control systems to additional outside systems and to the Internet, increasing the overall attack surface. The reliance on power plant operators and utility companies to self-report security regulation compliance—and the fact that regulations only require that minimum standards be met—makes it difficult to ensure that utilities employ adequate safeguards.[64]
- Utility administrators face a challenge from engineers and system operators who may resist upgrading or changing the legacy software. The reluctance to upgrade or change software could manifest itself in varying ways. For example, engineers and operators may be reluctant to operate modern cyber-physical systems or to install new security updates for fear of causing unanticipated consequences that damage established and understood configurations.[65]
- It is often prohibitively expensive or disruptive to service to update or replace outdated systems. Administrators may therefore choose to accept the risk of operating with legacy systems.
- Some large components, such as transformers and turbines, have a limited number of manufacturers and are only made to order, and therefore have long lead times for replacement. If these components are damaged, the long replacements time can lengthen the impact of attacks on smart power plants.

[61] Monitor 360 Interview with Smart Grid Expert, October 31, 2014.
[62] Monitor 360 Interview with a Cyber-Physical Security Expert, July 24, 2014.
[63] Monitor 360 Interview with Cyber-Physical Energy Expert, August 28, 2014.
[64] Monitor 360 Interview with Cyber Security Expert, June 30, 2014, and, "Feds Fear Coordinated Physical, Cyber-Attack on Electrical Grids." http://www.nationaldefensemagazine.org/archive/2012/september/Pages/FedsFearCoordinatedPhysical,Cyber-AttacksonElectricalGrids.aspx, accessed October 17, 2014.
[65] Monitor 360 Interview with Energy System Engineer, November 3, 2014.

Attacks on smart power-generation plants could have a significant impact at the local or regional level if they cause ongoing brownouts or blackouts, especially if an attack targets multiple plants at the same time. In addition, a purposefully caused power outage could cause significant economic damage as many businesses would be unable to operate. Blackouts that are publicized as resulting from attacks may cause mistrust towards public utilities, and increase the potential for unrest or panic. An attack targeting multiple smart power-generation plants would increase the affected area and lead to longer outages, increasing the likelihood of loss of life and other negative impacts. The effects of any attack targeting physical hardware would be particularly problematic, as some generation components do not have regularly available spare units in storage due to their size and cost, and also require long lead times to build, ship, and install.[66]

Sample Vector 2: A malicious actor exploits vulnerabilities in widely used information technology (IT) services or third-party vendors to disrupt smart power-generation plants.

By targeting hardware and technology manufacturers—i.e., inserting security vulnerabilities or backdoors prior to device installation—a malicious actor could potentially gain access to multiple power-generation facilities simultaneously A malicious actor could also take advantage of widely used commercial IT services to attack multiple power systems concurrently. By gaining system administrator access or by altering software, a malicious actor could target critical components in smart power-generation plants. Software or control systems could be adjusted to decrease efficiency and system responsiveness; to shut down components or power-generation plants; or to damage or destroy specific components within generation plants. Similarly, as the linking of power-generation facilities to one another increases, a malicious actor potentially could access power-generation facilities in smaller cities to gain access to facilities in larger cities.[68]

The National Information Solutions Cooperative is an example of smaller energy and telecommunications companies working together to share collective knowledge and information technology systems, and create a more affordable IT solution for the operation of Smart City technologies in the Energy Sector.[67]

- Cities and utilities may employ third-party or cooperative IT systems, potentially increasing the number of vulnerabilities that could be exploited by a malicious actor.[69]
- Alternatively, groups of smaller cities may seek to collaborate in the form of IT cooperatives, utilizing their collective experience and knowledge to overcome their resource limitations.

These vulnerabilities could have a significant impact on national security if they were exploited to destroy components in smart power plants and to cause power outages. If a malicious actor inserted malware or design flaws into a widely used third-party IT system, the actor could gain the ability to cause blackouts across multiple power-generation facilities, possibly leaving entire regions without power.[70] If power-generation companies within a city rely on third-party or shared IT systems for all of their power-generation, cutting off power to all systems that rely on these tools could leave hundreds of thousands without power. If malicious actors were able to penetrate several distinct widely used systems, the loss of life and economic impacts could be greatly multiplied.

Sample Vector 3: Installation of new cyber-physical components onto legacy components leads to interoperability problems, unintended consequences, and smart generation system disruptions.

System errors involving SCADA systems in power plants are not a new development. However, the level of interconnectedness, automation, and controllability of cyber-physical components will likely lead to a trial-and-error period, necessitating near-constant system updates. Updates themselves often increase overall complexity by fixing a specific problem but introducing more unintended risk.[71]

Evolving smart generation systems are also likely to experience system errors caused by the increase in system interactions, particularly surrounding distributed generation technologies—i.e., solar panels on residential roofs or

[66] Monitor 360 Interview with Smart City Security Expert, July 21, 2014.
[67] National Information Solutions Cooperative, http://www.nisc.coop/, accessed December 5, 2014.
[68] Monitor 360 Interview with Smart Grid Analyst, November 3, 2014.
[69] Monitor 360 Interview with Smart Grid Expert, October 31, 2014.
[70] bid.
[71] Townsend, Anthony, "Smart Cities: Big Data, Civic Hackers, and the Quest for a new Utopia." New York: W.W Norton & Company, 2013.

wind turbines on university or corporate campuses.[72] Many of these systems will be installed and managed by customers themselves, with little or no involvement from utility companies, likely leading to unintended consequences with potentially system-wide effects.[73] For example, although active voltage regulation is currently not permitted for residential customers, in the future a home solar panel may be able to automatically adjust voltage settings on a distribution feeder. Regulators and capacitors may then seek to readjust the voltage back to its original settings.[74] This constant back and forth could put a strain on system hardware, increasing breakdowns and shortening device lifespans. In general, the addition of new distributed generation systems into smart grids will bring new uncertainties, as control systems will interact with new combinations of hardware and software.

In 2008, a nuclear power facility in Baxley, Georgia, was forced to shut down for two days after a system software update caused a system reboot. Water reservoir sensors in a nuclear cooling system interpreted the reboot as a dangerous lack of water, triggering an emergency shutdown. Although not directly caused by cyber-physical elements, this type of malfunction highlights the potential for unanticipated consequences in highly automated and networked systems.[1]

- In the event of any incidents caused by distributed generation components, it is unclear who would be responsible for repairs and ongoing solutions. Utilities may be reluctant to pay to repair damage caused by systems owned by private companies or residences, and technology vendors may be reluctant to get involved because of intellectual property and liability concerns.[75]
- Utilities and consumers will likely use a larger variety of generation components, which will likely increase instances of hidden failures. Although installation of distributed generation systems—or, to a lesser extent, cyber-physical systems within power plants—may appear to function correctly under normal conditions without causing immediately visible problems, a change or system error in the broader distribution system could cause unexpected interoperability problems. The difficulty in anticipating and proactively fixing system errors broadens system vulnerability, as increased interconnectedness would allow system errors to spread beyond initial failure points.

SMART POWER-GENERATION PLANT TECHNOLOGY-SPECIFIC OBSERVATIONS

Changing Seams

- The integration of new components with legacy technology will create seams between different generations of technology, between staff with different skill sets, and, more generally, between functionality and security. These seams may hinder interoperability and operational transparency.

[72] Knapp, Eric and Raj Samani, Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure, Waltham, Elsevier, 2013.
[73] Monitor 360 Interview with Smart Grid Analyst, November 3, 2014; Monitor 360 Interview with Energy System Engineer, November 3, 2014.
[74] Monitor 360 Interview with Energy System Engineer, November 3, 2014; Monitor 360 Interview with Smart Grid Analyst, November 3, 2014.
[75] bid.

Inconsistent Adoption

- As distributed generation infrastructure (i.e., power-generation elements introduced into the system by individual or corporate consumers, such as solar panels or wind turbines) become more pervasive, it is possible they will experience errors and cause malfunctions in Smart City power grids. Although the impact of these errors could be localized, lack of clarity around responsibility for these elements could complicate vulnerability mitigation.
- System operators familiar with legacy generation systems may resist full adaptation of smart generation system components (e.g., software updates) out of concern for disrupting known functionalities. Inconsistent technology implementation and use across the system will increase the instance of avoidable vulnerabilities and system errors.
- Current staff may have difficulty learning to operate new control systems, and new staff may not have a comprehensive understanding of legacy systems. This will increase vulnerabilities stemming from system errors that may require manual fixes, particularly in instances where smart generation facilities have both new and old infrastructure components.

Increased Automation

- Widespread implementation of smart generation technology within a Smart City will eventually require new cyber-physical and networking components to be integrated with existing infrastructure. Learning curves and system errors associated with integrating new components into older and less advanced control systems may create vulnerabilities.
- The comprehensive networking and automation of power-generation infrastructure associated with smart generation can expose Smart Cities to a wide variety of new cyber-attacks (e.g., unexpected variations of the Stuxnet attacks) that could break components or cause outages, explosions, or other hazardous effects.

SMART DISTRIBUTION AND TRANSMISSION

Smart distribution and transmission systems are designed to increase overall smart grid intelligence, awareness, efficiency and flexibility, and reduce distribution and transmission errors. These systems include the installation of various automation, networking, and cyber-physical devices. Smart distribution and transmission systems use SCADA systems and other automation devices to increase response times to localized power outages and to gather grid performance data faster. Likewise, the gradual installation of phasor measurement units (PMUs) and other sensors along distribution and transmission lines allows operators to gather real-time usage information, better incorporate embedded renewable energy generation into the grid, and isolate system interruptions before they spread. Networked sensors on transformers allow utilities to track equipment performance and better anticipate failures, reducing outages and repair costs. Finally, increased communication networks throughout distribution and transmission systems will improve overall system intelligence, allowing for better incorporation of demand-response programs, which let customers track energy availability and pricing to make consumption decisions accordingly. Where the technology is available, consumers will also be able to configure in-home devices—including air conditioners, water heaters, and other appliances—so that they activate when utility companies or others provide certain signals, such as price signals indicating that energy prices are lower.

Utility companies across the country are actively implementing smart distribution and transmission technology in order to secure efficiency, cost gains, and reduced system outages. The Department of Energy-manages the funding from the American Recovery and Reinvestment Act of 2009, which provides the basis to support upgrades to smart grids nationwide, and this funding has also buoyed implementation of smart distribution and transmission technology, supporting the installation of PMUs, smart substations, smart transformers, and other cyber-physical components.[76]

[76] "President Obama Announces $3.4 Billion Investment to Spur Transition to Smart Energy Grid." http://www.whitehouse.gov/the-press-office/president-obama-announces-34-billion-investment-spur-transition-smart-energy-grid, accessed December 2, 2014.

PATHWAY 2: SMART DISTRIBUTION AND TRANSMISSION MANIPULATION

Sample Vector 1: A malicious actor targets one or more newly networked and automated system components to disrupt power supply to customers.

Although distribution and transmission systems are composed of multiple components, attacks on several individual components could be executed to damage hardware or to cause system-wide brownouts and blackouts. For example, a coordinated attack targeting SCADA and wide-area communication networks associated with multiple transmission substations could allow actors to trip switches and automated protection systems and cause outages.[78] At a localized level, highly automated reclosers could be manipulated to cut off specific neighborhoods or buildings from the broader system. Likewise, targeting and disabling PMUs throughout a distribution system could stall monitoring capabilities Alternatively, an actor could target the communication systems between networked devices, preventing the timely delivery of data and threatening load-management capability.

In 2014, the security firm Symantec uncovered a large hacking group, (nicknamed Dragonfly) that repeatedly gained access to energy companies' control systems. The group successfully stole information from companies in several countries, including the United States. Although Dragonfly has yet to inflict any physical damage on an energy system, they have demonstrated the ability to compromise networked devices within the smart grid.[77]

- Distribution and transmission systems rely heavily on existing SCADA systems to enable real-time monitoring and automation capabilities, giving the SCADA systems almost total control of processes throughout the distribution and transmission architecture. The high degree of connectivity and digital access that cyber-physical technology brings to SCADA systems adds an attack vector that potentially allows actors to disrupt normal functionality—a risk that expands through the use of email and Web services for administration and maintenance purposes.[79]
- Distribution and transmission networks are vulnerable to insider attacks, as the degree of controllability present in these cyber-physical technologies would allow a malicious actor with system access to create widespread disruptions.

Although targeting individual distribution and transmission components would affect a limited area, attacking several components simultaneously could lead to widespread system strain and power loss. A malicious actor could target communication networks to prevent load-management mitigation, increasing the likelihood of cascading failures.[80] At a minimum, such attacks would also interfere with a utility company's ability to gather system information accurately, thereby threatening to disrupt proper load management. The consequences of such attacks could be amplified if executed during a natural disaster or a terrorist attack, or if systems that support critical infrastructures were specifically targeted. Moreover, the consequences of these attacks—and the potential destruction to critical system hardware—would likely be drawn out and potentially difficult to resolve quickly because some energy grid components, such as extra high-voltage transformers, are typically expensive and often manufactured abroad, adding additional time to any repairs.[81]

Sample Vector 2: A malicious actor intercepts and manipulates energy price data in demand-response systems to cause demand fluctuations and potential outages.

Data integrity is critical for the Electric Power Subsector to function properly, and smart grids may be more affected by data integrity issues due to the high level of automation. By targeting pricing and operational data used in demand-response programs, a malicious actor could indirectly influence direct load control systems and price-responsible demand systems, causing consumer-side machines to power on and off.[82] For example, manipulating price information to make the electricity rate appear more expensive could cause devices—including air conditioners, water heaters, and other high-energy-use appliances—to turn off while cheap prices could cause

[77] Symantec, "Dragonfly: Western Energy Companies Under Sabotage Threat," http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat, accessed November 27, 2014.
[78] Knapp, Eric, "Applied Cyber Security and the Smart Grid," New York: Syngress, 2013.
[79] Monitor 360 Interview with Smart City Security Expert, July 21, 2014.
[80] University of New Mexico, On the Role of Power-Grid and Communication-System Interdependencies on Cascading Failures, Albuquerque: 2013.
[81] Monitor 360 Interview with Urban Infrastructure Expert, June 30, 2014.
[82] Monitor 360 Interview with Smart Grid Expert, October 31, 2014.

them to turn on. If prices were set low enough to cause a large number of machines to turn on simultaneously, the resulting surge in demand could strain the system or cause outages. By rapidly fluctuating prices between extreme highs and lows, it would be possible to cause some machines to repeatedly power off and on, stressing equipment, disrupting load-balancing capability, or potentially causing outages. Although altering data at the substation level would likely only impact a smaller group of machines, targeting data before it was sent to various substations could impact a greater number of networked devices.

- Before pricing information reaches individual customers, it travels through a variety of communication networks, often including the Internet, cloud storage, and commercial systems.[83] Many demand-response programs follow an industry standard of using Open Automated Demand-Response, which relies on Internet communication and, thus, is vulnerable to certain types of attacks.[84] These communication nodes are harder to monitor and secure, and the connection points between these nodes and smart grid networks offer a potential access point for a malicious actor. Further, many utilities employ third-party vendors to calculate and disseminate pricing data, giving utilities less security oversight.[85]
- The level of controllability involved in demand-response, and to a lesser extent direct load control, systems could allow a malicious actor to do a significant amount of damage through a single attack before fabricated data could be detected and removed. Although successfully intercepting and manipulating pricing information would likely be a complex process, it would be far easier for an insider to make the changes necessary to manipulate a demand-response system.[86]

As use of smart distribution and transmission technology continues to grow, a rising number of appliances will be connected to demand-response systems, increasing the potential impact of an attack. Depending on the capability of a malicious actor and the sophistication of an attack, the manipulation of energy-pricing data could affect millions of appliances and entire regions of the United States.[87]

SMART DISTRIBUTION AND TRANSMISSION TECHNOLOGY-SPECIFIC OBSERVATIONS

Changing Seams

- Widespread implementation of smart distribution and transmission infrastructure will facilitate an increase in demand-response programs. As these programs become ubiquitous and more sophisticated, so will the information available to malicious actors seeking to maximize negative consequences. For example, increased energy prices could signal low energy supply or systemic strain—potentially valuable information for a malicious actor looking to maximize harm to a Smart City's electricity grid.

Inconsistent Adoption

- As demand-response programs gain in prominence, utility companies will have numerous options for collecting information (e.g., for electricity price and available data). Diversity in demand-response programs will increase vulnerabilities to consumer data being compromised or to privacy violations, as different information aggregators will use different communication and security standards.
- Utility security administrators may devote the most attention to smart distribution and transmission components that heavily use SCADA systems and other controllable devices, as administrators may perceive these assets as most vulnerable to attack. Devices other than SCADA systems and with less controllability, may receive less scrutiny, however, allowing exposed vulnerabilities in the devices to linger and be exploited.

---

[83] Monitor 360 Interview with Smart Grid Analyst, November 3, 2014.
[84] California State University Sacramento, Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks, Sacramento: California Energy Commission, May 2012.
[85] "Here's a Great Way to Use Big Data for Auto-DR," http://www.smartgridnews.com/artman/publish/Technologies_Demand_Response/Here-s-a-great-way-to-use-Big-Data---for-auto-DR-5911.html#.VIH85_TF8dQ, accessed December 6, 2014; Knapp, Eric, "Applied Cyber Security and the Smart Grid." New York: Syngress, 2013.
[86] Monitor 360 Interview with Smart Grid Expert, October 31, 2014; Knapp, Eric, "Applied Cyber Security and the Smart Grid." New York: Syngress, 2013.
[87] Monitor 360 Interview with Energy System Engineer, November 3, 2014.

Increased Automation

- The combination of controllability and the integration of programs involving third-party vendors (e.g., demand-response programs) leaves proper system function dependent on data integrity (e.g., pricing data). Vulnerabilities within these third-party programs can have a disproportionate impact on the functionality of the system as a whole.

ADVANCED METERING INFRASTRUCTURE

Advanced Metering Infrastructure (AMI) is a system designed to bring new transparency and efficiency to energy consumption in smart grids. Smart meters—part of the AMI—measure, store, and transmit energy usage data and voltage data for residences and commercial buildings within a smart grid. Unlike traditional energy meters, some smart meters within AMI systems employ two-way communication technology, often using wireless connections to send and receive data from utilities and system operators. Dispatch and management centers can also physically control the meters, with the ability to connect or disconnect power remotely.

In addition to smart meters, AMI consists of a server to gather, store, and disseminate smart meter data and a communication system to connect the various components. These in-home smart meter connected appliances help to facilitate demand response programs and other dynamic energy-consumption programs. The majority of these in-home devices utilize a cloud infrastructure for connecting the appliance to the meters.[88] By incorporating new connectivity and networking, as well as increased insight and control over energy-consumption patterns, AMI allows utilities to monitor, track, and influence energy usage across millions of smart meters. Although the data collected by smart meters is invaluable in helping utilities increase efficiency and manage power consumption, it also holds value for individual consumers. Specifically, when utilities share real-time usage information with customers, consumers can make energy-consumption decisions based on pricing and otherwise improve their energy usage. As a result, many utilities will introduce built-in connection points, or customer gateways, that will allow customers to access and review their smart meter information.

Smart meters are already widely utilized by utility companies across the country. A report by Navigant Research estimates there were more than 300 million smart meters deployed globally in 2013, with that number expected to grow to over one billion by 2022.[89]

PATHWAY 3: SMART METER SECURITY IS COMPROMISED

Sample Vector 1: A malicious actor compromises AMI servers, cutting access to power from smart meters and targeted buildings.

Gaining control of an AMI server would give a malicious actor the ability to control all aspects of a local AMI system, such as blocking or manipulating energy-usage data or remotely controlling other functionality features. For example, many smart meters are designed with the ability to cut power remotely to a building in the event that a customer fails to pay a utility bill. A malicious actor with control of an AMI server could remotely disconnect smart meters, cutting off power to targeted buildings or areas. In addition to being able to execute remote attack, an actor could cause physical effects—tripping a building's circuit breaker, for example—that require a manual onsite fix.[90] Alternatively, a malicious actor could control an AMI server to access billing and energy usage information, a privacy concern for electricity customers.

- Many AMI servers use off-the-shelf operating systems and applications, which can lack purpose-built security features and can be straightforward for malicious actors to navigate.[91]

[88] Demand response refers to the ability of consumers to increase or reduce their use of electricity based on power grid needs, price changes, or special retail rates (PJM Staff White Paper, "Price Responsive Demand," http://pjm.com/~/media/documents/reports/pjm-whitepaper-on-price-responsive-demand.ashx, accessed July 9, 2015).
[89] Steitz, Christoph and Harro Ten Wolde, "Smart Technology could make utilizes more vulnerable to hackers," http://www.reuters.com/article/2014/07/15/utilities-cybersecurity-idUSL6N0PM2EC20140715, accessed December 9, 2014.
[90] Monitor 360 Interview with Smart Grid Security Expert, August 4, 2014.
[91] Balakrishnan, Meera, "Security in Smart Meters," http://cache.freescale.com/files/industrial/doc/white_paper/SECSMTMTRWP.pdf, accessed December 8, 2014.

- Causing a power outage through attacks on smart generation or distribution and transmission systems requires a series of steps, whereas smart meters present a direct path to power loss. The meters contain purpose-built elements designed to cut power to a building.
- AMI servers maintain direct links to multiple system components, including smart meters. A malicious actor able to compromise an AMI server would also gain access to, and potential control over, a range of connected devices.

In 2009, security research firm IOActive demonstrated the ability to install malware onto a commonly used smart meter. Simulations run by the firm further demonstrated how easily they could then spread the malware through AMI servers across millions of other smart meters, allowing them to remotely cut power to associated buildings. Although this particular attack preyed upon a hardware design flaw, the ease and impact of the attack demonstrates the possibility of a large-scale attack.[92]

The impact of AMI disruptions on public safety and security depends on the target and scale of the attack. By targeting multiple, widely used AMI servers, a malicious actor could potentially trigger switches on millions of smart meters, effectively cutting power to millions of homes and businesses. At a minimum, the magnitude of such power loss would cause confusion and damage businesses and services in the affected area. If focused on a commercial or business district, the cost of such an attack could be significant to local businesses and economies. If this attack were to occur on a particularly hot or cold day, it could have public health effects. Alternatively, a malicious actor could target specific facilities—such as hospitals, airports, police stations, banks, or transportation hubs—to shut down vital services and limit the ability of emergency personnel to respond to other public safety incidents.[93]

Sample Vector 2: A malicious actor manipulates smart meters to alter usage information, gain access to in-home devices, or cut power to consumers.

Access to and control of individual smart meters could allow a malicious actor to tamper with and alter the integrity of energy-use information flowing back to AMI servers and utility control centers. This type of attack could effectively allow a malicious actor to underreport or over-report consumer-energy use.[95] Similarly, smart meters could be manipulated to provide access to in-home devices, giving the malicious actor information about consumers' whereabouts (e.g., low-level energy use could be an indicator that a user is not home), habits, or personal and financial information—compromising consumer privacy, safety, and security. An alternative to remotely accessing an installed smart meter is targeting the meters during the manufacturing process. This strategy would compromise smart meters from the moment they are installed, removing the need to hack into the system.[96] For example, an actor could design a microcontroller—a small computing device—that allows the meter to function normally while also introducing security flaws. Smart meter manufacturers receiving these faulty microcontrollers could potentially install them into their products with no knowledge of the flaws.[97]

In 2009, the FBI uncovered widespread fraud in a Puerto Rican utility that used smart meter hacks to underreport energy use. The FBI assessed that utility employees offered to alter customers' energy meters for a fee. Meter tampering, thought to have involved 10 percent of system smart meters, cost the utility over $400 million.[94]

- The high degree of interconnectivity that smart meters allow amplifies the impact of an attack on even a single meter. Because smart meters share common network connections, malware could be designed to spread throughout a system, potentially removing all infected devices from the power grid.
- Alternatively, a malicious actor could use wireless communication systems to access smart meters. Unlike AMI servers, which are generally connected to individual consumers, malware introduced into a smart

[92] Naone, Erica, "Meters for the Smart Grid," http://www.technologyreview.com/hack/414820/meters-for-the-smart-grid/, accessed December 5, 2014.
[93] Monitor 360 Interview with Smart City Scholar, July 2, 2014.
[94] Krebs, Brian, "FBI: Smart Meter Hacks Likely to Spread," http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/, accessed November 20, 2014.
[95] bid.
[96] Monitor 360 Interview with Smart Grid Security Expert, August 4, 2014.
[97] Ardis, Kris, "7 Serious Smart Meter Security Threats that do Not Involve Hacking the Network." http://www.smartgridnews.com/artman/publish/Technologies_Metering/7-serious-smart-meter-security-threats-that-do-NOT-involve-hacking-the-network-6664.html#.VIH0v_TF8dQ, accessed December 5, 2014.

meter could spread throughout and beyond individual AMI server hubs, increasing the potential impact of a single smart meter-based attack.

- Smart meter vulnerabilities are also exacerbated by the heavy use of standard Wi-Fi technology for network communication, introducing associated security challenges.[98]

As with attacks on AMI servers, the impact of AMI disruptions on public safety and security depends on the target and scale of the attack. A small, targeted attack could have significant local and regional impacts, while the ability to cut power from millions of homes and businesses may affect a larger number of people, although the impacts may be less significant. The sudden removal of a large number of customers would likely hamper a utility's load-management capacity.[99] From an economic perspective, the ability to underreport energy usage could also lead to financial losses for utility companies. Underreporting energy usage could help disguise dangerous or illegal activity.[100] Lastly, as smart meters will be highly visible physical devices located on nearly every home, they may become a technology that people associate as being representative of all Smart City technologies. A widespread security breach involving smart meters could deal a blow to public confidence to all Smart City technology, technologies of which many people are already suspicious.[101]

ADVANCED METERING INFRASTRUCTURE TECHNOLOGY-SPECIFIC OBSERVATIONS

Changing Seams

- As AMI proliferates, it will introduce tens of millions of visible smart meters into electricity grids, creating an equal number of potential physical and remote access points into the overall system. These numbers make it nearly impossible to secure each device physically from a logistical perspective, increasing the level of vulnerabilities to the types of exploits described above.

Inconsistent Adoption

- Small but persistent groups of energy customers may resist smart meter adoption (e.g., because of concerns regarding privacy and the general controllability implications of smart meters). As people living in Smart Cities opt-out of smart meters, they could create pockets of homes relying on legacy analog meters. The resulting lack of interoperability across a city's smart meters could create system blind spots that also prompt diverting resources towards laborious maintenance of legacy meters and away from smart meter security.
- Although smart meters require a degree of interoperability, cybersecurity experts believe there may be ways to mimic diversity—often called "artificial software diversity"—in smart meters, thereby reducing the risk of widely exploitable vulnerabilities. However, the large number of smart meters that will be deployed in Smart Cities will likely make upgrading or replacing smart meter networks a labor-intensive and expensive task, outpacing the normal cost-of-doing-business capability of many resource-strapped utilities.

Increased Automation

- Smart meters are designed to communicate with control servers, each other, and customers. As smart meters become widespread over the next decade, successful communication will require a high degree of interoperability, increasing the risk of malware spreading between devices and increasing overall system vulnerability.
- Controllability of smart meters and the in-home devices to which they connect leaves consumer personal data (e.g., data regarding behaviors or personal information) vulnerable to exploitation by malicious actors, raising privacy concerns for utilities that are responsible for protecting the information.

[98] "Hacking the Smart Grid." http://www.technologyreview.com/news/418320/hacking-the-smart-grid/, accessed December 5, 2014.
[99] Monitor 360 Interview with Smart Grid Security Expert, August 4, 2014.
[100] Monitor 360 Interview with Urban Futurist, June 28, 2014.
[101] Monitor 360 Interview with Smart Grid Security Expert, August 4, 2014.

WATER AND WASTEWATER SYSTEMS IN SMART CITIES

This section focuses on the future dynamics of cyber-physical infrastructure in Smart Cities within the Water and Wastewater Systems Sector, as part of a broader series of sector-level inquiries emphasizing security and resilience. In addition to the general security risks inherent in water networks, Smart City water systems bring a unique set of security challenges, including the:

- Complexity of securing a cyber-physical system that transports and manages a physical substance.
- Difficulty of securing cyber-physical technology onto existing physical infrastructure that is oftentimes approaching its life expectancy or near-failure.[102]
- Complexity of ensuring smooth interface, communication, and security among multiple interdependent systems, including sensors, pumps, valves, control systems, treatment facilities, distribution pipes, ventilation systems, drainage systems, etc.
- Isolated or hard-to-access locations of certain water infrastructure, such as underground pipes or rural reservoirs, which increase upgrade costs, maintenance costs, and reliance on networked monitors.

Three cyber-physical technologies that will be part of future Smart City Water and Wastewater Systems are smart water treatment, smart water distribution, and smart water storage.

SMART WATER TREATMENT

Smart water treatment incorporates cyber-physical technology into three distinct processes: water reservoirs, water treatment, and water distribution. Smart wastewater treatment also incorporates three distinct cyber-physical technologies: wastewater collection, wastewater transmission, and wastewater treatment processes. Although functionality between data acquisition and actual control is different, the two processes involve similar applications of technology. In both cases, sensors and meters gather data, two-way connectivity and communication networks carry data from devices to central control systems, and networked programmable logic controllers and SCADA devices automate system adjustments.

Smart water treatment allows for increased automation in process control.[103] Networked sensors and increased automation of water treatment will increase the efficiency of reservoir management, water treatment, and water storage and transmission, allowing increased efficiency from a system management perspective in ways that save time and material. Implementing networked monitors on system components will allow smart treatment plant administrators to anticipate equipment failures and system errors, and otherwise improve maintenance and reliability.[104]

Likewise, smart wastewater systems allow for real-time monitoring and adjustments of collection systems, pumping stations, and chemical balance and treatment conditions throughout the wastewater treatment process. For example, cyber-physical technology could greatly increase the viability of rotating biological contactors, which use bacteria to break down toxic organic matter. To function, rotating biological contactors must maintain a complex system of live bacteria, which only thrive under certain environmental conditions. By networking and automating sensors, temperature controls, oxygen blowers, and other atmospheric devices, the proper atmospheric conditions are maintained to ensure rotating biological contactors system health. Similarly, smart wastewater treatment plants can also anticipate and minimize equipment breakdown and system errors, helping to increase overall efficiency. According to Hitachi, smart water treatment systems integrate automation and networking technologies that can increase efficiency by constantly monitoring treatment processes and making adjustments in real time.[105]

---

[102] "Aging Water Infrastructure Research," nepis.epa.gov/adobe/pdf/P100EQ6Q.pdf, accessed December 8, 2014; "2014 Black and Veatch Strategic Directions U.S. Water Industry Report," bv.com/reports/SDR-WaterUtility-DL, accessed December 8, 2014.
[103] Monitor 360 Interview with Water Administrator, July 23, 2014.
[104] Ibid.
[105] "Intelligent Water System for Realizing a Smart City," http://www.hitachi.com/products/smartcity/smart-infrastructure/water/solution.html#plink04, accessed December 3, 2014.

The amount of automation used in water and wastewater utilities is increasing, and a significant percentage of water utility companies recognize the value of smart water treatment; according to a survey sponsored by Badger Meter, a smart water metering company, "nine out of ten water utilities have a smart water plan."[106] However, a variety of concerns—including apprehension over cost and security, and a lack of awareness of many developing technologies—have impeded wider adoption of smart water treatment.[107] Experts interviewed for this study expect increased government funding and growing awareness of limited water resources may drive more rapid adoption of smart water-treatment technology over the next five years.[108]

PATHWAY 1: SMART WATER-TREATMENT FACILITY DISRUPTION

Sample Vector 1: A malicious actor conducts a cyber-attack on a smart water treatment facility to prevent proper functionality, endangering the systems and public health.

A disgruntled worker in Queensland, Australia, used insider knowledge to access a wastewater treatment plant's systems 46 times over a 4-month period in 2000. The employee used SCADA access to spill over 200,000 gallons of sewage into parks, rivers, and hotel grounds even though the facility was not highly networked or automated.[109]

As control of water treatment plants becomes increasingly automated, electronic or SCADA system components could become more vulnerable to remotely executed attacks. After gaining remote access to a smart water treatment facility, a malicious actor could control system devices and data sensors. For example, an attack on SCADA systems could damage or destroy critical system components—i.e., forcing pumps to stop—potentially rendering a smart treatment plant non-operational.[110] In another example, an actor could manipulate chemical feed pumps, introducing inappropriate levels thereby disrupting proper chemical feed.[111] An attack could be executed subtly, spoofing system sensors to report false readings that would allow dangerous conditions to remain unnoticed temporarily by operators and administrators, or an attack could be done on a larger scale, rendering water supplies untreatable, wasting water resources, and straining a city's water supply. At the same time, water treatment staff could take physical water samples—independent of the control system—to identify water quality issues missed or masked in the control system.

- The desire for increased transparency, information sharing, and remote connectivity leads many utilities to create Web portals, increasing the potential use of unsecured Internet connections and other vulnerable communication methods.[112]
- The consolidation of monitoring and device control systems in smart water treatment plants increases the chance of an insider threat attack, as a disgruntled worker could potentially execute a comprehensive attack from a single access point.
- Efficiency gains and increased automation will raise incentives for smart water treatment plants to maintain smaller staffs, decreasing human oversight and promoting reliance on the proper function of smart systems.[113]
- Finally, the implementation of cyber-physical and networked components can be expensive and may take extended periods of time to provide a return on investment.[114] This may cause some utility administrators, particularly those with limited budgets, to only upgrade certain components or to neglect subsequent security patches or needed modifications.[115]

---

[106] A 2014 survey found that 9 out of 10 utilities had a smart water treatment plan. See: "U.S. Smart Water Utility Report 2014," http://smartgridinsights.com/standard/u-s-smart-water-utility-report-2014/, accessed November 20, 2014.
[107] "Study says yes, the smart water market will (finally) grow," http://www.smartgridnews.com/artman/publish/Technologies_Smart_Water/Study-says-yes-the-smart-water-market-will-finally-grow-6850.html#.VIYIVfTF9LQ, accessed December 8, 2014.
[108] Monitor 360 Interview with Water Resource Scientist, December 4, 2014.
[109] Abrams, Marshall, "Malicious Control System Cyber Security Attack Case Study-Maroochy Water Services, Australia," http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf, accessed November 16, 2014.
[110] Monitor 360 Interview with Urban Infrastructure Expert, June 30, 2014; Monitor 360 Interview with Water Engineer, August 4, 2014.
[111] Monitor 360 Interview with Smart City Water Expert, July 22, 2014.
[112] Liebelson, Dana, "Bad News: Hackers are Coming for your Tap Water," http://www.motherjones.com/politics/2013/08/chinese-hackers-attack-trend-micro-honeypots, accessed December 3, 2014.
[113] Monitor 360 Interview with Smart City Security Expert, 21 July 2014, and Monitor 360 Interview with Smart City Scholar, July 2, 2014.
[114] Monitor 360 Interview with Water Resource Scientist, December 4, 2014.
[115] Abrams, Marshall, "Malicious Control System Cyber Security Attack Case Study-Maroochy Water Services, Australia," http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf, accessed November 16, 2014.

Sample Vector 2: A malicious actor gains remote access to a smart wastewater facility to cause water system backups and potential environmental damage.

A malicious actor with remote access could hinder the treatment process, creating a backup in a Smart City's wastewater system. For example, access to rotating biological contactor controls could be used to adjust temperature settings or to manipulate oxygen blowers in bioreactors, causing bacteria to die or to grow too rapidly, degrading the conditions needed to properly digest wastewater toxins.[117] Such consequences would prevent the proper treatment of wastewater and could effectively shut down a smart treatment plant. Alternatively, a malicious actor could manipulate sensors to hide the presence of remaining toxic substances, triggering the release of only partially treated wastewater. This shift could disrupt subsequent treatment processes or release unsafe water into the system. A malicious actor with a greater degree of system control could flush water in a smart wastewater treatment plant prior to the completion of the treatment process, affecting residents, businesses, and the environment surrounding the facility.[118]

In 2013, a wastewater treatment plant in Hull, Massachusetts, was shut down after a high volume of incoming wastewater overwhelmed pumps. With few other options, utility engineers pumped over 10 million gallons of untreated sewage directly into the Atlantic Ocean until the plant was repaired.[116]

- Because of the complexity of bacterial environments in rotating biological contactors—and in similar treatment technologies—replacing or restoring a damaged treatment ecosystem is a potentially time-consuming process.[119] As a result, a breach that disrupted a bacterial community could effectively take the bioreactor offline for an extended period of time.
- As smart wastewater technology becomes more pervasive, a growing number of cities will rely on wastewater treatment plants designed around—and dependent on—cyber-physical and networked technology. Thus, an attack on a single wastewater treatment facility could have a disproportionate impact on receiving waters, as the targeted facilities may not be able to operate as efficiently in a manual mode.[120] The impact of this attack would have the greatest impact in cities that maintain only a small number of smart wastewater facilities.[121]

Compromised wastewater treatment facilities could create public health crises and damage the environment in affected Smart Cities. Disrupting a Smart City's ability to treat wastewater could cause system backups and push wastewater and untreated sewage into public areas. In a worst-case scenario, sewage could backup through household drains or into low-lying streets, posing a significant public health risk. Although it is unlikely that a smart wastewater treatment shutdown would damage drinking water—as water treatment generally occurs through an independent process—untreated sewage in public areas could expose a targeted population to potential dangerous pathogens.[122] Untreated sewage may be expelled into the environment while treatment facilities are repaired to mitigate sewer backups and avoid greater risks to public health.[123] In addition to environmental damage, untreated wastewater could potentially affect local water supplies while damaging local businesses and the regional economy.

[116] Dezenski, Lauren, "Shutdown Persists at Hull Wastewater Plant; Sewage Pours into Atlantic for Second Day," http://www.boston.com/metrodesk/2013/03/01/shutdown-persists-hull-wastewater-plant-sewage-pours-into-atlantic-for-second-day/Y74Mzjuc2WifyKTBMsRlUL/story.html, accessed November 20, 2014;
"Wastewater treatment plant back online, stopping flow of raw sewage," http://www.watertechonline.com/articles/166185-wastewater-treatment-plant-back-online-stopping-flow-of-raw-sewage, accessed November 20, 2014.
[117] Monitor 360 Interview with Water Resource Scientist, August 1, 2014.
[118] Ibid.
[119] Monitor 360 Interview with Water Resource Scientist, December 4, 2014.
[120] Monitor 360 Interview with Water Resource Scientist, August 1, 2014.
[121] "The Deer Island Sewage Treatment Plant," http://www.mwra.com/03sewer/html/sewditp.htm, accessed December 4, 2014.
[122] Monitor 360 Interview with Smart City Water Expert, July 22, 2014.
[123] Dezenski, Lauren, "Shutdown Persists at Hull Wastewater Plant; Sewage Pours into Atlantic for Second Day," http://www.boston.com/metrodesk/2013/03/01/shutdown-persists-hull-wastewater-plant-sewage-pours-into-atlantic-for-second-day/Y74Mzjuc2WifyKTBMsRlUL/story.html, accessed November 20, 2014.

SMART WATER TREATMENT TECHNOLOGY-SPECIFIC OBSERVATIONS

Changing Seams

- The introduction of remote controllability in smart water and wastewater treatment plants will allow smaller staffs to monitor and operate plant functionalities from onsite and offsite locations, making it more difficult to profile and identify the source of an attack or failure. For example, system access originating from foreign countries may no longer be a warning sign, as authorized users could theoretically log in from anywhere.

Inconsistent Adoption

- Successful operation of smart water and wastewater treatment plants, particularly during initial rollout phases, will likely involve a variety of hardware and software vendors, as well as potential for multiple third parties involved in installation, maintenance, or operation—all requiring system access. Without clear, consistently up-to-date security requirements for third-party vendors, particularly those with remote access, this growth in third-party vendors could increase the attack surface and potential unauthorized system infiltrations.
- The advent of smart treatment plants is facilitating innovation in water and wastewater treatment that can only work with modern cyber-physical systems, increasing overall system vulnerability. For example, wastewater bioreactors would likely be prohibitively expensive and complex to operate without networked cyber-physical technology. Without incentives or resources to create manual backups, any system errors or attacks could leave wastewater systems particularly vulnerable.

Increased Automation

- As cyber-physical and networked components in water and wastewater treatment plants become increasingly pervasive, operation will require fewer personnel. In addition, the implementation of digital high-tech technology will require new skills and backgrounds that many existing staff will not possess. Some existing staff may need to be replaced with technologically proficient staff that may not have a comprehensive understanding of legacy systems.
- As water and wastewater treatment components become networked and automated, an increasing number of programmable logic controllers, actuators, monitors, sensors, and other devices will be controllable through a central command system. Although largely unavoidable, this centralization of control increases overall system vulnerability, as a single weak point feeding to central control could expose the entire system to attack.

SMART WATER DISTRIBUTION

Smart water distribution systems replace or augment existing infrastructure management with networked and automated technologies. Smart valves and smart pumps are able to adjust to their environment, automatically changing speeds and pressure levels as well as redirecting and diverting water as needed.[124] These devices can wirelessly communicate with each other and with a central control system, allowing administrators to maintain system awareness, monitor automatic system functionality, and remotely access and control distribution devices. Further, a network of sensors and monitors is able to gather data on system performance and water quality, alert administrators of abnormalities, and better anticipate equipment failures before they happen.[125,126] Smart water distribution technology stands to improve the delivery and movement of water in a Smart City by tracking water flows to identify leaks and pipe breakages.[127]

According to the Center for Neighborhood Technology—an organization that works with cities to advance urban sustainability—an increasing number of cities are motivated by economic and efficiency gains, and are implementing

[124] Mutchek, Michele and Eric Williams, "Moving Towards Sustainable and Resilient Smart Water Grids," Challenges, 2014.
[125] Ibid.
[126] Monitor 360 Interview with Water Smart Grid Engineer, July 28, 2014.
[127] Hodson, Hal, "Smart Sensors Warn Instantly of Citywide Water Leaks," http://www.newscientist.com/article/mg22429942.700-smart-sensors-warn-instantly-of-citywide-water-leaks.html#.VHoThvTF9LQ, accessed December 3, 2014.

smart water distribution systems.[128] Although cost and interoperability concerns can slow such implementation, several cities are engaging in smart water distribution pilot programs, and industry experts expect implementation to continue growing over the next 5 years.[129]

PATHWAY 2: SMART DISTRIBUTION SYSTEM DISRUPTION

Sample Vector 1: A malicious actor remotely attacks smart water distribution systems to damage system components, disable system sensors, disrupt storage and flows, or distribute contaminated water.

A malicious actor with access to smart distribution systems could disrupt normal functionality of water distribution systems in several ways. First, by obtaining access to system controls could allow an actor to damage or destroy infrastructure components remotely. Forcing a smart pump to operate in the absence of water could cause substantial damage, potentially destroying critical system components.[131] Second, a malicious actor could disable alarm mechanisms and prevent administrators from recognizing suboptimal conditions. Sensor manipulation could mask the presence of a second attack on smart distribution infrastructure, leaving intentional leaks, breaches, or contamination unnoticed.[132] A malicious actor could introduce a hazardous substance into drinking water and delay its detection by forcing sensors to provide false signals.[133] Although a malicious actor would need to inject a varying amounts of the substance—depending on the type of substance—into the system for it to have a widespread effect, the impact to consumers in a local area could be deadly.[134]

In 1997, a local water distribution system in Charlotte became dangerously contaminated when fire fighters conducting a safety exercise accidently pumped toxic fire retardant into a fire hydrant. Not realizing that their hose was still connected to the hydrant and that the hydrant was open, the pressure from the retardant pump overcame the pressure in the water main, causing a backflow into the local water supply. Despite immediately realizing the mistake and taking corrective action, only 60 gallons of the chemical was enough to put hundreds of customers at risk, prompting city staff to flush the entire system.[130]

- Many cities rely on decades-old water distribution infrastructure, including some pipelines that are more than 100 years old, and the cities have little incentive to upgrade devices that are expensive to replace and continue to operate satisfactorily. Because these systems are not designed for remote controllability and integration into broader networks, ensuring security and interoperability as smart technologies are integrated will be a challenge.[135]
- Many utilities rely on mobile broadband, wireless broadband, and satellite communication for data distribution. These technologies introduce a large attack surface and can also lead to increased security vulnerabilities often resulting from substandard security protocols, the sharing of widely used communication nodes, and the use of off-the-shelf technology platforms.[136]
- Installing remote sensors will likely decrease the need for manual monitoring of hard-to-reach, underground water distribution systems.[137] Although more convenient and cost effective for utilities, the remote sensors also increase reliance on a functioning system of networked technologies.
- Potential malicious actors will be able to use their own homes as an attack vector, presenting a security challenge to water utility administrators. Many components within a smart water distribution system are

[128] "The Case for Fixing the Leaks," http://www.cnt.org/media/CNT_CaseforFixingtheLeaks.pdf accessed December 3, 2014; Monitor 360 Interview with Water Administrator, July 23, 2014.
[129] "Indianapolis 'smart water grid' pilot project demonstrates local solution to national sustainable infrastructure problem," http://www.gwtr.com/2013_RWELLS_plan.pdf, accessed December 8, 2014; Monitor 360 Interview with Smart City Water Expert, July 22, 2014.
[130] "Chemical Leak Taints Water," The Charlotte Observer, September 3, 1997.
[131] Monitor 360 Interview with Water Engineer, August 4, 2014.
[132] Monitor 360 Interview with Water Resource Scientist, August 1, 2014.
[133] Monitor 360 Interview with Smart City Water Expert, July 22, 2014.
[134] Ibid.
[135] Monitor 360 Interview with a Cyber-Physical Security Expert, 24 July, 2014.
[136] McNabb, John, "Vulnerabilities of Wireless Water Meter Networks," http://www.southshorepcservices.com/McNabb%20-%20BH-WP-%20Vulnerabilities%20of%20Wireless%20Water%20Meter%20Networks.pdf, accessed November 20, 2014.
[137] Monitor 360 Interview with Urban Infrastructure Expert, June 30, 2014.

vulnerable to physical attack, but most are not within the physical control of a utility company, and remote components are more difficult to secure.

Attacks on smart water distribution systems could have regional public safety consequences if they cut off sections of a Smart City from access to potable water. The same consequences could happen if contaminated water is delivered to a large number of consumers, which could occur by targeting critical components higher up in the distribution system. Even if consumers or a utility were to detect foreign substances in drinking water quickly, it is possible that some amount of contaminated water would be consumed with potentially deadly effects. Combining this type of attack with manipulation of safety and quality sensors could likely further increase illness and loss of life.

Damaged or ruptured pipes also pose a danger because of leaked substances, which can cause sinkholes and infrastructure damage. Leaked wastewater can cause buildup of toxic chemicals, causing illness or potential explosions.[138] Finally, attacks on smart distribution infrastructure would also create significant repair costs for utilities (e.g., potential drinking bans on tap water, furnishing of alternative water sources for affected citizens, a complete flushing of smart distribution systems, and a security audit to detect the source of the attack).[139]

Sample Vector 2: A malicious actor disrupts storm water-management systems during severe weather to create unsafe conditions, strain storm water-management systems, and compound the consequences of inclement weather.

In September 2009, heavy rains overwhelmed the storm water-management capacity in Atlanta and other nearby towns, killing at least 10 people and inflicting over $500 million in damage. At least 20,000 homes and businesses were damaged in the resulting floods.[140]

Advances in water system efficiency and automation will increase Smart Cities' reliance on smart distribution technology to manage adverse weather events, which will also introduce new vulnerabilities into storm water-management capabilities. A malicious actor with remote access could target either the data informing storm water-management components or components themselves, including smart pumps and smart valves. A malicious actor could block or alter critical information, including real-time weather updates traveling to control centers or block and alter pumping capacity and performance updates from smart components in critical areas. During a weather incident, data blocking could hamper an administrator's or an automated control system's decision-making ability and potentially aggravate the impact of adverse weather on a Smart City's water system.[141] Similarly, a malicious actor could remotely close valves or deactivate pumps, preventing the pumping or transportation of excess storm water away from hard-hit or at-risk areas. Smart pumps could also be manipulated to reroute water already in the system towards hard-hit areas, increasing the strain on targeted areas and thwarting storm-management efforts.

- Anticipating and calculating optimal conditions for upcoming weather incidents requires internal and external data inputs. The corruption of any one data input could have significant consequences, as an incomplete picture of an operating environment could greatly decrease efficiency.[142] External data sources may be less secure and are likely harder to monitor than internal data inputs.[143]
- As storm water-management systems are typically only used during severe weather incidents, they are less likely to receive regular updates and security reviews during periods of disuse. A malicious actor could conceivably introduce malware into a storm water-management system that would not be discovered until a storm occurred, the system activated, and the malware executed an attack. If attacks go unnoticed before a severe weather event, the resulting dangerous and difficult weather conditions complicate matters for water utility technicians trying to repair any damaged physical infrastructure.

Attacks on storm water-management systems could have regional impacts if they resulted in extensive urban flooding during natural disasters. Sewer overflows and floods would pose an immediate contamination threat to

[138] Monitor 360 Interview with Water Administrator, July 23, 2014.
[139] States, Stanley, Security and Emergency Planning for Water and Wastewater Utilities, American Water Works Association, 2009.
[140] Ready Georgia, "Georgia Disaster Facts 2014," http://ready.ga.gov/news/, accessed November 12, 2014.
[141] Monitor 360 Interview with Water Resource Scientist, December 4, 2014.
[142] Monitor 360 Interview with Water Smart Grid Engineer, July 28, 2014.
[143] McNabb, John, "Vulnerabilities of Wireless Water Meter Networks," http://www.southshorepcservices.com/McNabb%20-%20BH-WP-%20Vulnerabilities%20of%20Wireless%20Water%20Meter%20Networks.pdf, accessed November 20, 2014.

drinking water and food that comes into contact with floodwater, as well as the potential for an increase in disease transmission. Attacks on storm-management systems during severe weather could overwhelm specific critical infrastructure. For example, inducing flooding around levies in low-lying cities or over primary transportation routes could significantly increase the danger to residents in the area, preventing emergency personnel from accessing affected areas and increasing the likelihood of dangerous sinkholes and failing infrastructure. Extended flooding could also cause extensive economic costs to affected areas, potentially damaging transportation infrastructure, energy infrastructure, and public and private property.

SMART WATER DISTRIBUTION TECHNOLOGY-SPECIFIC OBSERVATIONS

Changing Seams

- Pervasiveness of smart distribution and storm water-management systems will require the installation of networked sensors and other components throughout a water system. Many of these components will be hard to secure, as they will be located in remote and hard-to-access areas (e.g., rural areas where water originates before reaching a city or underground distribution systems within a city).
- Interoperability will be necessary for Smart Cities sharing the same water source—specifically, to facilitate communication and efficiency between upstream reservoirs, watersheds, and the downstream systems receiving water supplies within cities—creating potential security vulnerabilities in the "seams" between cities at different stages of Smart City development.
- Since several Smart Cities may share a single water source, vulnerabilities in one city's water-distribution system could impact other cities sharing the same source. For example, a malicious actor with access to a distribution system in a city with weaker security processes could potentially target components further up the water delivery and distribution process, damaging or destroying pumps needed to bring water from a reservoir to several cities. The inability to mitigate problems quickly when they originate in other cities could also be complicated by the use of third-party vendors, who may be slower to recognize and respond to cybersecurity breaches.[144]

Inconsistent Adoption

- The long lifespan of water distribution and storm-management components means that Smart Cities contain diverse legacy infrastructure—in terms of age and technology—that are physically dispersed and oftentimes hard to access (e.g., underground pipes). It is particularly challenging to update these systems in a consistent, comprehensive way and to design security and operational protocols for new cyber-physical components.

Increased Automation

- Even after smart storm water-management systems become pervasive, they will generally only be accessed during or immediately after periods of heavy use (e.g., after heavy rainfall or flooding). Lighter use and scrutiny during normal operating conditions may leave these systems more vulnerable to security breaches, with any tampering going undiscovered until inclement weather necessitates heavier system use.
- The automation of smart distribution systems will lead to an increasing reliance on remote sensors and actuators to monitor and adjust system performance. The resulting decrease of onsite human verification will make it more difficult to identify the occurrence of attacks that are not immediately recognizable, particularly in hard-to-access areas.
- Automation combined with the need for physical transportation of water makes it particularly challenging to mitigate the consequences of an attack on, or failure of, smart distribution systems. Although the attack or failure could occur in an automated component of the system, effects such as pipe ruptures or loss of water require physical labor to be fully addressed.

[144] "2014 Trustwave Global Security Report," https://www2.trustwave.com/rs/trustwave/images/2014_Trustwave_Global_Security_Report.pdf, accessed December 9, 2014.

- Remote controllability increases the vulnerability of hard-to-secure physical system access points. Whereas these physical access points have historically not been networked with the larger water system—e.g., fire hydrants and drains in residences and private buildings—the ability to manipulate local pumps magnifies the potential impact of either a cyber or physical attack.

SMART WATER STORAGE

Smart water storage encompasses a series of automation and networking technologies that are integrated into reservoirs, water towers, and other storage facilities, as well as the distribution systems linking those facilities to other water systems. To meet changing demand, SCADA systems and industrial control systems can effectively manage demand and flow of water. The systems also monitor inflow to reservoirs to prevent overflows and can block contaminated or unsafe water from entering water supplies. Networked sensors provide the real-time data to control these operations, constantly gauging levels; tracking water usage; and measuring quality as water enters, remains in, and exits water storage facilities. A series of networked sensors allow water system operators to remotely access real-time information on system performance, water quality, and the presence of foreign or hazardous substances.[145] Many, if not most, water utilities currently practice continuous automated monitoring of storage reservoirs to some degree.

PATHWAY 3: INFILTRATION OF A SMART WATER-STORAGE FACILITY

Sample Vector 1: A malicious actor targets smart pumps, valves, and other components in smart water-storage facility control systems to manipulate water flow.

The combination of automation and SCADA systems in smart water-storage facilities will give anyone with system control a degree of influence over water resources. A malicious actor could remotely control components of smart water-storage systems to drain water stored. By targeting a smart reservoir, an actor could activate release valves, or gates in the dam on much larger reservoirs, causing downstream flooding. A malicious actor could target a smart hydrotank or ground level storage tank and force pumps to constantly pull water from the storage tank into other parts of the system. Both scenarios could cause system confusion and inefficiencies, require lengthy and costly refill periods, and damage a utility's ability to meet consumption demand.[147]

Over the course of 12 months between 2012 and 2013, hackers from China, Russia, and Germany illegally accessed a decoy water control system set up by American security researchers. Designed to test commonly used security protocols, the fake system suffered at least ten "critical attacks"—i.e., attacks that could have shut down actual water pumps and, in turn, access to drinking water.[146]

Alternatively, an actor could control smart pumps to force water into already full storage facilities, causing overflowing and flooding. Although some storage facilities contain built-in overflow capacity, others located in more urban areas do not, which could result in large amounts of water flowing into highly populated areas (i.e., if water towers with compromised overflow valves continuously released water into urban areas). In elevated storage or ground-level storage facilities without overflow valves, actors could remotely manipulate water pressure, rupturing the towers to drain water and damage the storage facilities themselves.

- Because many smart water-storage facilities use water pressure and gravity to help move water efficiently, control of a single component could allow a malicious actor to flush a facility's water resources remotely. For example, opening one or more release valves could cause a reservoir to lose the majority of its stored water. This relatively straightforward attack strategy could allow someone with only moderate technical sophistication to inflict significant damage to a water system.[148]
- Many cities rely on a limited number of water-storage facilities, increasing system vulnerability to this type of attack. By damaging or draining only a few smart storage facilities, a malicious actor could impact a

[145] Monitor 360 Interview with Water Resource Scientist, December 4, 2014; Monitor 360 Interview with a Cyber-Physical Security Expert, July 24, 2014.
[146] Liebelson, Dana, "Bad News: Hackers are Coming for your Tap Water," http://www.motherjones.com/politics/2013/08/chinese-hackers-attack-trend-micro-honeypots, accessed December 3, 2014.
[147] Monitor 360 Interview with Water Engineer, August 4, 2014.
[148] Monitor 360 Interview with a Smart City Expert, June 25, 2014.

significant percentage of a city's storage capacity. Cities that employ alternative water-storage models—such as New York City, which uses a large number of small storage facilities instead of a small number of large storage facilities—also face unique vulnerabilities. Specifically, utility administrators face logistical challenges in retrofitting and upgrading existing infrastructure to accommodate cyber-physical and networked technology, and in maintaining and monitoring storage facilities in a system.[149] If specific components on a smart water tank are discovered to have design or firmware flaws, manually fixing or replacing thousands of devices across a utility's network could be resource-intensive beyond a water utility's means.

Vulnerabilities in smart water-storage facilities could pose a threat to public safety if they were exploited to drain a city's water resources, create flood conditions, or hinder other critical services. Draining smart reservoirs and water towers, or rupturing smart water-storage tanks, could severely limit a water utility's ability to meet consumption demand for drinking water. Although bottled water and other water sources would help alleviate some losses, the logistical challenge of providing alternative water sources to citizens throughout a large city would likely leave many without access to water. If an attack were conducted during a heat wave or drought across multiple smart water-storage facilities in a Smart City, the result could involve ongoing gaps in water availability. The sudden release of a reservoir's water stores, many of which can hold over a million gallons of water, could create a surge of water, damaging infrastructure and property.[150] Although many reservoirs and water towers are designed with specific overflow and drainage capacity, potentially limiting the volume and severity of resultant flooding, many of these systems are poorly maintained, out of date, and susceptible to failure.[151] An undersupply of water could also hinder other critical infrastructure sectors, such as the Emergency Services Sector, because fire hydrant pressure is lacking and the water needed to generate electricity is unavailable.[152]

Sample Vector 2: A malicious actor manipulates safety sensors to mask the presence of dangerous substances in smart water-storage facilities.

An actor could remotely alter data outgoing from smart water-storage facilities by gaining access to the facility sensors and monitors, either through a central control system or remote access portals. This access could allow an actor to poison a smart water-storage facility and cause sensors to send false signals despite the presence of added toxins.

Conversely, an actor could force sensors to send warning signals despite actual dangerous substances not being present in storage facilities. These actions could trigger automatic safety protocols within storage facilities and elsewhere in the system, including isolating or diverting water or, in rare instances, flushing water. False warning signals could also trigger automatic public service announcements to water consumers, warning them to avoid drinking water in certain areas and causing unnecessary confusion. Further, this type of attack would likely necessitate manual water quality checks by utility engineers—beyond those normally conducted—for all storage facilities sending faulty warning signals. Finally, a malicious actor could stop quality and usage sensors from sending any information, leaving utility administrators blind to real-time safety and operational conditions for as long as it took security personnel to identify and mitigate the attack.

- Although implementing networked sensors and cyber-physical components into water-storage facilities will bring efficiencies, it will also bring certain vulnerabilities. Introducing cyber-physical technologies into water-storage systems will likely decrease human monitoring and increase reliance on new technology to confirm safe water conditions.[153] Any successful attack on cyber-physical and networked technology could limit an administrator's response ability unless well-designed manual overrides and physical response plans were in place (e.g., to recover or repair physical damages or water release that occurs).
- Implementing networked and remotely controllable systems into water-storage facilities could also allow for combined cyber and physical attacks. Although water-storage facilities, particularly reservoirs, have long been vulnerable to contamination attempts and other physical attacks, actors had few feasible options to easily hide their attack or spread the attack to other system components. By introducing a contaminant

[149] Monitor 360 Interview with Smart City Security Expert, July 21, 2014.
[150] "Roadmap to Secure Control Systems in the Water Sector," http://www.awwa.org/portals/0/files/legreg/security/securityroadmap.pdf, accessed November 24, 2014.
[151] Monitor 360 Interview with Water Resource Scientist, December 4, 2014.
[152] Monitor 360 Interview with Smart City Security Expert, July 21, 2014.
[153] Monitor 360 Interview with a Smart City Expert, June 25, 2014.

into a reservoir and then gaining control of water quality sensors, a malicious actor could mask the presence of an attack, increasing the likelihood that contaminated water would have time to spread into the distribution system.

Attacks on smart water-storage sensors could have national or regional-level consequences if they masked the presence of a contaminant long enough for it to reach a large population of consumers. Failure to prevent the delivery of contaminated water to consumers for even a matter of hours could lead to illness and loss of life. Use of a slower acting toxin or less distinguishable substance would also increase the risk to consumers.[154]

SMART WATER STORAGE TECHNOLOGY-SPECIFIC OBSERVATIONS

Inconsistent Adoption

- The nature of vulnerabilities associated with smart water storage will be different for cities based on population size and density (i.e., New York City has a particularly high and dense population). Unlike Smart Cities that maintain a small number of larger water-storage facilities, some high-population cities employ a larger network of smaller tanks located throughout the city (e.g., on top of buildings). Additionally, many of the small tanks on top of buildings are owned by buildings owners and not the city. As hundreds, if not thousands of smaller water-storage tanks are networked, there will be logistical challenges to ensure networking is secure and all systems remain up to date. Security and economic concerns may slow the pace of adoption and lead to uneven deployment of smart water-storage technology, particularly compared to smart treatment and smart distribution systems, which tend to be less regulated than water storage. This dynamic could result in system blind spots and gaps in water utility administrators' ability to manage all aspects of their systems.
- The localized nature and variety of local and State regulations regarding the storage of water will likely lead to a variety of implementation strategies for smart water technology. The resulting diversity in system design will limit the utility of information sharing and collaborative learning, and it may increase vulnerabilities resulting from interoperability challenges.

Increased Automation

- Automation in water-storage facilities will bring with it increased availability of information on water flow, usage patterns, and storage facility maintenance schedules. As the amount of time water is held in a storage facility varies, a malicious actor could use this information to magnify the impact of an attack.

[154] Monitor 360 Interview with Water Administrator, July 23, 2014.

OPPORTUNITIES FOR DHS

The preceding sector-specific sections highlight potential vulnerabilities as cyber-physical or other related technologies become integral parts of the fabric of Smart City infrastructure systems. State and local governments, in partnership with industry, will largely drive the evolution of cyber-physical technologies. There are areas where DHS can contribute to this stakeholder community to aid in anticipating and designing for potential risk and to influence the overall security environment in which these technologies will exist. The following section details opportunities for DHS to assist with mitigating and designing for potential risk associated with cyber-physical technologies.

STANDARDS AND REGULATIONS

As the stakeholder community considers standards and regulation relating to Smart City cyber-physical infrastructure security, DHS could potentially assist in the consideration of specific areas, including:

- **Minimum staff number and qualification thresholds for system operations, security, and maintenance.** Although many cyber-physical technologies will bring new operational and budgetary efficiencies—incentivizing smaller staffs and leaner operations—maintaining focus on adequate numbers of maintenance and operational staff will be crucial to avoid errors and mistakes.
- **Communication standards.** All aspects of cyber-physical infrastructure in Smart Cities will require and use various communication networks and systems. Supporting ongoing efforts to standardize and regulate communication architecture and security guidance will help mitigate vulnerabilities stemming from inconsistent protocols, which may also facilitate the use of local and regional security information and event management monitoring on Smart City networks to identify malicious traffic.
- **Smart City "tiers."** Not all cities will consistently implement cyber-physical infrastructure systems technology because of resource limitations and varying levels of demand. Tiered standards or regulations to manage different cities' implementations appropriately will help anticipate new risks, promulgate lessons learned, and ensure proper security measures are taken for cities in different stages of Smart City evolution. Similarly, specific sectors may require tailored regulations or standards for public safety (e.g., in the Transportation Systems Sector with automated vehicles carrying hazardous materials; or, in the Water and Wastewater Systems Sector with shared water systems that service multiple cities).
- **Physical system security.** As standards and regulations are developed for cyber and cyber-physical systems, re-examining and modifying existing standards for physical components of those systems—particularly older or isolated elements, such as underground pipes, rural facilities, or isolated water reservoirs—will be an important part of securing against a combined cyber-physical attack.
- **Embedded-generation technology.** As individual consumers and private organizations increasingly implement solar and wind energy-generation systems, there will be a need for clear standards and regulations referencing installation, security, and integration into the smart grid. Although some standards exist, the rapid pace of implementation and adoption among a wider group of consumers will likely necessitate regular readjustment and clarification.
- **Signal-jamming technology.** As cyber-physical transportation technologies rely on a variety of sensors for functionality, it will be necessary to understand and consider additional regulations for signal-jamming technology that could compromise operation (e.g., GPS, LIDAR, and radar).[155]
- **Security for third-party vendors.** IT and data providers will play a significant role in system functionality, particularly during the initial rollout of smart transportation, energy, or water systems. Working with third-party vendors across sectors to ensure adequate security steps are taken and external inputs are reviewed for compatibility will help minimize and anticipate potential vulnerabilities. Such vendors should include international vendors (e.g., foreign car manufacturers) to ensure they meet cybersecurity and interoperability standards as they develop U.S. Smart City technology platforms.

[155] For example: https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-55A1.pdf.

- **Comprehensive security.** Cities needing to prioritize limited resources may give devices or system components with minimal SCADA connectivity or controllability less security scrutiny than devices or system components with extensive SCADA connectivity or controllability. Ensuring all components are examined for vulnerabilities provides an important starting point, but comprehensive security efforts should address overall system security, as well, since components will be interconnected through other systems and can be manipulated to cause significant problems.
- **Security regulation and enforcement.** Regulation for many infrastructure utilities relies on self-reporting (e.g., power plants). As systems are increasingly automated and networked across large regions, encouraging more stringent security regulation and enforcement—or otherwise providing incentives for regular and reliable self-reporting—may help minimize vulnerabilities and illuminate unanticipated issues.
- **Adaptive standards and regulations.** Cyber threats and vulnerabilities evolve rapidly as malicious actors become more skilled and new technologies are implemented. Therefore, standards and regulations must be able to quickly adapt to evolving situations or else risk becoming ineffective.

COMMUNICATION AND ENGAGEMENT

As Smart Cities adapt technologies at varying rates, strategic communication and engagement may influence a more secure evolution of cities' cyber-physical infrastructure, including:

- **Public trust.** Messaging and engagement—to acknowledge that accidents and mistakes will happen during early adoption and rollout phases of cyber-physical transportation technology—can help minimize negative public reactions (including loss of faith in the system) to inevitable disruptions. Such engagement includes educating users on why the mistakes occurred and how they are being addressed. Similarly, plans for rapid response and public messaging after disruptions will also help manage public trust levels.
- **User education.** It may take time for consumers to understand the security vulnerabilities associated with new technologies. Similar to education campaigns focusing on protecting computers from cyber threats, consumers will have to adopt analogous practices for new cyber-physical technology, as cyber-attacks will have the potential for physical consequences (e.g., vehicle collisions or infrastructure destruction). Programs aimed at educating users on how to protect against cybersecurity vulnerabilities will help promulgate security best practices and could create more incentives for manufacturers to address potential security issues. Examples of areas to pay attention to include:
- **Autonomous vehicles.** Consumers may have to play an active role in keeping autonomous vehicle security up-to-date as manufactures develop increasingly automated ways to manage security updates.
- **Smart electricity.** Education about smart electricity technologies and programs—such as smart meters, embedded technology, or demand-response programs—including warning signs that these systems are not functioning properly, will help individual and corporate users minimize vulnerabilities while monitoring the system. Such information will be particularly important regarding demand-response and integration with in-home devices (e.g., educating customers on how they work, what devices in their homes are connected, and what signs a breach or attack would leave).
- **Encryption education.** Many consumers and utility workers misunderstand encryption and incorrectly assume that it provides all-inclusive security. Messaging that explains what encryption does and does not secure—and that clarifies vulnerabilities are still inherent in smart electricity technology—will help utilities and consumers adjust to new dynamics brought by cyber-physical technology.
- **Owner and Operator Education.** Cyber-physical technology will bring new opportunities for companies to streamline efficiency. Central to this innovation is the training of staff capable of preventing, detecting, and mitigating potential threats that come with new technology. Retaining institutional knowledge about legacy infrastructure is also important. Properly training and educating infrastructure owners and operators on security risks can help ensure that technological expertise and risk management evolves at a steady pace. Examples of areas to focus on include:

- **Skill atrophy.** As city residents and public transportation operators become more accustomed to cyber-physical technologies, they are likely to spend less time manually operating vehicles or trains, which will reduce opportunities to test and maintain skills and reflexes over time. Incentivizing individuals to maintain the skills required to operate vehicles or trains, through education or public awareness campaigns, will help minimize negative impacts of intentional or unintentional system failures.
- **Targeted training.** In instances where manual or normal backup operations may be replaced by cyber-physical systems (e.g., bioreactors), both skills and emergency response training will help minimize response time and negative impacts in the case of an attack or system failure.
- **Remote connectivity.** Remote access to networked systems can inadvertently cause confusion or false alarms. Training at all personnel levels will help staff understand and separate authorized activity from unauthorized.
- **Insider threat.** The potential impact of insider attacks will increase with the level of automation and subsequently decrease user oversight and networking. Working with utilities to communicate the heightened vulnerabilities of insider threats and risks involved in centralizing and consolidating system control will help them identify safeguards and prevention mechanisms.
- **City administrator education.** Local governments, city administrators, and city planners face a learning curve as cyber-physical infrastructure becomes more pervasive. Education focused on technology implementation and mitigating anticipatable risks in cities can help create more informed and better prepared local administrations.
- **Networked infrastructure.** V2I, ITS, and similar systems are less likely to receive the attention or public scrutiny that cyber-physical vehicle or rail technology will. Education and outreach programs that communicate the unique vulnerabilities presented by networked infrastructure will help city governments better allocate maintenance and security resources to these elements of new transportation infrastructure. Such outreach programs could be particularly useful for cities in early adoption stages of various Smart City technologies.
- **Best practice promulgation.** Creating a forum for infrastructure owners and operators—to share experiences relating to integrating cyber-physical systems into legacy infrastructure—can prompt mutually beneficial discussions on unintended consequences, common mistakes, etc. that cities or utilities at different stages of Smart City development have encountered. These forums can occur at a national level or in smaller groups of cities with similar or shared legacy infrastructure.

FEDERAL ASSISTANCE

In some areas, DHS can facilitate or direct Federal assistance to State and local governments to support the growth of Smart Cities, including:

- **Skill atrophy.** Information banks and on-demand technical assistance or instructions can help cities combat skill atrophy and loss of institutional knowledge. In addition, such exchanges can help cities prepare for new cyber-physical technologies. This assistance will be particularly helpful in ensuring that city administrators and utilities retain manual-fix or override capabilities in the case of cyber-physical system attacks or failures.
- **Cross-city coordination.** DHS can facilitate a national implementation system or guidelines to help cities install and support cyber-physical components effectively, including between cities at different stages of development. This coordination might include providing resources to help utilities with older infrastructure assess if and how they can implement cyber-physical components onto their systems, or if they need to undergo a more holistic upgrade.
- **Technology implementation across cities.** Cities with different populations, infrastructure, and resource bases will integrate new technologies at different rates, and they will likely see different challenges in their adoption or implementation, as well. Federal assistance in transferring lessons learned, assistance to less-resourced cities, and tiered standards or regulations will facilitate more secure and efficient transitions across different types of cities.

- **Navigating ownership questions.** As consumers and private corporations integrate embedded-generation technologies, DHS has an opportunity to help local government proactively prevent and anticipate issues that will arise when privately owned infrastructure creates a vulnerability or breakdown.
- **Security resources.** Resource-strapped cities may experience particular challenges transitioning to smart technologies and accompanying shifts in security posture. Federal assistance may help these cities navigate this transition.
- **Securing electricity infrastructure.** Working with local governments to make smart meters less visible or accessible, providing security audit resources for cities electing to use cooperatives or third-party vendors, or helping cities build additional resilience into the system can help strengthen city-level security as they evolve into Smart Cities.
- **Integration and maintenance resources.** Although cyber-physical systems will bring budgetary savings, they will likely be expensive to maintain and operate as cities integrate them with existing systems while maintaining current technical expertise. Federal assistance in the form of budgetary or human resources during implementation can help manage this transition.
- **City-specific assistance.** Smart Cities will experience city-specific challenges associated with adopting cyber-physical technology—such as high-population cities having to install and maintain smart water-storage tanks, or cities with particularly old or poorly functioning electricity grids that cannot be networked. Federal assistance in the form of training, regulation development, or resources can help such cities navigate these challenges.
- **Risk assessments.** Cities will have different levels and types of risk as they implement smart technologies. Federal assistance in the form of risk assessment teams with consistent standards and methodologies will help cities identify and assess their specific risks, and identify mitigation opportunities.
- **Securing Smart City "borders."** Certain Smart City technologies will extend beyond geographic city limits to a State or regional level, allowing vulnerabilities to be exploited in rural areas while the consequences extend to population-dense cities. DHS can help identify and address these potential issues.

APPENDIX A: SUBJECT MATTER EXPERTS

Shahid Abbas	Arlington County, Transportation Engineering and Operations
Kris Ardis	Maxim Integrated
Ger Baron	Amsterdam Smart City
Alex Bedig	Stockholm Environment Institute
Pater Brostram	East Bay Municipal Utility District
Cesar Cerrudo	IOActive
Zak Doerzaph	Virginia Tech Transportation Institute
Patrick Driscoll	Aalborg University
Dan Edwards	Hazen & Sawyer
Adel Elmaghraby	University of Louisville
Joe Grand	Grand Idea Studio
Adam Greenfield	Urbanscale
Chris Greer	National Institute of Standards and Technology
Mark Hadley	Pacific Northwest National Laboratory
David Kuehn	Federal Highway Administration
Paul Larrousse	Rutgers University
Thomas Maillart	University of California, Berkeley
Larry Marcus	Arlington County, Transportation Engineering and Operations
Giampiero Nanni	Symantec
Victoria Pillitteri	National Institute of Standards and Technology
Dhamodaran Ramakrishnan	IBM
Sokwoo Rhee	National Institute of Standards and Technology

Steve Raney	Cities21
Kevin Schneider	Pacific Northwest National Laboratory
Doug Smith	Chesapeake Crescent Initiative
Anthony Townsend	New York University
Anthony Vanky	Massachusetts Institute of Technology
William Whyte	Security Innovation
Henry Willis	RAND Corporation
David Wollman	National Institute of Standards and Technology
Richard Wyman	Idaho National Laboratory

APPENDIX B. ACRONYMS AND ABBREVIATIONS

AMI	Advanced metering infrastructure
DHS	U.S. Department of Homeland Security
DLC	Direct load control
GPS	Global positioning system
ICS	Industrial control systems
IT	Information technology
ITS	Intelligent transportation systems
LIDAR	Light detection and ranging
NHTSA	National Highway Traffic Safety Administration
OpenADR	Open Automated Demand-Response
PMU	Phasor measurement unit
PTC	Positive train control
SCADA	Supervisory control and data acquisition
V2I	Vehicle-to-vehicle
V2V	Vehicle-to-infrastructure
WMATA	Washington Metropolitan Transit Authority

GLOSSARY OF TERMS

Autonomous Vehicles	Autonomous vehicle technology enables automobiles to understand the environments in which they operate and execute safe and efficient commands based on this understanding. Autonomous vehicles can assume decision-making and operational tasks, enabling drivers to become passengers, entirely disengaged from the demands of driving.
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[156]
Intelligent Transportation Systems	A system in which real-time data is gathered and used to inform automated decisions regarding the function of traffic-related infrastructure and hardware.
Positive Train Control	PTC is a system of remote sensors and automated control devices primarily designed to stop or slow a train automatically to prevent dangerous situations. Through wired and wireless connections and automated acceleration and deceleration controls, PTC is used to prevent train-to-train collisions, derailments caused by excessive speed, and unauthorized movement of trains.
Smart City	Urban centers that integrate cyber-physical technologies and infrastructure to create environmental and economic efficiency while improving the overall quality of life. A smart city "gathers data from smart devices and sensors embedded in its roadways, power grids, buildings, and other assets. It shares that data via a smart communications system that is typically a combination of wired and wireless. It then uses smart software to create valuable information and digitally enhanced services."[157]
Vehicle-to-Vehicle	Vehicles "talk" to one another to provide data about speed, location, and other information.
Vehicle-to-Infrastructure	These systems allow physical infrastructure to inform vehicles of their presence and provide additional data, and also allow vehicles to send information to infrastructure.

[156] USA Patriot Act of 2001 § 1016(e).
[157] Smart Cities Council, "Vision," http://smartcitiescouncil.com/category-vision, accessed February 4, 2015.

DHS POINT OF CONTACT

National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis
U.S. Department of Homeland Security
OCIA@hq.dhs.gov
For more information about the OCIA, visit our Website: www.dhs.gov/office-cyber-infrastructure-analysis.