Securing Smart Cities

Moving Toward Utopia with Security in Mind

Philippe Lin, Dr. Morton Swimmer, Akira Urano,
Stephen Hilt, and Rainer Vosseler

Trend Micro Forward-Looking Threat Research (FTR) Team

A **TrendLabs** Research Paper

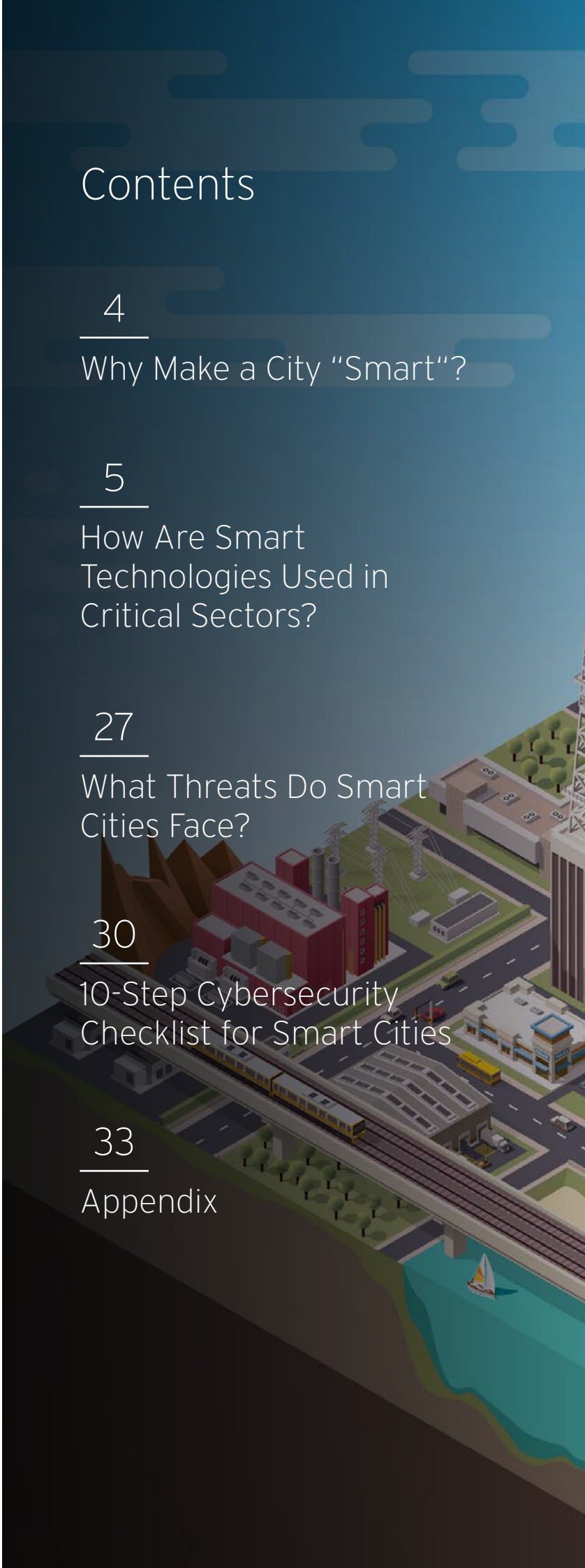
TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Contents



The concept of a "smart city" is not new and has been evolving over time. From serious urbanology books like Anthony M. Townsend's "Smart Cities" to three-minute cartoons on YouTube that illustrate how smart cities will change our daily lives,[1] people define the term from their respective perspectives, adding their own innovations based on their own imaginations. Authoritative organizations like the British Standard Institution (BSI) have also attempted to give a comprehensive definition in the publicly available specification, "BSI-PAS 180." It defined a smart city as "the effective integration of physical, digital, and human systems in the built environment to deliver a sustainable, prosperous, and inclusive future for citizens."[2] ISO/IEC, meanwhile, describes a smart city as a complex "system of systems—both traditional systems (e.g., critical infrastructure) and new ones resulting from emerging technologies (e.g., virtualization, sensor networks, etc.)."[3] A comprehensive article put more emphasis on the fact that a smart city is an "ultra-modern urban area that addresses the needs of businesses, institutions, and especially citizens."[4]

The characteristics of a smart city include:[5, 6]

- Has a networked infrastructure to improve economic and political efficiency and enable social, cultural, and urban development
- Puts underlying emphasis on business-led urban development
- Focuses on social inclusion of various urban residents in public services
- Understands the crucial role of high-tech and creative industries in long-term urban growth
- Accords profound attention on the role of social and relational capital in urban development
- Emphasizes social and environmental sustainability

Common among the definitions is the merger of the physical (urban area, citizens, and infrastructure) and digital environments that lead to the notion of "open-air computers."[7] The concept of a smart city did not come out of a vacuum though. Economic and developmental factors drive information and communication technology (ICT) use in cities, making the adoption of some form of smart city technologies inevitable for most cities worldwide.

This paper surveys some of the existing smart technologies currently used in smart cities worldwide. Much like our previous reports on exposed smart devices and the hacking of robots in smart factories, this paper will discuss the risks of using smart technologies in critical sectors and will provide actionable steps to help local governments and urban developers design more secure smart cities.

Why Make a City "Smart"?

More than half (54%) of the world's current population resides in urban areas compared with just 30% in the 1950s. In 2009, the global population was estimated at 6.8 billion[8]—around 3.7 billion lived in urban areas. By 2050, 66% of all people will be urban dwellers.[9]

Urbanization does not always occur organically. To accelerate China's "Four Modernizations" campaign, for instance, the country plans to move 250 million people to cities so it would end up with 900 million urbanized people by 2025.[10] The process of urbanization leads to exurban sprawl, the formation of slums, scattered workplaces, and aging infrastructure. These may cause huge inefficiencies in energy use, traffic, governance, waste management, and pollution, among others.

To meet these social, economic, and environmental challenges, public and private sectors invest heavily in smart city technologies. The following technologies and trends associated with smart cities were identified in the previously mentioned ISO/IEC Smart Cities Preliminary Report:

- Ubiquitous computing
- Networking
- Open data
- Big data
- Geographic information system (GIS)
- Cloud computing
- Service-oriented architecture
- E-government
- Embedded network
- Internet of Things (IoT)

The global smart city investment revenue is estimated to reach US$88.7 billion by 2025 from US$36.8 billion in 2016.[11] Technology use is expected to reduce carbon emission by 15% by 2020, resulting in 1 ton of CO2 reduction per capita or US$946 billion in financial savings.[12]

Public sector investments also play an important role in smart city implementation. The U.S. White House, for instance, announced an US$80-million federal investment in the "White House Smart Cities Initiative" to help cities address issues in specified key areas like climate, transportation, public safety, and city service transformation.[13] The U.S. National Science Foundation, meanwhile, announced over US$60 million in new smart city-related grants in 2016 and planned new investments for 2017.

How Are Smart Technologies Used in Critical Sectors?

For a city to be considered "smart," it must use smart technologies in its critical infrastructure sectors. In this section, we will discuss how these technologies are currently being implemented in the energy, transportation, environment, communications, and government sectors. We shall also briefly raise possible security concerns brought about by these implementations.

Smart Energy

Creating "smart energy" in a smart city is not limited to using a smart grid. The objectives of producing smart energy are also not limited to saving energy. Low carbon dioxide (CO2) emission, distributed generation and storage, energy security, the use of clean and sustainable energy, and energy efficiency are also of equal importance, which gave rise to certain standards for smart cities, including:

- IEC/TR 62357:2003 Power System Control and Associated Communications
- IEC 61850 Power Utility Automation
- IEC 61970 Common Information Model (CIM)/Energy Management
- IEC 61968 CIM/Distribution Management
- IEC 62351 Security

To improve its energy efficiency and reduce CO2 emission, Yokohama used energy management systems (EMSs). A community EMS (CEMS) and high-efficiency co-generation systems can also be used to generate electricity and heat up buildings. Using the Building Automation and Control Networking (BACnet) protocol for in-building control systems can also be considered.

Heating accounts for 41.5% of the total household energy consumption in the U.S. in 2009.[14] In Japan, this number reached 51% (space heating, 22.9%; water heating, 27.8%) in 2014.[15] To heat up houses during cold weather, smart cities plan to use hydrogen (Yokohama), solar heating (Songdo International Business District [IBD]), and geothermal heat pumps (both Songdo IBD and Yokohama). Solar power and hydrogen can be used to provide renewable and clean energy, in addition to wind power, if feasible.

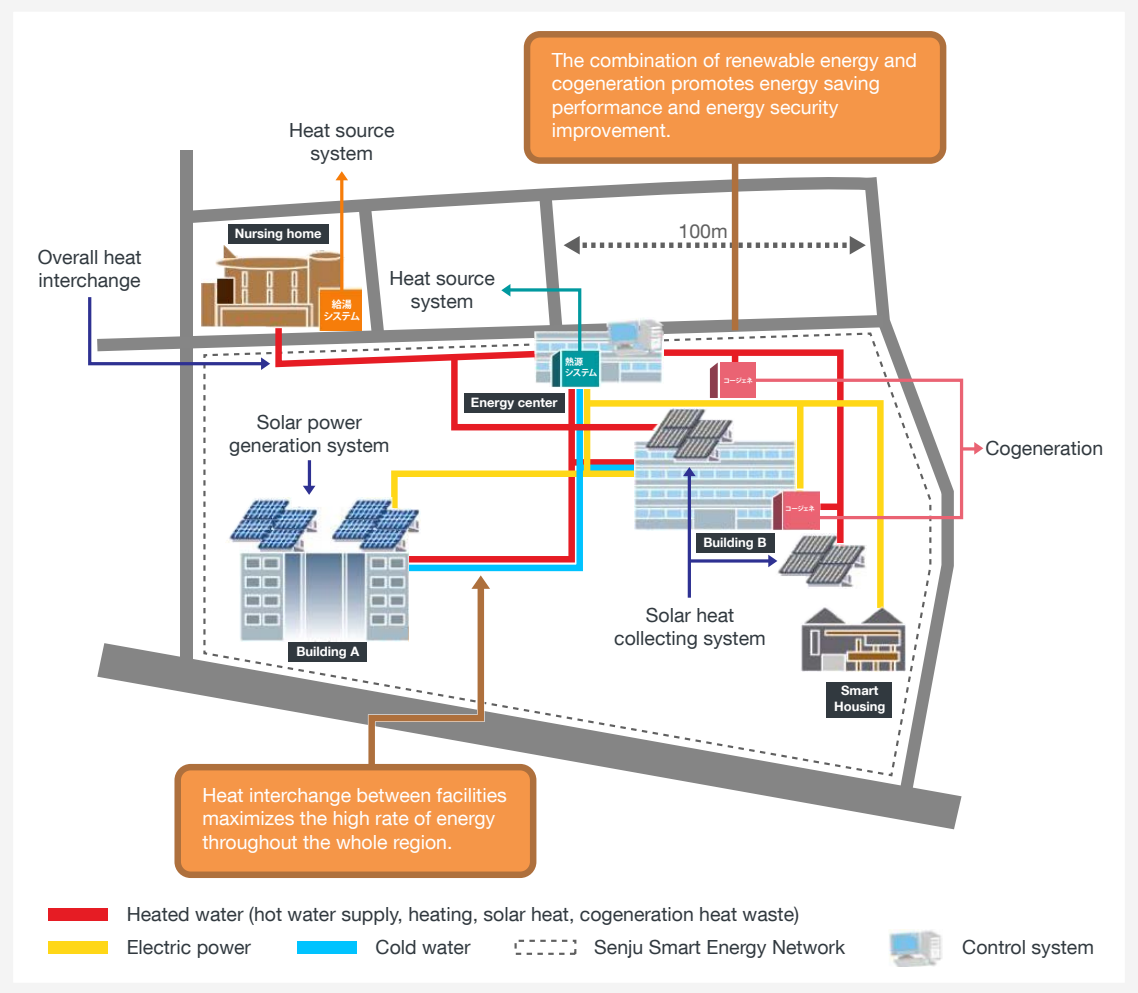


Figure 1. Heating system across buildings in Minami-Senju, Tokyo

(Source: http://www.meti.go.jp/committee/summary/0004633/pdf/018_05_00.pdf)

Smart Meters

Smart meters record electricity consumption between preset intervals (usually every 15 or 30 minutes) and send the data collected to the utilities provider. They use automatic meter reading (AMR) systems that use radio transmitters to send readings to a network, handheld devices, or rooftop receivers[16] via Wi-Fi; the industrial, scientific, and medical (ISM) radio band; or mobile networks.

This poses strong privacy concerns because it is possible to profile people through their electricity consumption.[17] Electronic Reporting Tool (ERT)-compatible meters that work in the ISM band can be hacked, allowing attackers to sniff smart meter data with a piece of software that is publicly available. Even cheap USB radio dongles can be used to read smart meters. Given that, it is possible to read neighbors' meters by just inputting specific meter IDs.

```
10:38:27.348667 decode.go:83: SampleRate: 2359296
10:38:27.348716 decode.go:84: DataRate: 32768
10:38:27.348764 decode.go:85: SymbolLength: 72
10:38:27.348810 decode.go:86: PreambleSymbols: 21
10:38:27.348855 decode.go:87: PreambleLength: 3024
10:38:27.348900 decode.go:88: PacketSymbols: 96
10:38:27.348946 decode.go:89: PacketLength: 13824
10:38:27.348991 decode.go:90: Preamble: 11111001010100110000
10:38:27.349036 main.go:96: GainCount: 29
{Time:2016-12-07T10:38:36.812 SCM:{ID:56195484 Type:12 Tamper:{Phy:00 Enc:00} Consumption:  150532 CRC:0x4A15}}
{Time:2016-12-07T10:39:02.812 SCM:{ID:56195484 Type:12 Tamper:{Phy:00 Enc:00} Consumption:  150532 CRC:0x4A15}}
{Time:2016-12-07T10:39:30.810 SCM:{ID:56195484 Type:12 Tamper:{Phy:00 Enc:00} Consumption:  150532 CRC:0x4A15}}
{Time:2016-12-07T10:41:04.807 SCM:{ID:56195484 Type:12 Tamper:{Phy:00 Enc:00} Consumption:  150532 CRC:0x4A15}}
```

Figure 2. Smart gas meter reading decoded with a US$20 USB radio dongle

Figure 3. ERT-compliant smart gas meters.

Advanced metering infrastructure (AMI) enables two-way communication between meters and a central system. This allows systematic control of power consumption and throttling, making peak shifting and cutting possible. Attackers can send fake demand signals or block incoming signals which could cause issues with electric power distribution. This is not easy to do, but also not impossible.

Figure 4. Smart meter that supports Route B services in Tokyo

The Device Language Message Specification (DLMS) Green Book, 7th edition, defined a key management mechanism, which includes a master key, a global unicast encryption key, a global broadcast encryption key, an authentication key, and a dedicated key for smart meter-AMI communication. A session key, however, has not been defined so vendor implementations may drift from the standard and become vulnerable. Fortunately, the Green Book version implemented in each smart city is usually not disclosed.

Penetration testing can assess potential vulnerabilities in smart meters and suggest improvements. Companies and universities have thus studied both smart meters and AMI. More than 40 denial-of-service (DoS) weaknesses and vulnerabilities were found in a recent smart meter penetration-testing contest in Taiwan alone,[18] which could translate to risks for users.

CEMS

A CEMS coordinates subsidiary EMSs in a community, including household EMSs (HEMSs), building EMSs (BEMSs), electric vehicles (EVs), battery supervisory control and data acquisition (SCADA) systems, and photovoltaic (PV) systems, for peak shredding and shifting.

A CEMS helps determine the peak or maximum demand for power and decides what size of generators and capacity of transmission lines to use for a short period of time to meet the demand. Grid stability is impacted if power consumption is not regulated. Unplanned overloading activates circuit breakers and results in power outages. A CEMS releases the electricity stored in batteries to the grid when consumption peaks. Solar panels that generate too much power, meanwhile, store this in community battery centers for use in charging EVs.

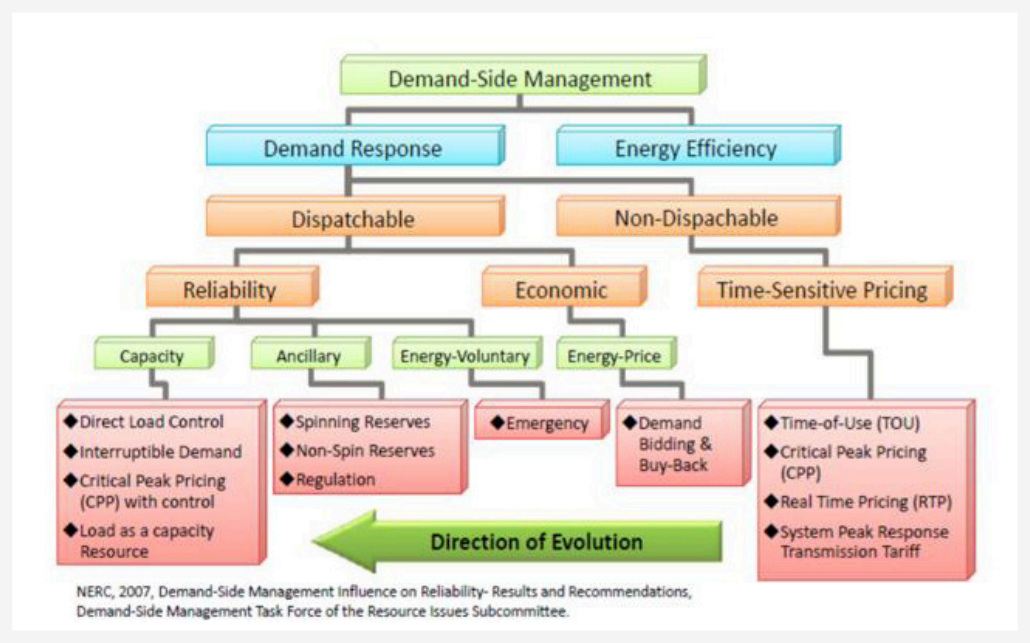


Figure 5. Demand-side management evolution

(Source: http://report.nat.gov.tw/ReportFront/report_detail.jspx?sysId=C10403013)

In Yokohama, CEMS use resulted in a 22.8% peak-cut in the business sector and a 15.2% peak-cut in the residential sector.

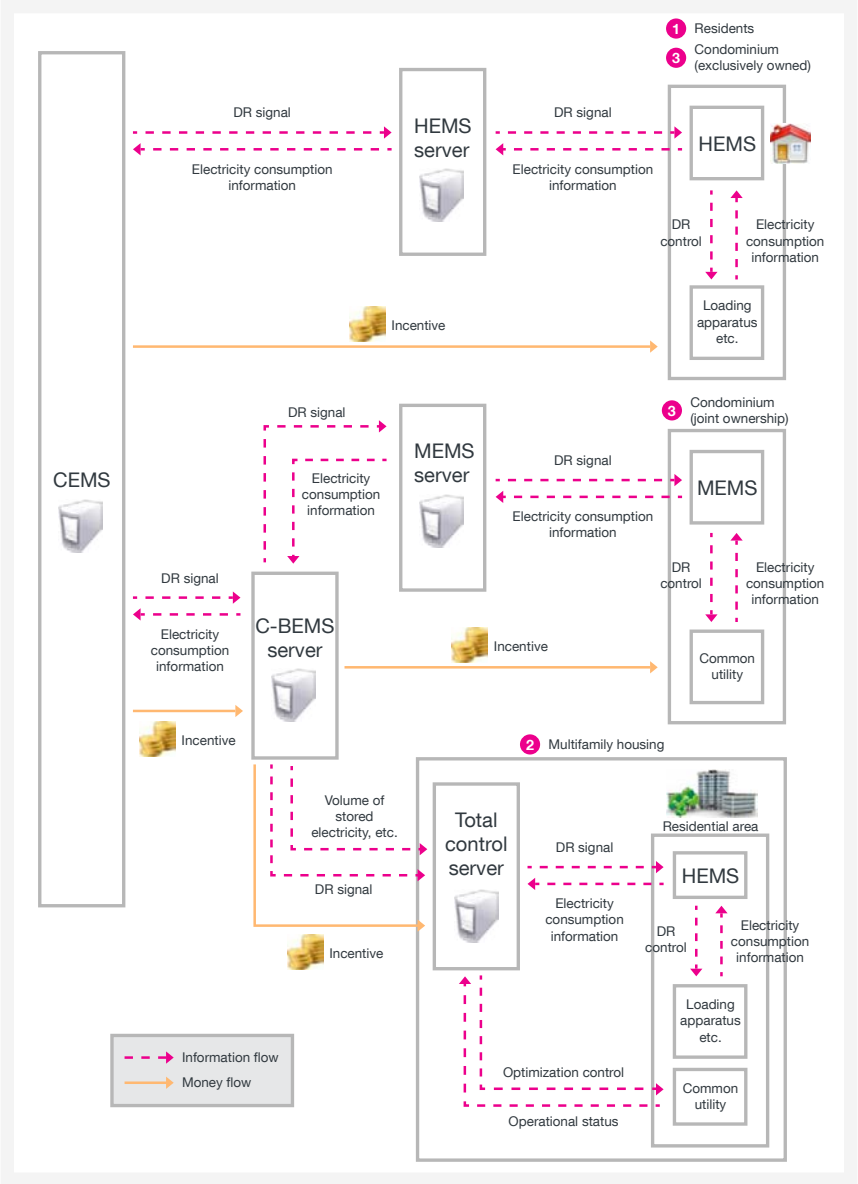


Figure 6. Demonstrative model of demand-response and real-time consumption

(Source: http://www.meti.go.jp/committee/summary/0004633/014_03_00.pdf)

A CEMS coordinates with BEMSs and HEMSs in mansions, buildings, and apartments. Power consumption information is then fed back to the CEMS for automated load balancing. When the consumption exceeds a preset threshold, demand-response commands are broadcast to the AMI, causing regulated households to automatically turn off high-volume appliances to reduce the demand in exchange for incentives. As in any other communication-enabled system, however, a CEMS is vulnerable to DoS attacks and counterfeit messaging.

HEMSs

Feedback technologies like in-house energy displays encourage smart energy practices.[19] HEMSs visualize energy use and help users monitor their electricity consumption, encouraging them to save power and spend less.

Some HEMSs monitor their energy consumption, allowing them to save on costs by setting limits.

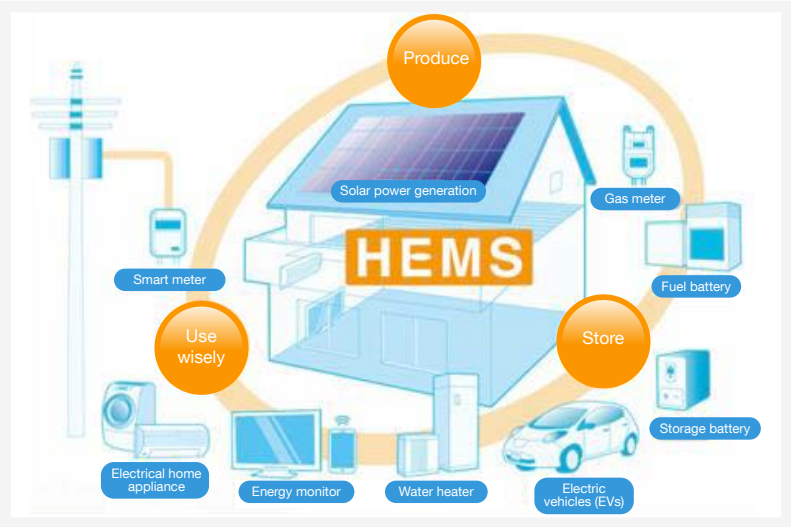


Figure 7. HEMS architecture

(Source: http://kaden.watch.impress.co.jp/docs/news/527582.html)

In Japan, the Protocol for carrying Authentication for Network Access (PANA) is used in HEMSs. It uses Extensible Authentication Protocol (EAP) to authenticate between clients and an IP network. After authentication using a preshared Route B ID and password, a PANA session is established and ECHONET Lite messages are encrypted with a session key. A PANA session expires after 24 hours and a new session key is generated for each new connection.[20] Despite PANA's robustness and intrinsic security, some HEMSs use only a four-digit password instead of the recommended 12-character password. This opens the device to brute-force attacks that can allow attackers to send commands and affect even connected devices. It does not help that some vendor sites require users to key in their HEMSs' media access control (MAC) addresses and passwords when filing service requests, making them lucrative phishing targets.

We have not seen attacks against smart energy systems or AMI. But we have seen a solar software and analytics company issue patches for its power meters to protect them against command injection and remote code execution vulnerabilities.[21] We have seen attacks against industrial control systems (ICS) used in power grids too, which caused power outages.[22] As such, we believe attacks against smart energy systems are possible.

Smart energy systems like those used in Yokohama can be hacked as well. Jamming radio signals can stop or impair demand-response, at least in households. HEMS control panels can be targeted by brute-force attacks if users do not change default passwords. Stolen passwords can then be used to control or hold connected appliances hostage in exchange for ransom. Attackers who do not wish to seek attention, meanwhile, can just quietly steal power generated by the users' solar panels. HEMS owners can also be tricked into thinking their devices are broken. Fake or modified devices can also be installed in new houses.

Really good attackers can find ways to upgrade system firmware over the air (OTA). Corrupted firmware require repair or replacement, resulting in unwanted costs on the service provider's part. Attackers can also send tons of fake demand responses that can lead to heavy fluctuation in the regional grid.

To mitigate such risks, hiring licensed penetration-testing contractors to test the stability and reliability of smart meters and AMI on a regular basis is necessary. A self-adaptive system like a demand-response mechanism can also cause a domino effect. As such, systems should have manual override features by design.

Smart Transportation

Smart transportation or smart mobility addresses issues in traffic management like congestion, pollution, and insufficient fuel supply. In highly dense cities, these issues have to do not only with too many private vehicles, but also with the design of commuter bus lines, metro systems, taxis, and shared vehicles.

Smart Parking Lots and EVs

Parking is a problem for many vehicle owners. In Pasadena, common parking pain points include:[23]

- Inadequate information on parking availability and pricing
- Inefficient use of existing parking lots
- Difficulty in finding parking spaces within walking distance from destinations at specific times of the day
- Lack of sufficient parking slots at event sites

Parking spaces can be intrinsically insufficient, especially in overcrowded cities. For example, 2.7 million cars and motorcycles are registered in Taipei in 2016 but there are only 1.4 million available parking lots. To address such an issue, many cities now provide mobile apps like ParkCBP in Canberra, Australia. Smaller cities like Bolzano, Italy, meanwhile, have websites that show the number of available parking spaces in real time. Private parking lots have also adopted vehicle sensors to manage parking lots and

mobile apps to provide information, including pricing and automatic credit card billing. Some private parking lots even allow drivers to book slots in advance. Softbank in Japan also announced a country-wide smart parking project that uses buried sensors with NarrowBand IoT (NB-IoT), a low-power wide area network (LPWAN) radio technology, to monitor parking spaces in real time.[24]

In cities that promote EV use, EV charging stations have been integrated with parking lots. In Japan, the Kanagawa Municipality has 1,028 public EV chargers, 377 of which are located in Yokohama. EV charging stations are integrated with EMSs. Surplus electricity detected by BEMSs and HEMSs are used to charge EVs. In case of emergencies, EVs can drive into the basement of a building to stream back excess electricity.

Figure 8. Vehicle-to-building (V2B) system used in Yokohama

Booking parking slots in advance can provide good business, akin to event ticket scalpers. But this can also be abused by enterprising cybercriminals, specifically ransomware operators.[25]

Metros and Buses

Public transportation, specifically transport timetable and information coordination, fare and ticketing integration, quality transport infrastructure and interchange building, and community and demand-responsive public transport provision, can be facilitated with ICT.

In 2010, for instance, Groningen initiated a €39,000 smart city pilot project for a public transport planner to create a mobile app that provides real-time bus schedule information and bus monitoring for partners.[26] The Taipei City Public Transportation Office also provides Global Positioning System (GPS) tracking data for running buses on a website, allowing people to use apps like BusTracker Taipei. That said, tracking buses with in-vehicle GPS devices is not a new idea. In 2009, half of the transit buses in the U.S. were equipped with GPS, providing automated stop announcements.

Unlike buses that require drivers, metros can be fully automated. Although connected trains are usually safe and efficient, some cases of temporary service interruption have been seen. In November 2013, for instance, the Bay Area Rapid Transit (BART) closed down due to a software glitch after a server upgrade. People were stuck in trains and track switching had to be done manually.[27] Though unrelated to rail operations, the San Francisco Transportation Agency was hit by a ransomware attack that encrypted 2,000 of its computers, allowing passengers to ride for free until the problem was fixed.[28]

Fully dynamic and optimized transportation systems will definitely benefit citizens. But when transportation becomes really "smart," attackers will always find more ways to benefit from intrusions.

Taxis and Shared Cars

Car-sharing, carpooling, and transportation network companies have found a way to increase the per capita utility of a car while reducing congestion and carbon emission, and addressing insufficient parking spaces.

Uber and Lyft are categorized as transportation network companies, as their business is essentially providing an online platform that connects passengers to commercial drivers. Despite tax and safety issues and protests organized by taxi drivers, such services continued to be provided.

Taxi and car-sharing services in smart cities can, however, better help reduce carbon footprint.[29] By combining trips and with a new dispatch algorithm that analyzes travel patterns, the Massachusetts Institute of Technology (MIT) Senseable City Lab showed that cumulated trip lengths may be reduced by 40%, resulting in less congestion and lower costs.[30]

Shared Bicycles and Scooters

Bicycle sharing is not a new idea to city planners too and is also a means to reduce the amount of space needed for streets and parking spaces, along with carbon footprint. Since 1998, for instance, Le vélo STAR has been serving citizens in Rennes, France, along with around 700 cities in more than 50 countries.[31] Users can pay via preregistered smart, credit, citizen, or other payment cards. The biggest bicycle-sharing city in the world is Hangzhou with 84,100 bikes in 3,354 stations.

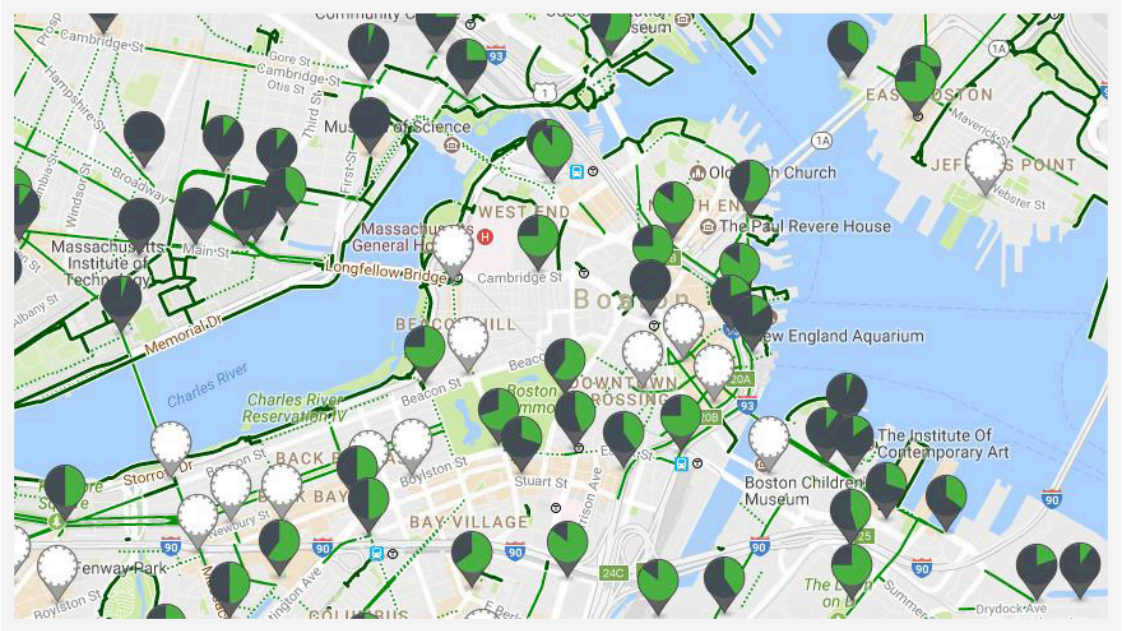


Figure 9. Map showing available bikes and open docks

(Source: https://secure.thehubway.com/map/)

Even private companies like Mobike and Ofo offer similar services. To prevent abuse and theft, Mobike uses GPS to track its bikes and designed a credit system that does not allow users with less than 80 points to rent a bike. That way, only those who have been known to return bikes can use them again.

Gogoro partnered with Coup to provide 200 electric scooters in Berlin.[32] Preregistered members use a mobile app to locate the nearest available scooters. Once payment is made, scooters are unlocked and made ready for use. Yugo provides a similar service in Barcelona.

Previous research[33] suggested vulnerabilities in Gogoro's Bluetooth stack. These have since been fixed but new bugs can be abused to give attackers free rides. Attackers use ransomware attacks to disrupt vendors' services. In one instance, U-Bike Taiwan upgraded to a corrupted firmware, which prevented users from borrowing and returning bikes. The business model can also put users' privacy at risk, as vendors get personal itinerary data.

Traffic Lights

Several cities are currently investing in "smart roads" to support driverless vehicles or cars with vehicle-to-infrastructure (V2I) equipment. Though smart roads have yet to be implemented, smart traffic management already exists in some cities.

Smart traffic management requires a centralized system to control traffic lights and sensors that regulate traffic throughout a city[34] to reduce delays or optimize "green" time and reduce waiting time for pedestrians who want to cross streets. The data collected from induction coils, cameras, radars installed on intersections, Bluetooth detectors, and closed-circuit TV (CCTV) feeds are sent to a traffic control center to optimize traffic flow. Cambridge and hundreds of other cities worldwide use the Split Cycle Offset Optimisation Technique (SCOOT), which uses queue detectors and cameras on main roads.[35] Another option is to use fiber optics. The Utah Department of Transportation, for example, adjusts connected signals within 30 seconds.[36]

Smart traffic lights controlled via radio signals may be prone to hacking if they have open and unencrypted protocols. Controllers that have debugging ports are also prone to physical intrusion, allowing attackers to physically disable their malfunction management unit.[37]

Smart traffic lights can also collect data (sometimes more than necessary) for analytical use. Collecting MAC addresses, for instance, has been the subject of controversy, raising concerns about privacy.

An in-vehicle service like Audi Traffic Light Information (TLI), which allows OTA updates, can be prone to remote access vulnerabilities. It is possible for attackers to issue false OTA updates to hijack it, install ransomware on its system, or simply push wrong traffic information to it. Traffic lights that collect tons of data can be hijacked and the stolen data monetized. Hackers can also sell "always green" services by abusing open and unencrypted radio signals to control traffic lights. Newer traffic lights connected via Long-Term Evolution (LTE) may be prone to a downgrade attack that can cause city-wide chaos as well.

Evacuation Systems

To evacuate crowds from overpopulated places during rush hour or public events, smart evacuation systems are being considered. Collective human behavior and public mentality are being considered to deal with panic and point people to the most intuitive routes while motion direction, density distribution, and obstacles are measured to dynamically maintain movement.[38] The European Union (EU) funded a research program for smart evacuation—eVACUATE, a scenario-independent, situation-awareness guidance system for sustaining active evacuation routes (AERs) for large crowds.

Similar research used a smartphone app to collect and deliver information to the crowd. It may be dangerous and unstable to depend on cellular networks for evacuation purposes though. An LTE base station is configured to maintain approximately 100 simultaneous connected users. Even when the theoretical maximum number is around 1,000, an emergency event can interrupt the services of the nearest base station.

Smart evacuation systems, if misused, can cause severe damage and injuries to people. They can lead targets toward danger.

Smart Environment

Apart from energy and transportation, the environment also plays a role in making a smart city more sustainable and livable. Air quality sensors allow people to decide whether playing outdoor sports is a good idea or not (if it is too polluted). Smart solid waste management systems use actionable data to optimize dumper truck schedules and vacuum overflowing trash cans. Smart sewage systems, meanwhile, reduce the amount of unprocessed water to overflow to bodies of water, reducing the possible impact to cities downstream.

Air Quality Monitoring Systems

Official air quality data is collected from air quality measurement stations. More than 9,000 stations in 600 major cities publish data as part of the World Air Quality Index project.[39] Instruments in measurement stations have to comply with legal accuracy and quality assurance operations to maintain data quality.

Nijmegen is not the only city that developed a distributed air quality network. Chicago also launched Array of Things (AoT) in August 2016, which uses fitness trackers to measure temperature, air pressure, light, vibration, and air quality, including gas emissions and ambient sound intensity. The data collected is publicly accessible. Researchers and policymakers can use it to support the development of innovative projects and administrative decisions. AoT promises not to monitor Bluetooth and Wi-Fi communications for the sake of privacy and uses the AT&T cellular network.

Figure 10. AoT used in Chicago

(Source: https://ci.uchicago.edu/press-releases/chicago-becomes-first-city-launch-array-things)

Newer air quality monitoring projects with better accuracy, lower price, or better connectivity are now available. Airly, a sensor tied to a streetlight, uses LoRa LPWAN. Yuktix is a purely India-made fixed air quality station deployed in Jaipur. Most projects though use MCU (Arduino or similar MCU) or embedded Linux as controller and rely on common communication modules like Wi-Fi or Bluetooth. Given the limited computing power of MCU, Wi-Fi credentials may be stored in clear text from in EEPROM or removable media while Bluetooth usually works with the default PIN code, 1234, if at all. Security is also harder to ensure for projects that use embedded Linux. Vulnerabilities in Linux can also affect embedded chips. A single air quality sensor may not be worth breaking in to, but all air quality sensors in a city are a different matter.

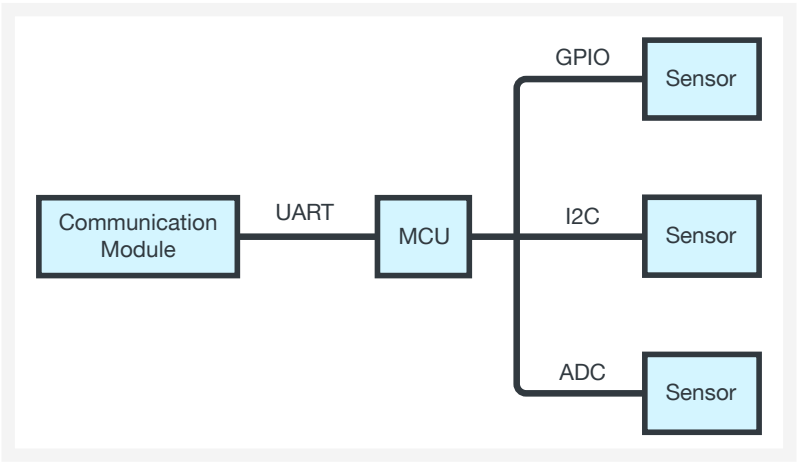


Figure 11. Architecture of many air quality projects

Solid Waste Management Systems

Integrated solid waste management (ISWM) has a great impact on public health, the environment, and resource management. Disasters[40] occur when ISWM fails to work.

Cities generated 1.3 billion tons of solid waste in 2012, which cost US$205.4 billion to manage. This number is expected to reach 2.2 billion tons by 2025. Knowing that solid waste management budgets are low, it makes perfect sense to use smart technologies to reduce costs.

Garbage trucks usually run on fixed routes at fixed times. Unfilled and overflowing bins are collected at the same time, which can cause public health issues. Researchers thus proposed algorithms to introduce dynamic waste collection schemes that reduce costs by optimizing collection routes and increasing collection efficiency.[41]

Songdo IBD uses a pneumatic waste system to suck garbage to a central location. Most cities that cannot build such a system from scratch can consider smart trash cans with sensors, radio-frequency

ID (RFID), and optional compactors. Philadelphia, Hamburg, Melbourne, and many cities worldwide use solar-powered smart trash cans called “Bigbelly” since 2009. It comes with a solar panel that charges its internal battery, light-emitting diode (LED) status indicators, and uses General Packet Radio Service (GPRS) for online monitoring and management. When the amount of trash reaches a certain level (measured by a pressure sensor), a compactor is activated to reduce the volume, reducing the need for collection.

Figure 12. A Bigbelly installed in Rathausmarkt, Hamburg

It is possible to hack a smart trash can. Attackers can bring dust carts to a specific place. If the platform used is centralized, they can manipulate dust carts from multiple cities to converge in one place. For this, attacking the application programming interface (API) of the management system is a common starting point.

Sewage Systems

UN-HABITAT estimates that 90% of wastewater is discharged untreated into rivers, lakes, and oceans in developing countries. Some developed countries, meanwhile, have problems with legacy sewage systems.

DontFlushMe (or SewerSense Combined Sewer Overflow [CSO] monitor) is a famous project initiated by Leif Percifield in 2011. It monitors sewer levels in New York and alerts subscribers via SMS, email, Twitter, or Internet-connected “Visualight.” It allows people to limit water use, decreasing the environmental impact by reducing CSO amounts. It has been reported as successful though we found that the official Twitter account (@dontflushme) stopped updating in February 2015. A Google search shows the site may have been hacked, putting the whole project on hold.

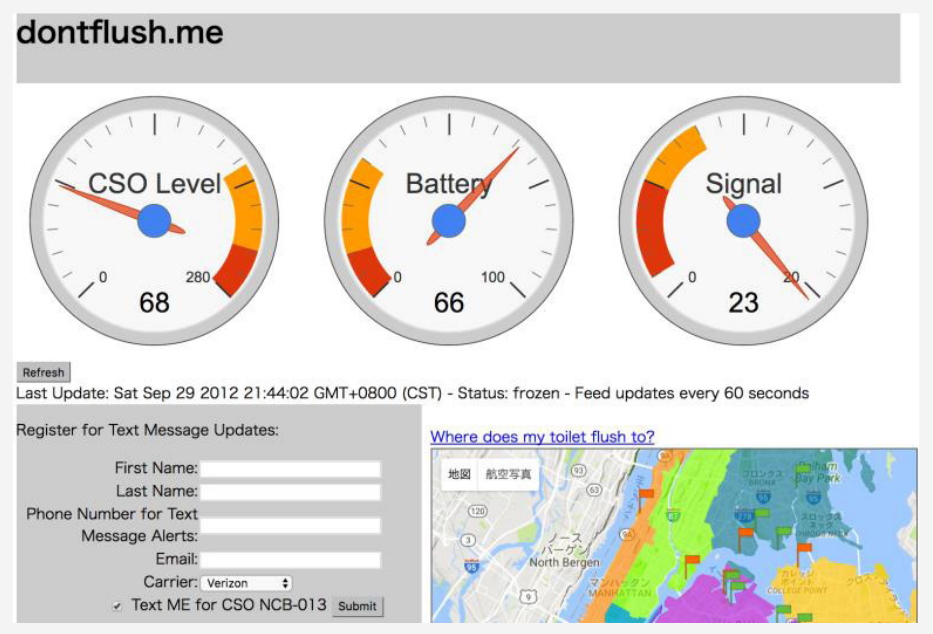


Figure 13. Dashboard on http://dontflush.me

Radio security is critical for Cyber-Physical Systems (CPSs). EmNet and the University of Notre Dame developed CSOnet for South Bend, Indiana. CSOnet is a control network that opens and closes smart valves to prevent basement backups; maximize the flow to publicly owned treatment works (POTW); and redirect flow into throttle pipes, inline storage, or overflow reservoirs at key points. If the system is hacked to open all smart valves, wastewater in trunk lines will flow to the interceptor, causing POTW to let go of untreated wastewater, which can be hazardous to the environment. Low-power radio signals are often unencrypted and unauthenticated. If hackers find a way to blind or manipulate the data sent to data acquisition points, they can also mislead the control center to make the wrong decisions.

In 2011, a hacker claimed to have broken into a water plant in Texas.[42] Though this is a case of unprotected ICS or, more precisely, its human-machine interface (HMI), hacking into a smart sewage system, especially those with smart valves, can cause similar damage, if not more.

Smart Connectivity

Smart city infrastructure and apps rely on a robust backbone and stable connectivity. Dedicated communication channels, fiber optics for smart traffic lights, or directional radio for emergency broadcasting are efficient, but can also be costly. As such, existing and generic means of communication are used and extended for wider coverage. Choosing the right technology is a far from straightforward endeavor, as it concerns the area of deployment, the expected amount of data, and battery life.

Public Wi-Fi Connection

Public Wi-Fi is part of the broadband infrastructure that supports economic development, career training, education, healthcare, and job hunting, provided by municipalities and the private sector.

Despite the usability and speed provided by public Wi-Fi, it can be slow and unstable, and its communication distance quite limited in urban areas. It also brought to fore privacy concerns, as many public Wi-Fi networks require users to register with a mobile phone and input a verification code or an email address. In addition to data breach woes, collecting "anonymized" Wi-Fi data is another concern. Access points still get the MAC addresses of all connected devices and users' session keys, which can be leaked. Even worse, public Wi-Fi networks are usually "open," which means data transmitted from and to a client device is not encrypted. Hackers with a wireless card that works in monitor mode can intercept at least part of all communication.

Public Wi-Fi networks can also be turned into massively deployed International Mobile Subscriber Identity (IMSI) catchers under given circumstances. Auto-connected encrypted Wi-Fi allows users authenticated with SIM cards to connect to the network provided by their mobile operator or its partners. Though the communication is encrypted, the IMSI is not, making it prone to passive attacks.[43]

Cellular Networks

Cellular networks work well in places where endpoints are widely distributed and the volume of data transmitted is limited. Municipalities can work with existing network operators to save on costs. GPRS has an approximate maximum range of 26km and a data rate of 56–114kbps. Base stations are also used in urban areas, making them accessible to embedded smart things.

Inexpensive cellular modules for embedded projects using Arduino or a more powerful system on a chip (SoC) work off the shelf.

Figure 14. A SIM808 module

(Source: https://www.adafruit.com/product/2542)

Power consumption is a major concern with regard to IoT. The components of most projects stay in sleep mode and are only woken up in designed cycles, as power is limited by battery type. Cellular modules are power greedy. As such, to launch a massive DoS attack, hackers only need to find a way to wake sensors up at the wrong time so the system cannot be synchronized properly. They can use a mobile signal jammer to drain the battery. They can also intercept communications[44] using a rogue base transceiver station (BTS) that can gain full control of victims' GPRS data communication. 3G and LTE are prone to downgrade attacks or redirections. Analyzing the data intercepted allows hackers to know how a system works, its instruction set, the IP addresses or phone numbers of its cloud services or backend servers, and hardcoded credentials, if any. The backend can also be further fuzzed to cause more damage or instigate a takeover.

To mitigate such risks, encryption is critical. If session key base encryption is not feasible due to power restraints, use at least symmetrical encryption with a good key.

802.15.4 and 6LowPAN Protocols

The 802.15.4 and 6LowPAN protocols are standards used in connected lighting and more than 70 million smart meters. It is characterized by lower power consumption, data throughput, power digital radio, and cost. Like Bluetooth, devices that use these have application profiles for home automation, healthcare, light linking, and smart energy, among others.

Göteborg Energi deployed 265,000 smart meters in Sweden in 2010. These reached an actual distance with a free sight line of 2km. Some 8,000 concentrators aggregated and sent meter readings to the central system via GPRS or fiber optics. The AMI supports hourly and on-demand readings, remote switching, power failure alarms, and power usage and voltage monitoring levels.

The protocol supports AES-128-CCM encryption, Transport Layer Security (TLS) v1.2 end-to-end security, and PANA/EAP and network rekeying. The 128-bit key can be a network or link key, but this should be preinstalled or obtained through a secure medium. Because smart meters that use the protocols are widely deployed, they are also widely studied. Manipulating the grid voltage via vulnerable meters can possibly lead to a household power outage and physical damage.[45] Vulnerabilities in home automation and light linking profile implementations were also found.[46] Keys can also be extracted from firmware and sniffed when a new node joins a vulnerable network.[47]

We have not yet seen a city-wide blackout caused by vulnerabilities in the protocols, their GPRS concentrators, or vendor implementations of DLMS/COmpanion Specification for Energy Metering (COSEM). Given the wide attack surface, however, this can change in the future.

LPWANs

LoRa, SIGFOX, and NB-IoT are among a long list of LPWAN solutions designed for long-range communications with very low data throughput and power consumption. As such, LPWANs are used in dispersed sensors that send a few bytes every hour to a server. Its high signal penetration capability makes it suitable for urban deployment where dense buildings cause signal blind spots.

The Netherlands is the first country to have nationwide LoRa coverage. It has deployed 1.5 million devices in a span of just eight months. LoRa has already been tested in the Schiphol Airport for baggage handling and facility service provision.[48] South Korea followed suit with SK Telecom's help. Taipei has also deployed LoRa city-wide with only 12 gateways.[49]

Figure 15. MQTT message for payload transmitted over LoRa

The message in the screenshot is not encrypted with a preshared application key, as the LoRa Alliance claims. LoRa's radio features uses chirp spread spectrum modulation to resist channel noise, multipath fading, and the Doppler effect. Its closed-source protocol did not make it safe though, as its physical layer was decoded via blind signal analysis in a demonstration by Matt Knight in DEFCON 24.

Smart Governance

In 2015, the New York City Department of Health and Mental Hygiene detected the cooling towers that spread the legionnaire's disease using prospective space-time permutation scan statistics from SaTScan.[50] In Singapore, a rogue Circle Line train was found using open government data. These show how smart governance can benefit from data science.

E-Governments

A United Nations (UN) e-government survey revealed that 90 countries provide public services online through one or more single-entry portals while another 148 provide at least one form of online transactional service. E-governance ensures that public institutions are inclusive, effective, and accountable to scrutiny,[51] which are also requirements for a smart city.

Bristol, a smart city in the U.K., allows residents to interact with the government via a single-entry portal. They can pay council taxes, fines, allotments and rent; order new trash bins and boxes; check for Christmas tree collection schedules; renew parking permits; report street issues and repairs; and other things that people used to go to the town hall for. This portal has improved the accessibility of public services and improved efficiency.

Many cities have mobile apps that enhance convenience. BOS:311 can, for instance, let a user send a photo of a road in need of repairs to authorities. These apps may require some form of personally identifiable information (PII) disclosure though.

Portals and apps have reduced barriers for people to access municipal services, encouraging civic engagement. Cities can leverage the data collected to improve decision making. However, the stakes are always higher when governments collect data. As such, excellent security policies are mandatory for e-governance to become viable. Unfortunately, this rarely happens. Taipei City's government site was, for instance, unintentionally crawled by Yahoo! Spiders, leaking the salary and bank account information of its employees.[52]

Apart from improving the cybersecurity of municipal sites, independent auditing and penetration testing of portals and apps are also critical to better protect residents' privacy and avoid incurring unnecessary costs. The screenshot below shows a 311 app that stores the Google API key in clear text, which allowed a hacker to use paid Google services courtesy of the City of Los Angeles.

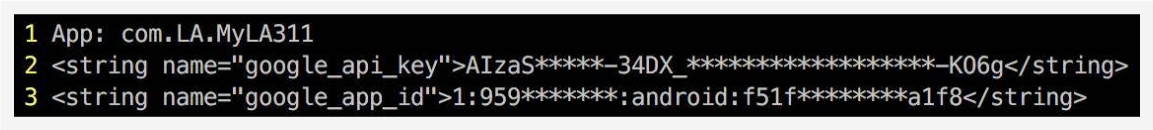


Figure 16. Google API key in clear text in MyLA311 app

Public Security Cameras

Public security or surveillance cameras are an inevitable part of smart governance. Many websites like Opentopia and Insecam list "public" cameras (using public IP addresses with no or default passwords).

Rio de Janeiro is a good example with its Orwellian "Center of Operations." On 80 screens, the government can monitor traffic and the weather from videos collected from 500 municipal cameras. More than 20 operators can access the videos remotely. Operators can easily zoom in on places where incidents occur aided by information from more than 30 government bodies, allowing the authorities to easily make decisions and act fast.

Figure 17. Centro de Operações Prefeitura do Rio

(Source: Facebook page of the center)

We are bound to see more municipal cameras installed worldwide even if not all of them will be connected to an operation center. New York has its Lower Manhattan Security Initiative since 2005, for instance. London has its "Ring of Steel" surveillance system even before Rio did.[53] Even without cameras, surveillance is made possible with smart streetlights in Kansas City. The lights can detect large gatherings of people, allowing the authorities to allocate police resources, if necessary.

The increasing number of surveillance equipment raises concerns on how adversaries can take advantage of them. IP cameras have been targeted by malware like Mirai in 2016[54] and will likely be easy prey for others in the future. As more cyber attacks target municipalities, we cannot simply assume that cameras will stay safe because they use local area networks (LANs). The risks are even greater if a center of operation—a single point of failure that collects and provides actionable intelligence—gets hacked.

Open Government Data

Open government data refers to government information proactively disclosed and made available online for everyone's access, reuse, and redistribution without restrictions. It promotes inclusive, effective, accountable, and transparent institutions, and improves the quality of their decision-making processes. This kind of data allows nongovernment organizations (NGOs) and the public to use and remix information to make more digestible and visualized interpretations, correlated with and hyperlinked to other data sets so people can better understand government actions that usually come under public scrutiny.

Efforts to promote and benefit from open government data are not limited to central governments. Municipalities also want to use open data and data science to improve the efficiency and effectiveness of their services. But like any publicly available data, the information can be maliciously used and abused by attackers. They can steal data for use in phishing and other fraudulent activities. Attackers can devise deanonymization techniques to recover anonymized data that do not follow set national standards like NIST 800-188, allowing them to trace actual people's whereabouts.[55]

What Threats Do Smart Cities Face?

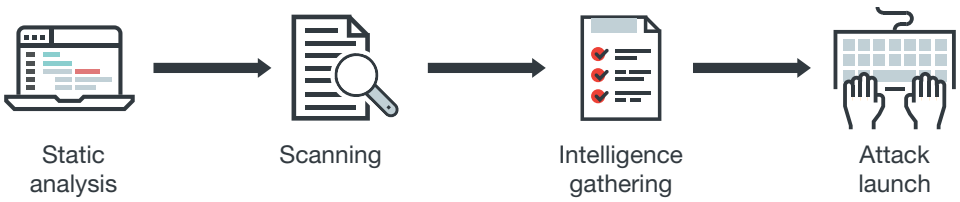
Since cities account for the consumption of around 70% of the energy produced globally and the generation of 70% of the world's gross domestic product (GDP),[56] any kind of intrusion, sabotage, and intelligence collection with malicious intent will have a great impact on smart cities.

In this section, we discussed who are likely to attack smart cities and what possible areas they can compromise.

Attacker Motivations and Steps

Attackers would set their sights on smart cities for a number of reasons. Malicious individuals may consider smart cities as playgrounds they can test their hacking skills on. They may toy with available technologies for personal satisfaction. For cybercriminals, the interconnectedness of devices and systems in a smart city can be a means to steal money and data from citizens and local enterprises. State-sponsored actors can also abuse the pervasiveness of smart city technologies to launch their own espionage or hacktivist campaigns. In very extreme cases, smart implementations may even be exploited for acts of terror.

Whatever motivations they have, threat actors would normally follow these steps when launching attacks:



Step 1: Static analysis: Using publicly available firmware, codes, and apps, they do a static analysis of devices and systems and see what vulnerabilities can be exploited.

Step 2: Scanning: Attackers do a scan of exposed systems and devices within the smart city so they can identify their targets or points of entry.

Step 3: Intelligence gathering: They gather any relevant information such as access credentials via phishing, data mining, and other means.

Step 4: Attack launch: Once attackers have all the components they need, they can perform several kinds of attacks. They can, for example, manipulate codes and processes, infect systems with malware, brick devices, and so on.

In the previous section, we noted how smart technologies are being used in critical infrastructure sectors. Below is a table that summarizes some of the possible attacks on each sector.

Critical Sector	Possible Attacks			
	Public Safety	Finance	Operations	Privacy
Energy	Cause instability in the city's power supply, affecting critical functions	Launch ransomware attacks on EMSs or steal energy	Disrupt EMS communications	Sniff smart meter data and steal citizen information
Transportation	Cause potential vehicular accidents	Exploit vulnerabilities to get free rides or hold vehicles hostage	Interrupt and manipulate transportation services	Compromise user data
Environment	Hack smart valves to cause wastewater overflow	Hold systems or devices hostage	Manipulate commands and impair system responses	Take advantage of sensors to track activity
Connectivity		Hold systems or devices hostage	Disrupt network communications causing downtime for connected systems	Intercept communications to sniff information and credentials
Governance		Hold systems or devices hostage	Hold systems or devices hostage; turn connected devices into bots	Gather intelligence on targets via surveillance feeds and open data

Table 1. Possible attacks on critical sectors

Risk Factors

A famous Dutch architect and urbanist once criticized that smart cities are "apocalyptic scenarios managed and mitigated by sensor-based solutions,"[57] reliance on which can lead to danger. Given the experimental nature of technologies used in smart cities, a smart city has been dubbed a "perpetual beta city."[58] This means things are eventually bound to go wrong at some point.

The security of a smart city very much depends on two key factors—the limitations of the technologies used and how they are implemented.

Technology Limitations

A number of smart devices are made lightweight, meaning they only have enough computing power to function as they are designed. Edge devices like switches and routers have very limited computing power, which makes encrypting them a challenge.

It is also inevitable for smart technologies—as with any device that runs on software—to get outdated. This is a serious concern when we consider how critical infrastructure rely on these technologies to function. Systems that run on legacy software will always be prone to attacks.

Poor Implementation

The brunt of a smart city's security risks falls on how smart technologies are implemented throughout it. How systems and devices are configured can dictate whether or not they are susceptible to attacks. Public-facing online platforms like app stores, for example, can be poisoned if not secured. Devices with open ports or factory-designed backdoors can be easily found and compromised. Given how many Internet-connected devices have publicly available code repositories and default credentials, unencrypted and poorly configured devices can be just as easy to abuse.

Firmware also come into play when thinking about the risks. Imagine the number of smart devices deployed throughout the city; without a proper and secure way of pushing updates to these said devices, they are left vulnerable to attacks.

10-Step Cybersecurity Checklist for Smart Cities

We delved into how smart technology implementations in critical sectors can be attacked. We also learned how the absence of well-defined security standards and regulations can turn projected benefits into unforeseen problems.

To guide smart city developers, we came up with a quick 10-step cybersecurity checklist they can refer to when implementing smart technologies.

1. Perform quality inspection and penetration testing.

Smart technologies have to undergo strict inspection and testing before any kind of city-wide implementation. This step allows the implementing body to catch any security issue (e.g., data leakage) or maintenance concern (e.g., service malfunction) before any smart device, infrastructure, or service is made available to the public.

Municipalities should hire independent contractors to run penetration tests on a regular basis. Since penetration testing only focuses on vulnerability scanning, standard product-testing procedures like quality assurance or testing should also be made mandatory. Quality assurance focuses on spotting defects in smart technologies while quality testing zooms in on their functionality.

2. Prioritize security in service-level agreements (SLAs) for all vendors and service providers.

Smart city adopters should draft SLAs that list the security criteria smart technology vendors and service providers need to meet. It should be clear to both parties that noncompliance to the specified conditions has corresponding penalties. The criteria could include a guarantee on the data privacy of citizens, a 24 x 7 response team in case of problems, or the abovementioned regular penetration testing and security audits.

3. **Establish a municipal computer emergency response team (CERT) or computer security incident response team (CSIRT).**

When any security incident involving smart implementations arise, a dedicated municipal CERT or CSIRT should be readily available to respond. The team needs to be adept at performing appropriate countermeasures in case of attacks or service recovery in case of system failures. It may also be in charge of vulnerability reporting and patching, vendor coordination, and sharing of best security practices.

4. **Ensure the consistency and security of software updates.**

Once software and firmware updates are available for devices used in smart cities, they should be deployed immediately. Both municipalities and vendors must make sure that updates are delivered in a secure manner—encrypted and digitally signed—to ensure software integrity. Digital signatures are used to verify if updates are authentic and not corrupted or tampered with before installation.

5. **Plan around the life cycle of smart infrastructure.**

Smart infrastructure have a longer service life than run-of-the-mill consumer products. However, it is important that municipalities create detailed procedures they need to take once the infrastructure become obsolete and vendor support for them ends. End-of-support may lead to serious vulnerabilities that can be exploited and attacked.

Smart city adopters should also consider the physical state of infrastructure. Years of deployment, lack of maintenance, and overuse can wear them out. By planning around infrastructure's life cycles, it will be easier for municipalities to fix or replace them in the future.

6. **Process data with privacy in mind.**

As a rule of thumb, any data collected in a smart city should be anonymized in order to protect the privacy of citizens, especially if it is going to be published as open government data. Access to sensitive data should be restricted to only those accredited by the municipality such as service providers who are bound by SLAs. A clear information-sharing plan should be in place. This should cover what data can be shared, to whom, and what privacy controls will be implemented for the data. The plan must also include data backup provisions and a recovery strategy in case of disasters.

7. **Encrypt, authenticate, and regulate public communication channels.**

All communications—both wired and wireless—should be protected against eavesdropping, interception, and modification, especially if they contain sensitive information. Strong cryptography should be used and encryption keys, well-kept and protected.

All smart communication systems should at least require an authentication token or session key to be accessed. Strong authentication mechanisms like one-time passwords, biometrics, and two- or multifactor authentication can be adopted to enhance security when citizens have to log in. Master, application, and session keys should be imposed in machine-to-machine (M2M) communications.

Unnecessary functions and features on smart communication systems should be disabled. This limits the attack surface and deters attackers from abusing them.

8. Always allow manual override.

Despite the allure of fully automated smart systems, keeping the manual override feature is still very important. In case of a serious system malfunction or compromise by a malicious actor, the feature offers municipalities the ability to perform incident response even if there is no Internet connection or the attacker locks out their remote access capabilities.

9. Design a fault-tolerant system.

When smart infrastructure and applications continue to operate properly even if one or more of their components fail, you have a fault-tolerant system. Smart city services may experience reduced response or performance but the system ensures continued functionality rather than failing completely. This will require redundancy techniques (hardware, software, and time) to tolerate operational faults and perform necessary functions.

10. Ensure the continuity of basic services.

In the unfortunate scenario where all systems fail, citizens should always have access to basic utilities (e.g., electricity and water) and services (e.g., emergency response). If the primary electric delivery system fails, for example, there has to be an alternative source of power.

Cities will get smarter over time. This is inevitable as governments slowly move toward techno-utopianism. Whether these cities are built from the ground up or around and over established metropolises, it is always important to balance functionality with security. Cities are created by citizens to meet their needs. It is only right to protect them.

Appendix

How Are Cities Around the World Getting "Smart"?

Smart city implementations reflect the way people in them perceive their daily needs. New York, for instance, provides gunshot alerts,[59] which do not exist in countries where owning weapons is not legal. Boston, meanwhile, puts greater emphasis on improving transportation and reducing CO2 emission.[60] Its mobile apps like BOS:311 and Commonwealth Connect[61] are popular among urban planners.

Smart cities are not limited to developed countries. China, for instance, had 386 smart cities as of 2015;[62] India had 329 projects in 60 cities, according to the web page of the Smart Cities Mission, Ministry of Urban Development;[63] Chişinău, Moldova just had a smart city hackathon in July 2016;[64] and grassroots open data projects take place in Africa, including "Map Kibera."[65]

We chose several cities to show various aspects of the smart city concept and discuss how smart infrastructure can be attacked. While technological deployment may not cover an entire smart city, we still listed the area and population of each city featured in this paper for reference.

City	Area (in Square Kilometers)	Estimated Population
Yokohama, Japan	433[66]	3,728,021 (2017)[67]
Songdo IBD, South Korea	6[68]	36,000 (2017)
Singapore	720[69]	5,766,316 (2017)[70]
Nijmegen, Netherlands	58[71]	170,000 (2017)[72]
Rotterdam, Netherlands	319[73]	617,000 (2017)[74]
Jaipur, India	485[75]	3,046,189 (2011)
Jun, Spain	3	3,500 (2016)[76]

Table 2. Cities featured in this paper

Yokohama

Yokohama is a port city developed in 1859 as a result of the Convention of Kanagawa in 1854. It is the second-largest city in Japan by population (3.7 million) with an area of 433sq. km. The Yokohama Smart City Project (YSCP) focuses on using EMSs. Yokohama was chosen by the Ministry of Economy, Trade and Industry (METI) in 2010 to pilot a "next-generation energy-social system." In 2013, it installed 4,200 HEMSs and 37MW solar panels, and used 2,300 EVs, translating to 39,000 tons in CO2 emission reduction.[77] Despite its discontinuation on 31 March 2015,[78] forums and seminars on it are still taking place.

Japan's National Policy Unit under the Cabinet Secretariat implemented the Green Policy in 2012[79] after the Great East Japan Earthquake that occurred on 11 March 2011. This policy demanded national energy security and efficiency such that:

- Renewable energy should account for one-third of the total power generation.
- 80% of greenhouse gases should be cut by 2050.
- Smart meters should be installed in homes and time-based rate programs to encourage energy efficiency should be introduced.
- The power generated by solar panels should be sellable to the grid.

To achieve these objectives, the Japanese government mandated that:

- New buildings and houses should comply with energy efficiency standards by 2020.
- New houses should become Net Zero Energy Buildings by 2020.
- HEMSs should be installed in all households by 2030.
- Fuel cells should be deployed in houses by 2016—1.4 million units by 2020 and 5.3 million units by 2030.
- 2 million EV charging stations must be installed by 2020, including 5,000 fast chargers.
- Fuel cell cars should go to market by 2015 and 100 hydrogen supply units should be installed.
- Smart meters should be installed in 80% of the total number of locations by 2016.
- The number of bulk power in-house complexes should reach 1 million households by 2020.

Yokohama uses a CEMS, HEMSs, building energy management systems (BEMSs), EVs, and battery SCADA systems.[80] In addition to energy efficiency, Yokohama aims to become a cultural, artistic, and emerging industrial business space with low CO2 emission; sufficient healthcare, social welfare, and child-rearing provisions; and environmental safety.[81]

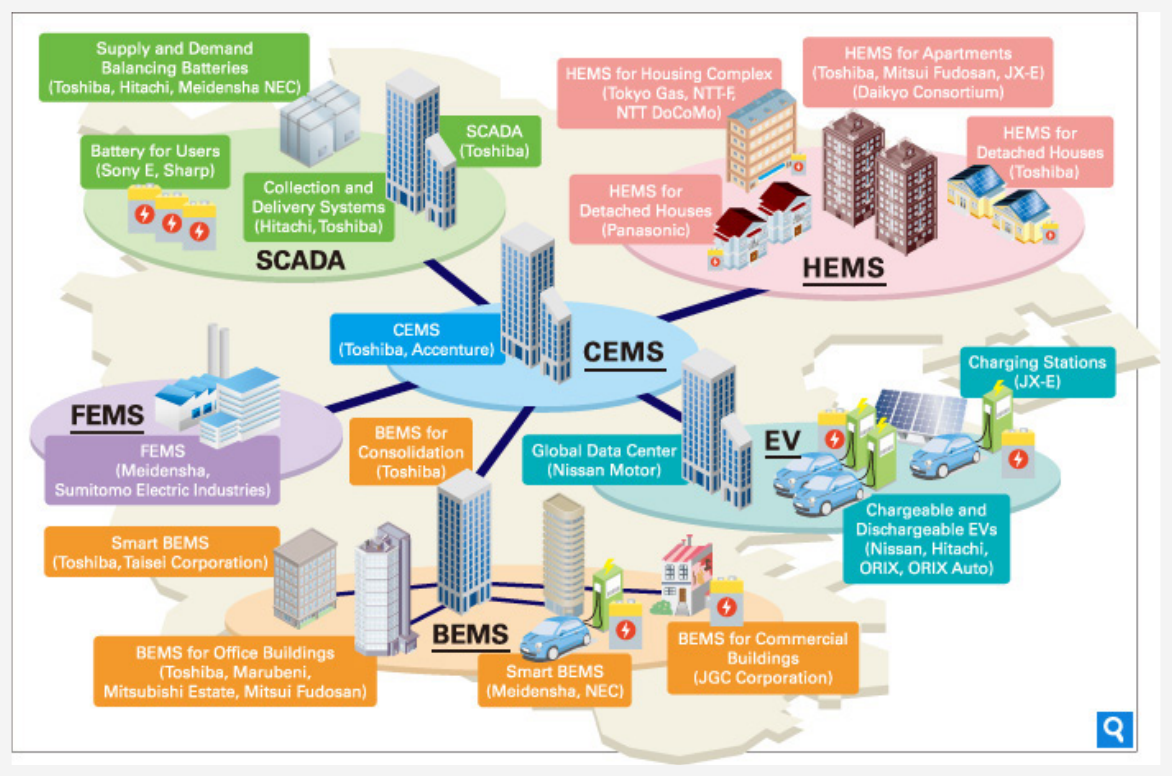


Figure 18. EMSs in Yokohama

(Source: http://www.city.yokohama.lg.jp/ondan/english/yscp/)

Yokohama's EMS ecosystem is complex and run via the CEMS, which coordinates with HEMSs, BEMSs, EVs, battery SCADA systems, and PV systems for peak shredding and shifting. Power consumption is measured by smart meters and uploaded to regional electricity utilities in real time. When consumptions peaks, the grid is optimized via demand-response commands broadcasted to the advanced metering infrastructure (AMI) and throttles it in contracted households and buildings. Yokohama uses a dispatchable demand response system that integrates reports for BEMSs (maximum 22.8% peak-cut) and HEMSs (15.2% peak-cut).

Yokohama residential areas accounted for 33% of the total energy consumption in 2014.[82] Water heating constituted 30% of the total consumption. To reduce energy use and CO2 emission, YSCP introduced HEMS use in existing houses and new buildings. HEMSs allow residents to keep track of their energy consumption, encouraging them to save power and spend less. HEMSs also allow throttling of high-power household appliances during peak hours, optimizing energy use.

Communication between the CEMS and BEMSs and HEMSs require VPN over Internet connection in Yokohama. AMI, meanwhile, communicates via power lines (power line communication; not used in YSCP), sub-1G radio connections,[83] fiber optics, Ethernet, and cellular data.

With the termination of YSCP in 2015, Route B service provision also ceased. This does not, however, mean that Japan gave up on smart energy. In fact, the Tokyo Electric Power Company (TEPCO) has been providing free Route B services to subscribers since July 2015.[84] The Kaisai Electric Power Company (KEPCO) also installed 6.5 million smart meters in October 2016.[85] Japan's overall smart meter installation rate is less than 40%, half its expected number. To help out, Tokyo Gas began selling household fuel cells known as "Ene·farm," which serves as an in-house power generation and heating unit.[86]

As new energy technologies emerge, Yokohama aims to deploy 40,000 household fuel-cell batteries, 2,000 fuel-cell cars, and 10 hydrogen stations for the upcoming Olympics,[87] in addition to EVs.[88, 89]

Songdo IBD

Songdo IBD lies right next to the Incheon International Airport, 56 km away from Seoul. As a "US$35-billion smart and sustainable city," Songdo IBD has been under construction since 2003 on 600 hectares of reclaimed land along the shores of the Incheon Free Economic Zone as the world's first smart[90] or "ubiquitous city" with smart infrastructure provided by U.Life Solutions.[91] The project is a joint venture of Gale International, POSCO E&C, and the city of Incheon. It also integrated Cisco products,[92] including 3,000 units of Cisco TelePresense® to provide real-time video communication means to residents.[93]

As the earliest smart city built from the ground up, Songdo IBD's goals have changed over time. Various completion dates have been given from 2014 to 2020. The city's population has also increased from 2,000 in 2009 to 36,000 in 2016. Some websites even reported as high as 90,000 registered residents in August 2015. Some 8,500 people live in First World Towers, a huge complex, 67 stories tall[94] though it is hard to come by hard figures.

A ubiquitous city is one "that provides ubiquitous city services at any time and in any place through a ubiquitous city infrastructure constructed by utilizing ubiquitous city technologies to enhance the competitiveness of the city and the quality of life therein."[95] Using RFID and the U.Life technologies, residents can use their citizen cards to ride the subway, pay for parking, see movies, borrow public bicycles, and so on. The cards are anonymous and therefore not linked to citizens' identities. If lost, owners can quickly cancel them and reset connected devices like door locks.[96]

Figure 19. U-Service concept

(Source: http://www.ulifesolutions.com/new/neweng/html/sub02_04.html)

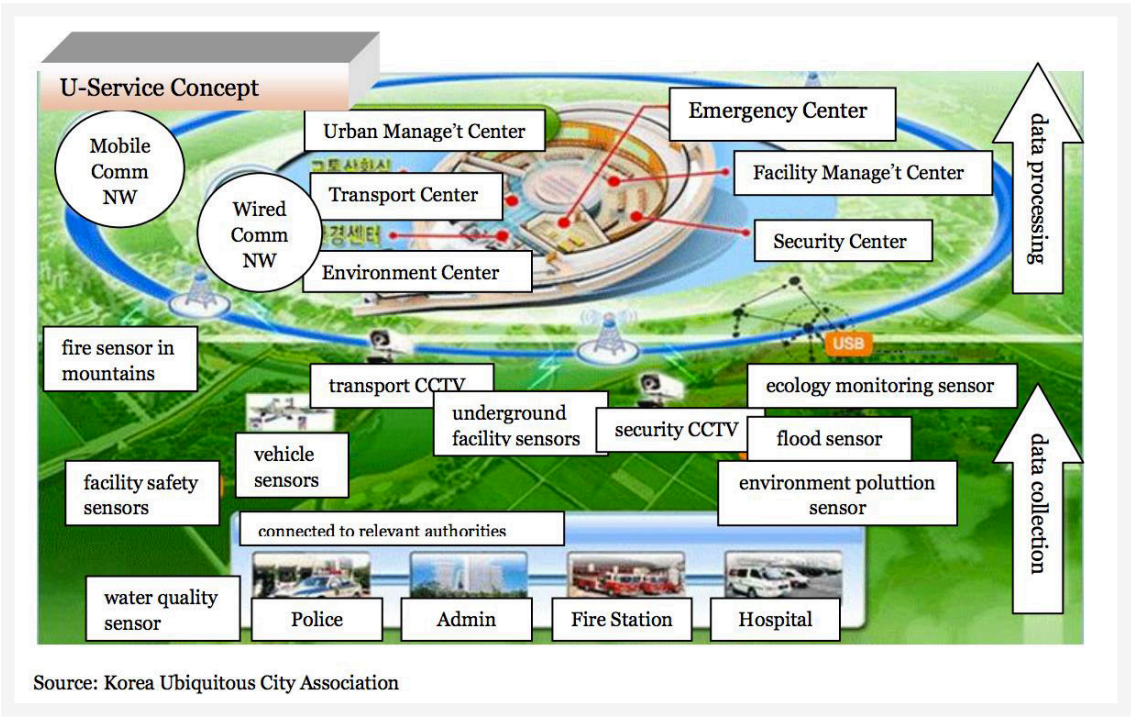


Figure 20. U-Service concept

(Source: https://www.tekes.fi/globalassets/global/ohjelmat-ja-palvelut/ohjelmat/ubicom/aineistot/raportit/korea/ubiquitouscityinkorea.pdf)

Sensors to monitor temperature, humidity, air pollution, and energy and water consumption are installed as part of U-Service. RFID tags on cars, meanwhile, are used to monitor traffic. Not only can the citizen cards open doors, they are also required for garbage disposal. CCTV cameras are omnipresent for security purposes. A pilot program hopes to use GPS-enabled bracelets to track children too, along with 228 service offerings to cover all aspects of citizens' lives.[97] The data generated by sensors and tags are processed for apps and can be used to further optimize city services.[98]

To attain sustainability, Songdo IBD has 106 Leadership in Energy and Environmental Design (LEED)-certified[99] buildings. The city separates fresh, sewage, and treated water. Natural gas is used to generate power and for heating.[100] About 40% of Songdo IBD is "green" with a 25-km bike lane. One of its most remarkable features is its pneumatic trash-collection system,[101] a centralized underground vacuum-powered tube system that sucks garbage to a central location, doing away with surface trash removal vehicles.

The technologies used to make Songdo IBD smart include near field communication (NFC)—both passive and active RFID; physical movement, gas, biometric, and infrared sensors; GPS; ultrasonic technology for 3D location recognition; 3D and CCTV cameras; smart cards; ubiquitous sensor network (USN) technology; ZigBee; Broadband Code Division Multiple Access (B-CDMA); and Bluetooth and mobile networks. These are no longer uncommon but were quite advanced in 2009. To process the data collected, RESTful web and location-based services (LBSs), along with context-aware technologies are used. Songdo IBD also uses standard protocols for data security, including Secure Sockets Layer (SSL), firewalls, public key infrastructure (PKI), and intrusion detection systems (IDSs), among others.

Songdo IBD uses typical configurations too. A U-Streetlight, for instance, has a CCTV camera, various sensors, a ZigBee module, and a wireless access point installed. The local government controls these and wireless Internet access via CDMA. Street surveillance relies on CCTV and IP cameras connected to the Urban Management Center (UMC). The UMC is also connected to police headquarters and security providers, along with other service providers (calamity responders, pedestrian support providers, parking lot owners, etc.). Its centralized architecture is similar to Rio de Janeiro's Centro de Operações.[102]

Singapore

Singapore announced its plan to build a Smart Nation on 24 November 2014. As such, Singapore hopes to become "a nation where people live meaningful and fulfilled lives, enabled seamlessly by technology, offering exciting opportunities for all."[103] The country envisions huge endeavors until 2025, including but not limited to the following domains:[104]

- Big data analysis
- IoT

- Cybersecurity and trustworthy systems
- Digital harbor
- Data marketplaces and data as a service
- Urban logistics, including goods shipped from shopping malls
- Creators' space that encourages risks and innovation
- Smart health assistance

The Smart Nation plans are being executed by several government entities. The National Research Foundation initiated the Research, Innovation and Enterprise 2020 (RIE2020) Plan for advanced manufacturing and engineering, urban solutions and sustainability, and services and digital economy.[105] The total investment is expected to reach US$13.6 billion, 5% of which will be allocated to urban solutions. The Infocomm Development Authority (IDA), meanwhile, is building a Smart Nation Platform (SNP)[106] that collects data from sensor networks then analyzes the information and shares insights with public and private partners. A dedicated website (http://www.smartnation.sg/) also delivers information, documents, and more than 20 mobile apps to citizens while another site (https://data.gov.sg/) makes government data available to the public.

RIE2020 also proposes to enhance the living environment and address resource constraints within urban mobility solutions, including public transport, self-driving vehicles, urban logistics, cycling and walking, car sharing, on-demand mobility, as well as livable spaces, smart grids, water treatment, and seawater desalination. A dynamic 3D city model with semantics called "Virtual Singapore" was designed for virtual experimentation and test-bedding, planning and decision-making, research and development, and other whole-of-government (WOG) projects will be made ready this year.[107]

On-demand mobility is a component of Smart Nation. It is enabled by Beeline,[108] a mobile app that users can download for both Android and iOS. It helps commuters book seats on private bus lines and allows them to choose the routes they wish to take.[109] News routes can be created by crowd-sourcing. nuTonomy, n MIT spin-off start-up company, also chose Singapore to deliver the world's first public, self-driving taxi.[110]

Beeline users who are also Singtel subscribers who wish to book bus seats while on the go can use Wireless@SG. Connectivity is maintained via the Heterogeneous Network (HetNet) trial, making the Info-communications Media Development Authority (IMDA)'s E3A vision—connect everything, everyone, everywhere all the time—a reality.[111]

Connectivity via the SNP forms the basis of nationwide sensor networks built with Aggregation Gateway or Above Ground (AG) Boxes. An AG Box aims to provide connectivity to shared sensors via Wi-Fi and CAT-5 Ethernet and transmits the data received to the Smart Nation OS (SN-OS), which provides actionable

insights. The sensors comprise security cameras; air quality monitors; temperature, humidity, and traffic sensors; and speed detectors. An advanced video-sensing technology which detects people smoking in prohibited areas, for instance, also serves to measure the length and flow of taxi queues. This kind of data can alert taxi companies to send more units or commuters to take the bus instead if they are in a hurry.[112]

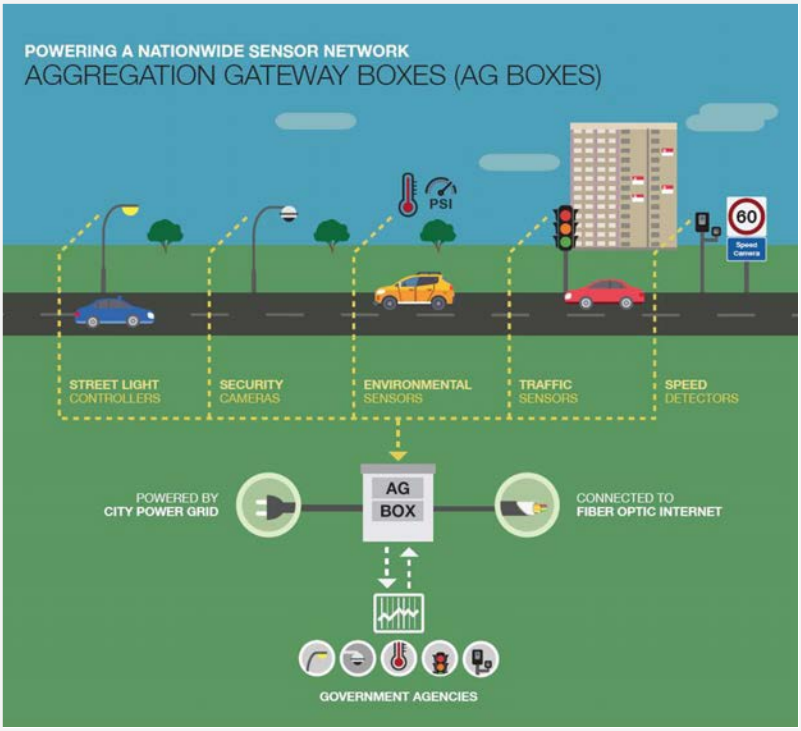


Figure 21. Functional description of an AG Box

(Source: http://www.mci.gov.sg/~/media/data/mci/docs/imm%202025/infocomm%20media%202025%20full%20report.pdf)

IMDA began IoT field trials for smart homes in 2016 in domains like elderly care, chronical disease management, obesity, home energy management, and assisted living. All of the devices are Internet accessible and more than 20 smartphone apps that use publicly available government data have been made available in Google Play and iTunes App Store, including:

- **HealthHub:** Provides personalized health records.
- **myENV:** Provides Pollutant Standard Index (PSI), dengue hotspot, and weather data.
- **myTransport.SG:** Provides bus arrival times, journey planners, and other transport information.
- **OneInbox:** Allows the receipt of government letters.
- **Beeline:** Lets users to book seats in private bus lines and suggest new routes.
- **One Historical Map:** Serves as a geo-historical map.
- **OneService:** Lets users report municipal issues.

In addition to highly integrated mobile apps, data.gov.sg also provides conventional statistical data like population by gender and birth rate; economic data like GDP, job vacancy rates, and consumer price index (CPI); and environmental and municipal data like real-time PM 2.5 readings (air pollution). Real-time data is particularly useful for citizens to know when to stay indoors, for instance, to avoid pollution. Third-party app developers can also use publicly available government data to create location-based services. Data from the SNP can also be used by businesses to create smarter, more productive, and more competitive services, powering the country's economic growth.

Netherlands

Amsterdam boasts of an innovation ecosystem (https://amsterdamsmartcity.com/) where ideas, projects, and products are categorized and made accessible to all site visitors. Outside it, however, three other smart cities can be found in the Netherlands—Nijmegen, Rotterdam, and ReGen.

Nijmegen

Nijmegen, the oldest city in the Netherlands, implemented Smart Emission, a joint project of the municipality and Radboud University, in January 2016. Smart Emission aims to monitor, visualize, and communicate fine-grained "environmental footprints" of the city in real time. As such, an innovative set of low-cost outdoor sensors and a related Open Geo Data infrastructure were developed.[113]

Intemo, a Dutch company, designed a waterproof multisensor device called "Jose" for the project. Jose is connected to household Wi-Fi access points that send data to CityGIS servers. This data is then uploaded to the Geonovum Server for distribution to users, apps, and data analysts. Real-time data, including on air quality, noise, humidity, and air pressure are visualized on a map in the Smart Emission portal (http://smartemission.ruhosting.nl/) or browsed with the Heron Viewer or SOSViewer. Sample Smart Emission data and source code are available on GitHub.[114] The data collected is publicly available and accessible via the OGC Sensor Observation Services (SOS) API[115] or can be downloaded using a command line tool.[116]

Figure 22. Jose by Intemo

(Source: http://smartemission.ruhosting.nl/wordpress/wp-content/uploads/2016/04/presentatie_smartemission_ru_sgs_21januari2016_lc_ck_v14_voorsgs.pdf)

Jose is an outdoor device that monitors nitrogen dioxide (NO2), carbon oxide (CO), CO2, and ozone (O3) emissions; tilting; sound pressure; barometer readings; humidity; temperature; light intensity; air color; GPS location; and rainfall. The data collected is sent to the so-called "Jose input service" in CityGIS in encrypted binary form.[117]

As a pilot project with limited deployment, Smart Emission prioritized transparency and "democratization," thus posing important questions such as:[118]

- Can cheap sensors add value to existing air quality sensors?
- Does the concept of citizen-sensor-network work?
- Does the idea open a new opportunity for environmental-information-aware urban policies?

Nijmegen is not the only city seeking for answers.

Rotterdam

Two-thirds of the Netherlands is vulnerable to flooding. Rotterdam, its second-largest city, is 6m below sea level and so is protected by dikes and a complicated pumping system with extended pipes underground. Though the city has not suffered from extreme flooding from 2002 to 2009, severe incidents (August 2010 and June 2016) recently damaged it. A man was, for instance, electrocuted and died in his flooded cellar on 23 June 2016.[119] That same day, displays and rare books were evacuated from Boijmans Van Beuningen Museum as excess rainfall caused water and sewage to seep into its basement.[120]

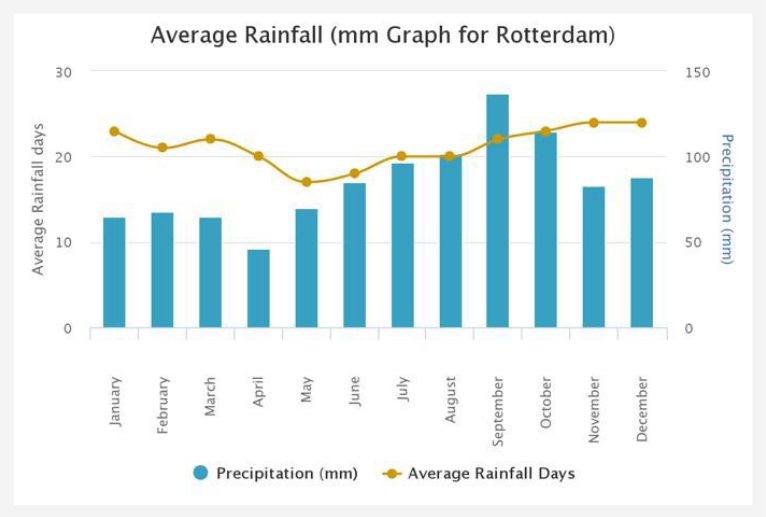


Figure 23. Precipitation levels and rainfall days in Rotterdam from 2002 to 2012

(Source: https://www.worldweatheronline.com/rotterdam-weather-averages/south-holland/nl.aspx)

To address issues caused by extreme downpour and extended periods of drought, the city proposed the Rotterdam Climate Initiative. Green roofs and flood-control water plazas, along with a children's playground that stores up to 1 million liters of water[121,122] were built as small-scale facilities that will act as "sponges" for the city. Multifunction car parks with huge underground water storage could also be used to save rainfall during dry months.[123] One such underground tank with a 10-million liter capacity was constructed below Museumpark.

The Rotterdamse Regenradar under RainGain is a pilot project of SBS6.[124] It measures rainfall for accurate water management with a 9.3-9.5 GHz X-Band radar installed on the roof of Delftse Poort. The radar has a 30-meter spatial resolution and a scan interval of 1 minute.[125] Data from the radar is combined with information from the C-Band radar of Meteorological Service (KNMI) and a series of rain gauges with 0.2mm resolution that sample data every minute.[126] The data answers how much rain has fallen and where, enabling the municipality and the water board to smartly control water in playgrounds and underground water tanks or pump it out to Nieuwe Waterweg.

ReGen

ReGen is an off-grid capable village designed by EFFEKT, a Danish architecture company. Contracted with Almere, Netherlands, the company plans to build the first pilot village with 25 houses this year,[127] in hopes of creating a self-contained living space that recycles waste, produces its own energy and food, emits no pollution, and does not depend on outside resources. It involves 75–100 villagers on a piece of land that measures 15,450sq. m that houses homes, greenhouses, aquaponics, seasonal gardens, livestock, solar cells, water storage, community houses, social spaces, infrastructure, and electric car spots.[128]

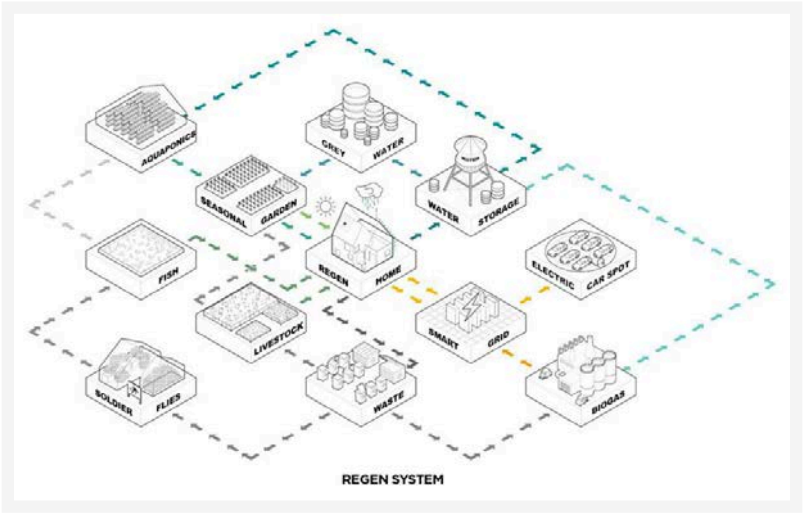


Figure 24. Facilities in a ReGen village

(Source: http://www.effekt.dk/regenvillages/)

The technologies used to create the village are not fully described to date, except for the solar panels, biogas power system, smart grid, waste recycling plant, and water harvester,[129] which coordinate with each other via smart technologies. Networking is required, after all, to pump water for irrigation, automatically control the biogas factory, and connect solar panels to electric cars.

Jaipur

Jaipur was elected as one of the first 20 cities for smart "makeover" in January 2016. Being the "Pink City of India," it is part of an initiative that Prime Minister Modi announced, which covers the creation of 100 smart cities in India by 2022.[130] It is also one of the "lighthouse cities"[131] that Cisco provided with routers and access points that enable Wi-Fi hotspots and video surveillance cameras, in addition to interactive kiosks, remote access government services (REGSs), and parking management systems from the Jaipur Development Authority (JDA).[132, 133]

Jaipur is a historical city visited by 40 million tourists a year. From polls, the most concerning issues raised include transportation and mobility, heritage and tourism, and solid waste and wastewater management.[134] Currently deployed digital infrastructure include:

- 17 interactive kiosks that offer maps to shop locations and parking lots and free mobile phone charging services
- 30 public Wi-Fi portals
- 22 surveillance cameras (plus 15 to be deployed and 10 proposed)
- 2 remote access government services (REGSs and two more to be deployed)
- Rooftop solar power plant[135]
- Real-time information display in Bus-Q-Shelter

Online citizen services like name transfers/substitutions and one-time lease certificate issuance are available on Jaipur Development Authority (JDA)'s web page. The city also proposed a City Infrastructure Management Center (CIMC) and a Response Control Room to deal with security incidents, along with 5,000 programmable and remote-controllable light poles, smart meters, public bikes, and so on.

Jaipur is a special case because of its strong intention to engage citizens before implementation. It uses dedicated website, an official Facebook account, a Twitter account, WhatsApp, and SMS Poll, in addition to face-to-face meetings, consolations, lectures, and seminars to reach out to citizens.[136] Implementation plans, indicators, targets, and resources are also clearly defined. We also saw night markets and eco-friendly, aromatic mist spray corridors in the plans, which widened the definition of the smart city to better fit its social context.

China

China is the third-largest country in the world with 1.4 billion people of multiple ethnic groups, hence the strong diversity in its smart city plans. It intends to integrate "four modernizations" in the fields of agriculture, industry, national defense, and science and technology into the construction of 386 smart cities, bringing a certain degree of unanimity among them. The National Development and Reform Commission (NDRC) requires smart cities to use IoT, cloud computing, big data, and GISs to improve public services, city management, environment, infrastructure, and Internet security.[137]

Chinese cities have high population densities. As such, smart solutions for sparsely populated cities like smart streetlights do not apply while solutions for megacities like smart energy and transportation do. Mobile apps developed by state-owned or private companies dedicated for a single purpose are widely used and play a major role. None of the macro-architectures are designed from scratch as in Songdo IBD. Plans for massive power grid adjustments like that addressed by the demand-response system in

Yokohama are being tested, though apps for monitoring electricity use, accessing public transportation, and giving directions to car drivers do. Apps to easily access Union Pay and Alipay for bill payments abound too. Some apps can be used in as many as 26 provinces and municipalities.

State Grid Corporation of China (SGCC) and China Southern Power Grid Co., Ltd. (CSG) installed more than 90 million smart meters in 2015.[138] An SGCC subsidiary also designed Zhangshang Dianli, an app that runs on both iOS and Android to provide various services, and is available in 21 out of 23 provinces. To serve elder citizens and people who have more than one meter, one user can access up to five accounts (allowing the user to pay the bills of relatives).

Local and municipal governments work with one or more companies for mobile apps that provide access to government services. Zhangshang Lulutong, for instance, is an iOS app that provides traffic information in Tianjin. Drivers can check for and pay unpaid fines with it as well as report infringements to the authorities. It also allows them to access cameras installed at intersections to see how heavy traffic is. Apps like Chelaile, meanwhile, provides real-time bus and metro information in all major cities. Special-purpose apps for healthcare like Menzhendating, which helps people set doctor appointments in more than 700 hospitals, also exist.

Private companies have also invested in developing apps that provide real-time parking space information, helping drivers find nearest available spots without the aid of smart sensors. Shared bicycles are operated by some municipal governments and private companies like Mobike and Ofo.

Huge investments from private companies do not imply lack of public sector funding though. Some 90% of the roads in Wuhan, for instance, have CCTV and IP cameras installed.[139] Hangzhou, the Alibaba Group's base city, meanwhile, initiated City Brain[140] to address traffic issues. Cameras will be used to gather inputs and create algorithms to optimize and control traffic lights, raising the average driving speed by 3–5%. It will use Ali's OS, Apsara, to process inputs from public sensors, including more than 50,000 cameras, for real-time analysis and resource dispatching. It will then be extended to uses in tourism, water management, and the creation of an artificial intelligence (AI) city.[141]

Urban planners initiated the Urban Data Lab, which collects government data, existing urban plans, mobile phone metadata from carriers, and behavioral data from location-based services obtained by third parties to analyze and determine the citizens' spatial behaviors within a city.[142] Though the analysis is unrelated to smart city hardware, its use of big data can be seen as an example of smart city governance. By observing departure and arrival data, the planners can distinguish between people who work in technological parks and those who only work part-time. They can also calculate commute times and recreational patterns, which can help city officials make more reasonable city plans and policies.

Jun

Jun is the first village that is totally run via social media, particularly Twitter. Citizens can report crime and broken streetlights, set doctors' appointments, and interact with the police and their mayor via the government's Twitter accounts[143]—@AyuntamientoJun (Jun government), @PoliciaJUN (local police), @BiblioJun (library), @EducacionJun (Department of Culture and Education), and @JoseantonioJun (the mayor).

Although Jun is not a typical smart city with smart infrastructure, it does show a new paradigm—how ICT can improve public service provision.

References

1. VINCI Energies. (24 August 2015). *YouTube.* "What Is a Smart City?" Last accessed on 12 April 2017, https://www.youtube.com/watch?v=Br5aJa6MkBc.

2. British Standards Institution. (2014). "Smart Cities—Vocabulary." Last accessed on 12 April 2017, http://shop.bsigroup.com/upload/PASs/Free-Download/PAS180.pdf.

3. ISO/IEC. (2015). "Smart Cities: Preliminary Report 2014." Last accessed on 12 April 2017, https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/smart_cities_report-jtc1.pdf.

4. Rida Khatoun and Sherali Zeadally. (2016). *Communications of the ACM.* "Smart Cities: Concepts, Architectures, Research Opportunities." Last accessed on 12 April 2017, https://cacm.acm.org/magazines/2016/8/205032-smart-cities/abstract.

5. Andrea Caragliu, Chiara Del Bo, and Peter Nijkamp. (2009). "Smart Cities in Europe." Last accessed on 12 April 2017, http://www3.ekf.tuke.sk/cers/cers2009/PDF/01_03_Nijkamp.pdf.

6. Robert G. Hollands. (26 November 2008). *Taylor & Francis Online.* "Will the Real Smart City Please Stand Up?" Last accessed on 12 April 2017, http://www.tandfonline.com/doi/abs/10.1080/13604810802479126.

7. The Economist Newspaper Limited. (27 October 2012). *The Economist.* "Open-Air Computers." Last accessed on 12 April 2017, http://www.economist.com/news/special-report/21564998-cities-are-turning-vast-data-factories-open-air-computers.

8. United Nations. (2009). "World Population Prospects: The 2008 Revision—Highlights." Last accessed on 12 April 2017, http://www.un.org/esa/population/publications/wpp2008/wpp2008_highlights.pdf.

9. United Nations. (2015). "World Urbanization Prospects." Last accessed on 12 April 2017, https://esa.un.org/unpd/wup/Publications/Files/WUP2014-Report.pdf.

10. Ian Johnson. (15 June 2013). *The New York Times.* "China's Great Uprooting: Moving 250 Million into Cities." Last accessed on 12 April 2017, http://www.nytimes.com/2013/06/16/world/asia/chinas-great-uprooting-moving-250-million-into-cities.html?pagewanted=all&_r=0.

11. Navigant Consulting Inc. (2016). *Navigant Research.* "Smart Cities—Smart Technologies and Infrastructure for Energy, Water, Mobility, Buildings, and Government: Global Market Analysis and Forecasts." Last accessed on 12 April 2017, https://www.navigantresearch.com/research/smart-cities.

12. Cisco. (2009). *The Network.* "Cisco Unveils 'Intelligent Urbanization' Global Blueprint." Last accessed on 12 April 2017, https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=4767464.

13. The White House Office of the Press Secretary. (26 September 2016). *The White House.* "Fact Sheet: Announcing Over $80 Million in New Federal Investment and a Doubling of Participating Communities in the White House Smart Cities Initiative." Last accessed on 12 April 2017, https://obamawhitehouse.archives.gov/the-press-office/2016/09/26/fact-sheet-announcing-over-80-million-new-federal-investment-and.

14. U.S. Department of Energy. (7 March 2013). *EIA*. "Heating and Cooling No Longer Majority of U.S. Home Energy Use." Last accessed on 19 April 2017, http://www.eia.gov/todayinenergy/detail.php?id=10271.

15. Ministry of Economy, Trade and Industry. (2016). *Agency for Natural Resources and Energy*. "Section 2 Trends in Energy Consumption by Category." Last accessed on 19 April 2017, http://www.enecho.meti.go.jp/about/whitepaper/2016html/2-1-2.html.

16. The City of New York. (2017). *NYC Environmental Protection*. "About Automated Meter Reading (AMR)." Last accessed on 19 April 2017, http://www.nyc.gov/html/dep/html/customer_services/amr_about.shtml.

17. Ariel Bleicher. (5 October 2010). *IEEE Spectrum*. "Privacy on the Smart Grid: Are Smart Meters Spies? They Don't Have to Be." Last accessed on 10 May 2017, http://spectrum.ieee.org/energy/the-smarter-grid/privacy-on-the-smart-grid.

18. Liu, Jingjun. (24 October 2016). *Economic Daily News*. "劉靜君. 智慧電表17組高手過招抓漏 (Smart Meter: Pentested by 17 Teams)." Last accessed on 19 April 2017, http://money.udn.com/money/story/5635/2042739.

19. Karen Ehrhardt-Martinez, Kat A. Donnelly, and John A. Laitner. (June 2010). "Advanced Metering Initiatives and Residential Feedback Programs: A Meta-Review for Household Electricity-Saving Opportunities." Last accessed on 24 April 2017, http://aceee.org/sites/default/files/publications/researchreports/e105.pdf.

20. Morooka, Kenichiro. (27 July 2016). "師岡健一郎. スマートメーターとECHONET Liteで通信できるようになるまで (Until You Can Communicate with Smart Meter with ECHONET Lite)." Last accessed on 19 April 2017, http://route-b.iij.ad.jp/archives/128.

21. Department of Homeland Security. (6 December 2016). *ICS-CERT*. "Advisory (ICSA-16-231-01) Locus Energy LGate Command Injection Vulnerability." Last accessed on 19 April 2017, https://ics-cert.us-cert.gov/advisories/ICSA-16-231-01-0.

22. Dan Goodin. (27 January 2016). *Ars Technica*. “Israel’s Electric Authority Hit by ‘Severe’ Hack Attack.” Last accessed on 19 April 2017, http://arstechnica.com/security/2016/01/israels-electric-grid-hit-by-severe-hack-attack/.

23. Banerjee & Associates. (August 2003). “An Overview of Common Parking Issues, Parking Management Options, and Creative Solutions.” Last accessed on 19 April 2017, http://pipta.org/wp-content/uploads/2014/04/Parking-Problems-and-Creative-Solutions.pdf.

24. Karashima, Hiroko. (25 November 2016). BusinessNetwork.jp. “唐島明子. ソフトバンクが*NB-IoT*活用したスマートパーキング実証実験を公開 (SOFTBANK Publishes the Experiment of Smart Parking Using NB-IoT).” Last accessed on 19 April 2017, http://businessnetwork.jp/Detail/tabid/65/artid/4992/Default.aspx.

25. Samuel Gibbs. (28 November 2016). *The Guardian*. “Ransomware Attack on San Francisco Public Transit Gives Everyone a Free Ride.” Last accessed on 19 April 2017, https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware.

26. City of Groningen. (21 July 2010). “Smart Cities Project Initiation Document.” Last accessed on 19 April 2017, http://www.smartcities.info/files/Project_Initiation_Document_WP_4_Groningen_public_transport_planner.pdf.

27. Heather Ishimaru. (22 November 2013). *ABC 7 News*. “Computer Tested Again in BART Tech Problem.” Last accessed on 19 April 2017, http://abc7news.com/archive/9335794/.

28. Chris Williams. (27 November 2016). *The Register*. “Passengers Ride Free on SF Muni Subway After Ransomware Infects Network, Demands $73K.” Last accessed on 19 April 2017, http://www.theregister.co.uk/2016/11/27/san_francisco_muni_ransomware/.

29. Michael Szell. (6 November 2012). “hubcab: A Network-Based Improved Urban Taxi Service.” Last accessed on 19 April 2017, http://senseable.mit.edu/urbancode/slides/Onmobility/MichaelSzell.pdf.

30. *HubCab*. “Exploring New York City Taxi Trails and Sharing Our Way to a More Sustainable Urban Future.” Last accessed on 19 April 2017, http://hubcab.org.

31. Gurgaon. (5 September 2015). *The Economist*. “Streetwise.” Last accessed on 19 April 2017, http://www.economist.com/news/international/21663219-cities-are-starting-put-pedestrians-and-cyclists-motorists-makes-them?frsc=dg%7Cc.

32. Sean O’Kane. (3 August 2016). *The Verge*. “Gogoro Starts an Electric Scooter-Sharing Program in Berlin.” Last accessed on 19 April 2017, http://www.theverge.com/2016/8/3/12358280/gogoro-electric-scooter-sharing-app-berlin-taiwan.

33. GD and CSC. (22 July 2016). “Challenge of BLE Certification Mechanism Design: Take Gogoro Smart Scooter as an Example.” Last accessed on 24 April 2017, https://hitcon.org/2016/CMT/slide/day1-r0-a-1.pdf.

34. Smarter Cambridge Transport. (2017). *Smarter Cambridge Transposrt*. “Smart Traffic Management.” Last accessed on 19 April 2017, http://www.smartertransport.uk/smart-traffic-management/.

35. Imtech Traffic and Infra UK Ltd., Siemens Traffic Controls and TRL Limited. (2000–2014). *SCOOT Systems*. “How SCOOT Works.” Last accessed on 19 April 2017, http://www.scoot-utc.com/DetailedHowSCOOTWorks.php.

36. Keith Barry. (11 September 2014). *From the Atlantic Citylab*. “The Traffic Lights of Tomorrow Will Actively Manage Congestion.” Last accessed on 19 April 2017, http://www.citylab.com/commute/2014/09/the-traffic-lights-of-tomorrow-will-actively-manage-congestion/379950/.

37. Branden Ghena, William Beyer, Allen Hillaker, Jonathan Pevarnek, and J. Alex Halderman. “Green Lights Forever: Analyzing the Security of Traffic Infrastructure.” Last accessed on 24 April 2017, https://jhalderm.com/pub/papers/traffic-woot14.pdf.

38. Tobias Franke, Paul Lukowicz, and Ulf Blanke. (22 December 2015). *Springer Open*. “Smart Crowds in Smart Cities: Real Life, City-Scale Deployments of a Smartphone-Based Participatory Crowd Management Platform.” Last accessed on 19 April 2017, https://jisajournal.springeropen.com/articles/10.1186/s13174-015-0040-6.

39. *Worldwide Air Quality Monitoring Data Coverage*. Last accessed on 19 April 2017, https://aqicn.org/sources/.

40. Franck Lavigne, Patrick Wassmer, Christopher Gomez, Thimoty A. Davies, Danang Sri Hadmoko, T. Yan W.M. Iskandarsyah, J.C. Gaillard, Monique Fort, Pauline Texier, Mathias Buon Heng, and Indyo Pratomo. (24 December 2014). *Springer Open*. “The 21 February 2005, Catastrophic Waste Avalanche at Leuwigajah Dumpsite, Bandung, Indonesia.” Last accessed on 19 April 2017, https://geoenvironmental-disasters.springeropen.com/articles/10.1186/s40677-014-0010-5.

41. George Asimakopoulos, Sotiris Christodoulou, Andreas Gizas, Vassilios Triantafillou, Giannis Tzimas, John Gialelis, Artemios G. Voyiatzis, Dimitris Karadimas, and Andreas Papalambrou. (May 2015). “Architecture and Implementation Issues, Toward a Dynamic Waste Collection Management System.” Last accessed on 19 April 2017, http://www.www2015.it/documents/proceedings/companion/p1383.pdf.

42. Ellinor Mills. (18 November 2011). *CNet*. “Hacker Says He Broke into Texas Water Plant, Others.” Last accessed on 19 April 2017, https://www.cnet.com/news/hacker-says-he-broke-into-texas-water-plant-others/.

43. Piers O'Hanlon and Ravishankar Borgaonkar. (3 November 2016). "Wi-Fi-Based IMSI Catcher." Last accessed on 19 April 2017, https://www.blackhat.com/docs/eu-16/materials/eu-16-OHanlon-WiFi-IMSI-Catcher.pdf.

44. David Perez and Jose Pico. (18 January 2011). "A Practical Attack Against GPRS/EDGE/UMTS/HSPA Mobile Data Communications." Last accessed on 19 April 2017, https://media.blackhat.com/bh-dc-11/Perez-Pico/BlackHat_DC_2011_Perez-Pico_Mobile_Attacks-wp.pdf.

45. Mihai Costache and Valentin Tudor. (December 2011). "Security Aspects in the AMI." Last accessed on 25 April 2017, http://publications.lib.chalmers.se/records/fulltext/154814.pdf.

46. Tobias Zillner and Sebastian Strobl. (August 2015). "ZigBee Exploited: The Good, the Bad, and the Ugly." Last accessed on 25 April 2017, https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly.pdf.

47. Li, Jun and Yang Qing. (May 2015). "I'm a Newbie Yet I Can Hack ZigBee." Last accessed on 25 April 2017, https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/DEFCON-23-Li-Jun-Yang-Qing-I-AM-A-NEWBIE-YET-I-CAN-HACK-ZIGBEE.pdf.

48. KPN. (30 June 2016). *KPN*. "The Netherlands Has First Nationwide LoRa Network for IoT." Last accessed on 19 April 2017, https://corporate.kpn.com/press/press-releases/the-netherlands-has-first-nationwide-lora-network-for-internet-of-things-.htm.

49. He, Shichang. (13 January 2016). *Liberty Times*. "何世昌. 自由時報. 北市首創城市級「IoT實驗平台」(Taipei's Innovation on City-Level 'IoT Experimental Platform).'" Last accessed on 19 April 2017, http://news.ltn.com.tw/news/life/breakingnews/1570935.

50. Sharon K. Greene, Eric R. Peterson, Deborah Kapell, Annie D. Fine, and Martin Kulldorff. (2016). *CDC*. "Daily Reportable Disease Spatiotemporal Cluster Detection, New York City, New York, USA, 2014–2015." Last accessed on 19 April 2017, https://wwwnc.cdc.gov/eid/article/22/10/16-0097_article.

51. United Nations Department of Economics and Social Affairs. (2016). *UN E-Government Knowledge Database*. "UN E-Government Survey 2016." Last accessed on 19 April 2017, https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2016.

52. Apple Daily News (10 January 2017). "蘋果日報. 北市資訊局：薪資報表暫存檔遭「爬蟲」程式「爬走」(Taipei City Department of Information Technology: Payroll Table in Temporary File 'Crawled' by 'Crawler.')" Last accessed on 19 April 2017, http://www.appledaily.com.tw/realtimenews/article/new/20170110/1032463/.

53. Heather Kelly. (26 April 2013). *CNN*. "After Boston: The Pros and Cons of Surveillance Cameras." Last accessed on 19 April 2017, http://edition.cnn.com/2013/04/26/tech/innovation/security-cameras-boston-bombings/.

54. Trend Micro. (26 October 2016). *TrendLabs Security Intelligence Blog*. "The IoT Ecosystem Is Broken. How Do We Fix It?" Last accessed on 19 April 2017, http://blog.trendmicro.com/trendlabs-security-intelligence/internet-things-ecosystem-broken-fix/.

55. James Siddle. (10 April 2014). *The Variable Tree*. "I Know Where You Were Last Summer: London's Public Bike Data Is Telling Everyone Where You've Been." Last accessed on 25 April 2017, https://vartree.blogspot.com/2014/04/i-know-where-you-were-last-summer.html.

56. International Electrotechnical Commission. (2016). "Smart Cities." Last accessed on 12 April 2017, http://www.iec.ch/about/brochures/pdf/technology/smartcities.pdf.

57. Rem Koolhaas. (24 September 2014). *European Commission*. "My Thoughts on the Smart City." Last accessed on 12 April 2017, http://ec.europa.eu/archives/commission_2010-2014/kroes/en/content/my-thoughts-smart-city-rem-koolhaas.html.

58. Steven Poole. (17 December 2014). *The Guardian*. "The Truth About Smart Cities: 'In the End, They Will Destroy Democracy.'" Last accessed on 12 April 2017, https://www.theguardian.com/cities/2014/dec/17/truth-smart-city-destroy-democracy-urban-thinkers-buzzphrase.

59. NYC Mayor's Office of Tech + Innovation. (September 2015). "Building a Smart + Equitable City." Last accessed on 12 April 2017, http://www1.nyc.gov/assets/forward/documents/NYC-Smart-Equitable-City-Final.pdf.

60. IBM Corporation. (2013). "IBM's Smarter Cities Challenge: Boston—Report." Last accessed on 12 April 2017, https://www.smartercitieschallenge.org/assets/cities/boston-united-states/documents/boston-united-states-full-report-2012.pdf.

61. City of Boston. (22 June 2016). "City of Boston App Showcase." Last accessed on 12 April 2017, https://www.boston.gov/departments/innovation-and-technology/apps.

62. CCIT. (12 September 2016). *CCIT*. "14 City, Ningbo, the Wisdom of the City: 'Smart City' or 'Smart City'? (Google Translated)" Last accessed on 12 April 2017, http://www.ccit.org.cn/fuwu/rdht/info3101.html.

63. Ministry of Urban Development, Government of India. (2016). *Smart Cities Mission*. "Home." Last accessed on 12 April 2017, http://smartcities.gov.in/content/.

64. Chisinau Smart City Hackathon. (2016). “Home.” Last accessed on 12 April 2017, http://smartcity.md/.

65. Map Kibera. “Home.” Last accessed on 12 April 2017, http://mapkibera.org/.

66. The Editors of Encyclopaedia Britannica. (3 March 2016). *Encyclopaedia Britannica*. “Yokohama.” Last accessed on 12 April 2017, https://www.britannica.com/place/Yokohama.

67. City of Yokohama. (7 April 2017). *City of Yokohama*. “Population News No.1088 (April 1, 2017).” Last accessed on 12 April 2017, http://www.city.yokohama.lg.jp/ex/stat/jinko/news1704-e.html.

68. Gale International LLC. (2015). *Songdo IBD*. “About.” Last accessed on 12 April 2017, http://songdoibd.com/about/.

69. Government of Singapore. (17 April 2017). *Data.gov.sg*. Last accessed on 17 April 2017, https://data.gov.sg/dataset/total-land-area-of-singapore.

70. Worldometers.org. (2017). *Worldometers*. “Singapore Population (Live).” Last accessed on 17 April 2017, http://www.worldometers.info/world-population/singapore-population/.

71. “3. Green Urban Spaces with Integration of Sustainable Land Use.” Last accessed on 20 April 2017, http://ec.europa.eu/environment/europeangreencapital/wp-content/uploads/2016/12/Indicator-3-Green-urban-areas_Nijmegen-2018-revised.pdf.

72. Gemeente Nijmegen. (2017). “About Nijmegen: Facts & Figures.” Last accessed on 17 April 2017, http://english.nijmegen.nl/municipality/facts__figures.

73. Europe-cities.com. (2004–2017). *Europe-cities*. “Facts about Rotterdam.” Last accessed on 20 April 2017, http://www.europe-cities.com/destinations/netherlands/cities/rotterdam/general/.

74. Supurbfood. *Supurbfood*. “Home.” Last accessed on 20 April 2017, http://www.supurbfood.eu/city-regions/city-region-rotterdam-the-netherlands/.

75. MapsofIndia.com. “Jaipur.” Last accessed on 20 April 2017, http://www.mapsofindia.com/jaipur/.

76. Mark Scott. (7 June 2016). *The New York Times*. “The Spanish Town That Runs on Twitter.” Last accessed on 20 April 2017, https://www.nytimes.com/2016/06/09/technology/the-spanish-town-that-runs-on-twitter.html.

77. City of Yokohama. (2008–2017). *Climate Change Policy Headquarters*. “横浜市温暖化対策統括本部. 横浜スマートシティプロジェクトYSCP).” Last accessed on 17 April 2017, http://www.city.yokohama.lg.jp/ondan/yscp/.

78. City of Yokohama. (26 March 2015). *Climate Change Policy Headquarters*. “横浜市温暖化対策統括本部. 横浜スマートシティプロジェクト（YSCP）実証実験終了のお知らせ (YSCP Announcement of Completion of Demonstration Experiment).” Last accessed on 17 April 2017, http://www.city.yokohama.lg.jp/ondan/yscp/finish.html.

79. National Strategy Office. (27 November 2012). “国家戦略室. グリーン政策大綱 (骨子 ¯グリーンエネルギー革命の胎動から成長へ一 (Green Policy Outline [Skeleton]: From the Sprout to the Growth of the Green Energy Revolution).” Last accessed on 17 April 2017, http://www.cas.go.jp/jp/seisaku/npu/policy09/pdf/20121127/shiryo4-1.pdf.

80. YSCP Promotion Council. (1 February 2012). “YSCP推進協議会. 横浜スマートシティプロジェクト (YSCP) 第14回次世代エネルギー・社会システム協議会資料 (YSCP: The 14th Next-Generation Energy and Social System Council Materials).” Last accessed on 17 April 2017, http://www.meti.go.jp/committee/summary/0004633/014_03_00.pdf.

81. The 17th Next-Generation Energy and Social System Council. (19 May 2014). “第17回次世代エネルギー・社会システム協議会資料. 次世代エネルギー・社会システム実証横浜スマートシティプロジェクト (Next-Generation Energy and Social System Demonstration: YSCP).” Last accessed on 17 April 2017, http://www.meti.go.jp/committee/summary/0004633/pdf/017_02_01.pdf.

82. The Federation of Electric Power Companies of Japan. (2016). “Electricity Review Japan.” Last accessed on 17 April 2017, http://fepc-dp.jp/pdf/03_electricity.pdf.

83. Mitsui Fudosan Co., Ltd. (January 2014). “三井不動産株式会社. *平成*25*年度地域* エネルギーマネジメントシステムの構築に向けた調査事業報告書 (2013 Research Paper for Constructing a Regional EMS).” Last accessed on 17 April 2017, http://www.kankyo.metro.tokyo.jp/energy/tochi_energy_suishin/%E5%9C%B0%E5%9F%9FEMS%E8%AA%BF%E6%9F%BBH25%EF%BC%88%E6%9C%AC%E6%96%87%EF%BC%89.pdf.

84. TEPCO Power Grid, Inc. “東京電力パワーグリット. 電力メーター情報発信サービス (Bルートサービス (Power Meter Information Transmission Service [Route B Service]).” Last accessed on 17 April 2017, http://www.tepco.co.jp/pg/consignment/liberalization/smartmeter-broute.html.

85. Nikkei Inc. (7 October 2016). *Nihon Keizai Shimbun*. “日本経済新聞社. 関電、スマートメーター*650*万台導入　管内の半数に普及 (KEPCO Plans to Deploy 6.5 Million Smart Meters Among Half of Its Customers).” Last accessed on 17 April 2017, http://www.nikkei.com/article/DGXLASHD07H3G_X01C16A0LDA000/.

86. Tokyo Gas Co. Ltd. “Tokyo Gas. 家庭用燃料電池コージェネレーションシステムエネファーム (Household Fuel Cell Cogeneration System: Ene Farm).” Last accessed on 17 April 2017, http://home.tokyo-gas.co.jp/living/enefarm/index.html.

87. Ryuushi Yinyama. (24 August 2015). *Smart Japan*. “陰山遼将. 2020年に “環境未来都市” の実現へ、水素インフラの整備を急ぐ横浜市 (Smart City: To Realize ‘Environment Futuristic City’ in 2020, Yokohama City Rushing Development of Hydrogen Infrastructure).” Last accessed on 17 April 2017, http://www.itmedia.co.jp/smartjapan/articles/1508/24/news041.html.

88. Yokohama City Global Warming Countermeasure Headquarters. “横浜市温暖化対策統括本部. 横浜市における “水素社会” に向けた取組 (Efforts Toward ‘Hydrogen Society’ in Yokohama City).” Last accessed on 17 April 2017, http://www.city.yokohama.lg.jp/ondan/etc/pdf/suiso.pdf.

89. Yokohama City Press Release. “横浜市記者発表資料. 「水素社会の実現に向けた取組について」 に係る要望の実施について (Regarding Efforts to Realize ‘About the Implementation of the Request Pertaining to Hydrogen Society’)”. (7 November 2016). Last accessed on 17 April 2017, http://www.city.yokohama.lg.jp/ondan/press/h28/1107press.pdf.

90. Maria Teresa Bilotta. (22 December 2014). *The Guardian*. “Songdo, South Korea: The World’s First Smart City—In Pictures.” Last accessed on 17 April 2017, https://www.theguardian.com/cities/2014/dec/22/songdo-south-korea-world-first-smart-city-in-pictures.

91. u.Life Solutions. (2011–2012). *u.Life Solutions*. “Songdo IBD.” Last accessed on 17 April 2017, http://www.ulifesolutions.com/new/neweng/html/sub03_01.html.

92. Cisco. (6 July 2011). *The Network*. “Cisco and New Songdo International City Join Forces to Create One of the Most Technologically Advanced Smart Connected Communities.” Last accessed on 17 April 2017, https://newsroom.cisco.com/press-release-content?articleId=426592.

93. Finnbar Toesland. (30 March 2016). *Raconteur*. “Smart-from-the-Start Cities Is the Way Forward.” Last accessed on 17 April 2017, https://www.raconteur.net/technology/smart-from-the-start-cities-is-the-way-forward.

94. Council on Tall Buildings and Urban Habitat. (2017). *The Skyscraper Center*. “The First World Tower 1.” Last accessed on 17 April 2017, http://www.skyscrapercenter.com/building/the-first-world-tower-1/1048.

95. Korea Legislation Research Institute. (23 March 2013). *Statutes of the Republic of Korea*. “Act on the Construction, Etc. of Ubiquitous Cities.” Last accessed on 17 April 2017, http://elaw.klri.re.kr/eng_service/lawView.do?hseq=28254&lang=ENG.

96. Pamela Licalzi O’Connell. (5 October 2005). *The New York Times*. “Korea’s High-Tech Utopia, Where Everything Is Observed.” Last accessed on 17 April 2017, http://www.nytimes.com/2005/10/05/technology/techspecial/koreas-hightech-utopia-where-everything-is-observed.html?_r=1.

97. Tekes. (1 January 2011). “Ubiquitous City in Korea: Services and Enabling Technologies.” Last accessed on 17 April 2017, https://www.tekes.fi/globalassets/global/ohjelmat-ja-palvelut/ohjelmat/ubicom/aineistot/raportit/korea/ubiquitouscityinkorea.pdf.

98. Mark van Rijmenam. (18 June 2016). *Datafloq*. “The Smart City of the Future Will Bring Big Data to a New Level.” Last accessed 17 April 2017, https://datafloq.com/read/smart-city-future-bring-big-data-level/183.

99. U.S. Green Building Council. (2017). *LEED*. “Better Buildings Are Our Legacy.” Last accessed on 17 April 2017, http://www.usgbc.org/leed.

100. Dan Frommer. (1 August 2012). *ReadWrite*. “Cities as Gadgets: 8 Features This Brand-New City Has That Yours Doesn’t.” Last accessed 17 April 2017, http://readwrite.com/2012/08/01/cities-as-gadgets-8-features-this-brand-new-city-has-that-yours-doesnt/.

101. Lucy Williamson. (2 September 2013). *BBC News*. “Tomorrow’s Cities: Just How Smart Is Songdo?” Last accessed 17 April 2017, http://www.bbc.com/news/technology-23757738.

102. Financial Affairs. (14 August 2014). “Taiwan’s Next Opportunity to Turn Things Off (Pick).” Last accessed on 17 April 2017, http://www.businesstoday.com.tw/article-content-80394-109746.

103. Lee Wan Sie. (18 January 2016). “Smart Nation & IoT.” Last accessed on 17 April 2017, https://www.itu.int/en/ITU-T/Workshops-and-Seminars/iot/20160118/Documents/Presentations/Session2/Session2-3-WanSieLee-18-01-2016.pdf.

104. Ministry of Communications and Information. (August 2015). “Infocomm Media 2025.” Last accessed on 17 April 2017, http://www.mci.gov.sg/~/media/data/mci/docs/imm%202025/infocomm%20media%202025%20full%20report.pdf.

105. Government of Singapore. (14 November 2016). *National Research Foundation*. “RIE2020 Plan.” Last accessed on 17 April 2017, https://www.nrf.gov.sg/rie2020.

106. Khoong Hock Yun. (2017). *APAC CIO Outlook*. “Using Data to Power Singapore into a Smart Nation.” Last accessed on 17 April 2017, http://www.apaccioutlook.com/cxoinsights/using-data-to-power-singapore-into-a-smart-nation-nwid-723.html.

107. Government of Singapore. (4 November 2016). *National Research Foundation*. "Virtual Singapore." Last accessed on 17 April 2017, https://www.nrf.gov.sg/programmes/virtual-singapore.

108. Beeline Singapore. (2017). *Beeline Singapore*. "Home." Last accessed on 17 April 2017, https://www.beeline.sg/.

109. Thinking Highways. (14 October 2015). *Thinking Highways*. "Look East." Last accessed on 17 April 2017, http://thinkinghighways.com/look-east/.

110. nuTonomy. (2017). *nuTonomy*. "Home." Last accessed on 17 April 2017, http://nutonomy.com/.

111. Michael Tegos. (22 April 2015). *TechInAsia*. "IDA Wants to Make Singapore a Smart Nation. Here's What You Need to Know." Last accessed on 17 April 2017, https://www.techinasia.com/singapore-smart-nation-2015.

112. Yuri Anisimov. (October 2015). *LinkedIn Slideshare*. "Singapore Smart Nation Program: Notes for a Weary Pedestrian." Last accessed on 17 April 2017, https://www.slideshare.net/anissiy/singapore-smart-nation-programme-notes-for-a-weary-pedestrian.

113. Radboud Universiteit. (1026). Last accessed on 17 April 2017, http://smartemission.ruhosting.nl/visitors/.

114. GitHub, Inc. (2017). *GitHub*. "Geonovum/smartemission." Last accessed on 17 April 2017, https://github.com/Geonovum/smartemission.

115. GitHub, Inc. (2017). *GitHub*. "Geonovum/smartemission." Last accessed on 17 April 2017, https://github.com/Geonovum/smartemission/blob/master/docs/platform/architecture.rst.

116. SE Platform. "Smart Emission—Data Platform." Last accessed on 17 April 2017, http://data.smartemission.nl/.

117. Geonovum. (2014). *SOSPilot*. "10. Raspberry Pi Installation." Last accessed on 17 April 2017, http://sospilot.readthedocs.io/en/latest/raspberrypi-install.html.

118. Linda Carton. (21 January 2016). "Smart Emission." Last accessed on 17 April 2017, http://smartemission.ruhosting.nl/wordpress/wp-content/uploads/2016/04/presentatie_smartemission_ru_sgs_21januari2016_lc_ck_v14_voorsgs.pdf.

119. DutchNews. (23 June 2016). *DutchNews.NL*. "Heavy Rain Causes Flooding, Man Electrocuted as Marijuana Cellar Floods." Last accessed on 17 April 2017, http://www.dutchnews.nl/news/archives/2016/06/heavy-rain-causes-flooding-man-electrocuted-as-marijuana-cellar-floods/.

120. Martin Bailey. (23 June 2016). *The Art Newspaper*. "Water and Sewage Leaks Close Basement Displays at Rotterdam's Boijmans Van Beuningen Museum." Last accessed on 17 April 2017, http://theartnewspaper.com/news/museums/water-and-sewage-leaks-close-basement-displays-at-rotterdam-s-boijmans-van-beuningen-museum/.

121. Linnie Mackenzie. *Water & Wastewater International*. "Rotterdam: The Water City of the Future." Last accessed on 17 April 2017, http://www.waterworld.com/articles/wwi/print/volume-25/issue-5/editorial-focus/rainwater-harvesting/rotterdam-the-water-city-of-the-future.html.

122. European Commission. "Rotterdam's First Full-Scale Water Square." Last accessed on 17 April 2017, http://ec.europa.eu/environment/europeangreencapital/rotterdams-water-square/.

123. Carol Howe and Cynthia Mitchell (Editors). (2012). "Water Sensitive Cities." Available at http://www.iwapublishing.com/books/9781843393641/water-sensitive-cities.

124. Gemeente Rotterdam. Regenradar Rijnmond. Last accessed on 17 April 2017, https://www.rotterdam.nl/apps/rotterdam.nl/wonen-leven/regenradar/index.xml.

125. Rain Gain. (2012). *Rain Gain*. "Rotterdam." Last accessed on 17 April 2017, http://www.raingain.eu/en/rotterdam.

126. Rain Gain. "Pilot Location: Centrum, Rotterdam, NL." Last accessed on 17 April 2017, http://www.raingain.eu/sites/default/files/fs1_tech_centrum.pdf.

127. ReGen Villages. Last accessed on 17 April 2017, http://www.regenvillages.com/.

128. Kurt. (2007–2017). *Web Urbanist*. "Off-Grid and Self-Sufficient: ReGen Villages with Vertical Farms." Last accessed on 17 April 2017, http://weburbanist.com/2016/05/22/off-grid-self-sufficient-regen-villages-with-vertical-farms/.

129. HT Correspondent. (28 January 2016). *HinsudtanTimes*. "Gov't. Names 20 Cities for Smart Makeover; Bhubaneswar Tops List." Last accessed on 18 April 2017, http://www.hindustantimes.com/india/list-of-smart-cities-announced-bhubaneswar-pune-jaipur-in-top-three-slots/story-92X0VMRu5DjxpnFkOqZqDO.html.

130. Cate Lawrence. (30 May 2016). *ReadWrite*. "Is Jaipur India's Smartest City?" Last accessed on 18 April 2017, http://readwrite.com/2016/05/30/jaipur-set-to-become-indias-smartest-city-cl4/.

131. Byron Magrane. (19 October 2016). *Cisco Blogs*. “Indian City in the Pink with New Cisco Network.” Last accessed on 18 April 2017, http://blogs.cisco.com/wireless/indian-city-in-the-pink-with-new-cisco-network.

132. Mohammed Iqbal. (18 October 2016). *The Hindu*. “Modi Launches Smart City Projects in Jaipur, Udaipur via Video Conference.” Last accessed on 18 April 2017, http://www.thehindu.com/news/national/Modi-launches-Smart-City-projects-in-Jaipur-Udaipur-via-video-conference/article14401726.ece.

133. Urban Development & Housing Department. (2015). *Jaipur Development Authority*. “Welcome to Jaipur Development Authority.” Last accessed on 18 April 2017, http://jda.urban.rajasthan.gov.in/content/raj/udh/jda---jaipur/en/home.html#.

134. Ashutosh A.T. Pednekar. “Preparing Smart City Proposal.” Last accessed on 24 April 2017, http://smartcities.gov.in/upload/uploadfiles/files/Jaipur_smartcity.pdf.

135. Express News Service. (26 June 2016). *ieNation*. “Rajasthan: CM Raje Dedicates Projects for Jaipur Smart City.” Last accessed on 18 April 2017, http://indianexpress.com/article/india/india-news-india/rajasthan-cm-raje-dedicates-projects-for-jaipur-smart-city-2876410/.

136. Mott MacDonald. “Smart City Jaipur.” Last accessed on 18 April 2017, http://www.smartcitieschallenge.in/files/dmfile/Draft-Smart-Cities-Proposal-jaipur1.pdf.

137. PRC National Development and Reform Commission. (27 August 2014). “中华人民共和国国家发展和改革委员会. 关于促进智慧城市健康发展的指导意见 (Guiding Opinions on Promoting the Healthy Development of Smart City).” Last accessed on 18 April 2017, http://www.ndrc.gov.cn/zcfb/zcfbtz/201408/W020140829399623302448.pdf.

138. ReportLinker. (May 2016). “China Smart Electric Meter Industry Report, 2016–2020.” Last accessed on 18 April 2017, http://www.reportlinker.com/p03837879-summary/China-Smart-Electric-Meter-Industry-Report.html.

139. Wuhan Research Institute for Smarter Cities. “武汉智慧城市研究院. 武汉智慧城市发展需求. (On the Development of Wuhan Smart City).” Last accessed on 18 April 2017, http://www.wrisc.cn/wrisc/type/zhcs.

140. CCIT. (17 October 2016). “中国智慧城市产业网. 智慧城市需要大数据 杭州启动城市大脑项目 (Smart City Needs Big Data: Hangzhou Initiates City Brain Project).” Last accessed on 18 April 2017, http://www.ccit.org.cn/news/hyzx/info3154.html.

141. ZAKER. (25 October 2016). “城市大脑” ，一场前所未有的人工智能进化. (‘City Brain,’ an Unprecedented Evolution of Artificial Intelligence).” Last accessed on 18 April 2017, http://www.myzaker.com/article/580f820d7f780bad3300c9a3/.

142. Wang, Peng. (14 June 2016). *China Big Data Industrial Observation*. “王鹏. 干货丨智慧城市与城市数据运营 (Real Stuff | Smart City and City Operations Based on Data).” Last accessed on 19 April 2017, http://www.cbdio.com/BigData/2016-06/14/content_4982662.htm.

143. Jemima Kiss. (2 July 2015). *The Guardian*. “Welcome to Jun, the Town That Ditched Bureaucracy to Run on Twitter.” Last accessed on 19 April 2017, https://www.theguardian.com/technology/2015/jul/02/twitter-jun-spain-bureaucracy-local-government.

Created by:

TrendLabs

The Global Technical Support and R&D Center of TREND MICRO

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit **www.trendmicro.com**.

TREND MICRO™

Securing Your Journey to the Cloud

www.trendmicro.com