June 2021

Securing the Internet of Things for a Smart City

A non-technical guide for government decision makers

About the author

Tom Zorde
ACS Internet of Things
Committee Chair

Tom Zorde leads purpose-driven communities to future-proof Australia for a changing digital world. He convened and led volunteers to deliver a free-to-use wireless Internet of Things Communications Network for Western Australia which now enables entrepreneurs, academia, industry, rural and city councils. His efforts were recognised by the Australian Computer Society, awarding the project the 2018 Digital Disruptor award for transforming skills of work teams of 21 to 200. In addition to launching the world's first certified Internet of Things practitioner accreditation in compliance with ANSI/ISO/IEC 17024 standards, Tom has become a respected ICT industry leader nurturing collaboration across industry, government and academia, and is a sought-after advisor for organisations embarking on digital transformation.

Twitter: @TomZorde

LinkedIn: http://linkedin.com/in/zorde

Contents

What is the Internet of Things (IoT)?

Not every device that connects to the internet is a traditional computer. There are billions of other devices – cameras, sensors, appliances, ticketing devices, and many more – that also connect directly to the internet. This is what is known as the Internet of Things, or IoT.

IoT devices are used extensively in smart cities. In a smart cities context, there are devices such as:

- Connected utility meters that automatically gather power, water and gas usage.
- Traffic monitors and sensors that can be used for dynamic traffic management and road monitoring.
- Parking monitors that can guide drivers to open parking spaces.
- Smart bins that can be monitored to help optimise pickup schedules.
- Sensors for air quality, water levels and water quality.
- Smart phone readers that allow citizens to use their phone as a form of ID for parking meters and other government services.

All these devices can use the internet to feed information back to an information store, where conditions can be monitored to inform immediate action as well as better planning and management decisions.

If you are deploying IoT devices in your smart city, or if you are contracting a third party to do so, there are security risks you need to be aware of and conversant in to safely adopt IoT. That is what this guide is all about.

01 The journey for smart cities

The Internet of Things (IoT) is one of the key elements of a smart city. It gives operational managers the capability to digitally interact with remote facilities and assets. It lets them automatically collect and analyse streams of data about infrastructure usage and performance, which can provide invaluable insight to inform operational decisions. Many improvements to the timeliness and cost of city services are possible when abnormal asset conditions are detected quickly and delivered as curated alerts for action. User friendly apps that collect relevant data around the clock can be built on top of smart city IoT deployments, providing information on when, where, and what is happening within sensory range of city assets.

The capability of IoT goes beyond remote monitoring of infrastructure assets. It also offers the capacity to remotely operate assets in a user actuated or automated way. This can include activities such as turning off a pump or lighting in response to current or predicted traffic or weather change events.

With the ability to remotely monitor, predict, and intervene on events, operational managers can do more with less, delivering better outcomes for the citizens they serve.

The benefits are exciting, but as many city councils have discovered, the journey to IoT adoption is not without challenge, especially when the topic of security risk arises. The numerous guides available about IoT are often technical in nature or too high level. Many are positioned with a sales agenda or are overly presumptuous about your technology, change and risk management maturity.

This article aims to offer pragmatic IoT security risk guidance for non-technical city personnel. It is written to help time, cost and risk-conscious decision makers evaluate and procure IoT solutions. It is relevant to those responsible for business operational risk and purchasing decisions. It also serves as a useful aid for collaborating with technical personnel who can use it in conjunction with IoT platform selection guidance, such as that provided by IoT Alliance Australia (see Recommended sources on page 11).

02 Security risk considerations

Unlike typical procurement of products and services, IoT solutions cannot be easily and reliably compared side by side. This is because they have a varying but high dependence on external services, including communications, power, physical installation and housing, and data platforms. These all need to interoperate in a resilient and reliable manner to provide the continuity of service required by the city. Various IoT products may deal with interoperability differently and may or may not work to recognised standards.

Comparison of IoT solutions is additionally challenged by trade-offs in non-functional features such as interoperability, scalability, reliability and, importantly, security. These are not obvious if the main concern is IoT solution cost, time-to-market, and utility.

The risk posture presented by an IoT solution will be the result of the chosen product's non-functional security features combined with the risk tolerance of the city for the specific scenario for which the IoT solution will be being used.

The requirements for non-functional features are different for every city council and are an important part of a sustainable IoT solution as they mitigate risks to continuity of service.

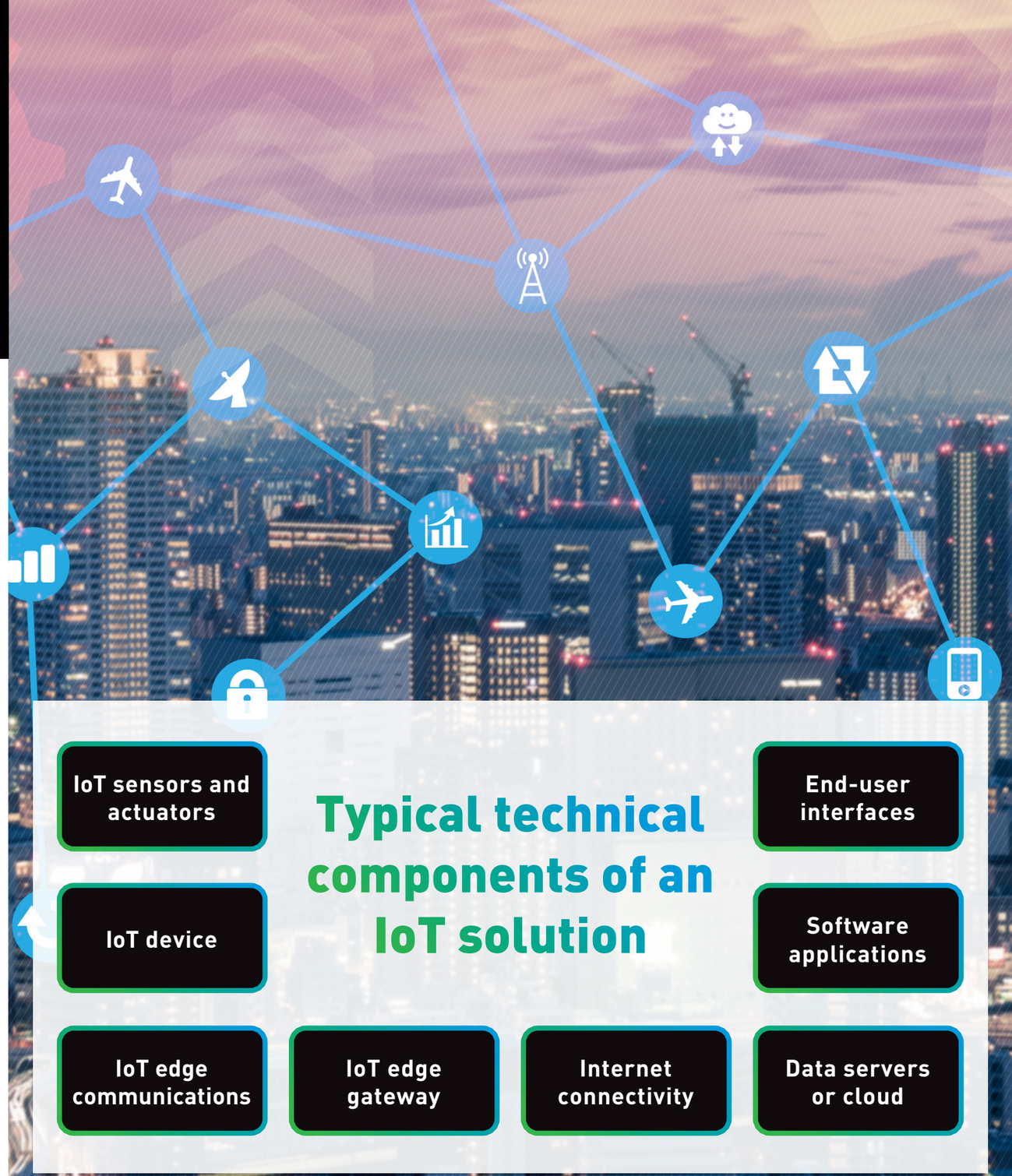
When evaluating IoT products, the requirements for both functional and non-functional features should be clearly understood by all stakeholders in the business processes that will be enhanced by IoT. The stakeholder list should include any indirect down-stream stakeholders who may be impacted by a service outage. This may include suppliers, citizens, local businesses, and other government services.

The security of an IoT solution is best considered early in the smart city IoT adoption process. It should encompass all technical components end-to-end, as well as processes for operating, managing, and governing the solution.

Common practice for smart cities encourages incremental baby steps for IoT adoption. This often takes the form of low-cost trial implementations to demonstrate value, viability, and feasibility before scaling up the solution for more IoT nodes, data, or users. But even small IoT deployments can present consequential impact if a security breach happens.

Consequences of incorrect or improper consideration of the right security features could lead to anything from the leaking of sensitive or private information, wasting city resources, right up to causing physical harm from malfunctioning devices.

All technical and non-technical components of an IoT solution should be identified before procuring any equipment. An IoT solution architecture will show the scope of each component to help identify accountabilities and the right specialists to be consulted to ensure there are no gaps or contradictions between various component security features. For example, communications may provide data encryption, but the sensor unit may store data un-encrypted, exposing a potential risk of data tampering or theft.



03 Leveraging existing city capabilities

A city council's information technology department is an important partner for guidance on IoT technology and cyber security. However, the security of physical equipment outside the controlled premises of a data centre or council facility presents unusual challenges and the IT department may not have the requisite expertise to handle those requirements. IoT security extends beyond information systems into the realm of real-time and possibly mission critical operational technologies that cannot be secured like other physical assets because they run software and are connected to the public internet. Management of them must cover both operational asset risk as well as information risk, and you should consider engaging specialist IoT security professionals.

IoT security incidents are challenging because they span both the physical and virtual world. For example, sensors for monitoring waste water sump drainage might be physically tampered with at site of installation, or electronically from a remote location, to manipulate the data and misdirect scarce city resources causing delays and disruption to city operations.

A city council would benefit from working with internal departments to establish a satisfactory set of minimum standards that encompass security for IoT procurement. This will support the advancement of smart city agendas and establish good foundations to protect against future IoT-based security incidents that may impact anything from critical city processes to state or even national infrastructure services.

Minimum standards should consider all city stakeholder interests and can be established by leveraging current and relevant operational risk assessment frameworks and capabilities. Remember to clarify the broader set of stakeholders that should be involved during both procurement and operation of new IoT solutions.

04 Risk assessment for IoT

The following steps describe key actions to assess the risk exposure an IoT solution may present and should be followed before selecting any products or partners. This would ideally be used in the early framing of a business case when the business problem is being defined and the high level IoT solution architecture components and stakeholders are known.

Assessing the risk of an IoT solution will help discover the viability and feasibility of the desired solution. Some holistic security risk categories can be seen in the diagram below:

Risk categories

Operational

- Risks to revenue
- Risks to staff, vendors and citizens
- Risks to infrastructure and assets
- Regulatory compliance risks

Environmental

- Risks to local flora and fauna
- Third party property risks
- Equipment disposal

Economic

- Risks to sustainable operations of businesses and agencies affected
- Risks to local government agency reputation

Social

- Risks to personal and private information of citizens
- Risks to location tracking and safety

Holistic risk categories to consider for IoT.

Operational risks are especially pertinent in a smart cities context where the IoT deployment affects critical infrastructure services such as water, power, transportation, emergency services and public safety.

The first four steps in the risk assessment process qualify the level of risk exposure presented and determine the tolerance levels. This is a helpful aid when scoping the security requirements that will inform suitable risk mitigation controls.

1. Establish a risk assessment group of stakeholders, including facility managers, business operations, and data owners who will agree to the desired risk tolerance and determine if mitigation is required. Be flexible about adding additional stakeholders if more are identified at later stages. Consider that this may include the community at large and other city councils.
2. With the various security risk categories listed above in mind, identify the likelihood of any security threats, making sure you explore solution vulnerabilities, and agree to the scope of the security assessment. Remember that IoT solutions are not limited to information risk. The integrity of physical equipment, any communication links and power sources can be compromised by malicious or natural events.
3. Identify if there is sensitive or confidential data stored or transmitted by the IoT solution. Review any existing regulatory compliance that must be adhered to such as the Privacy Act. Remember that IoT sensors such as cameras may capture data in addition to what is needed.
4. Assess the consequences of the confidentiality, integrity and availability of the solution or its data being compromised in light of the information gathered in steps 2 and 3. A risk rating may best be interpreted using existing risk management frameworks and appropriate risk rating matrices familiar to the city council operations, but it should be agreed by all the stakeholders identified in step 1.

		Consequence				
		Insignificant	Minor	Moderate	Major	Critical
Likelihood	Rare	LOW Accept the risk Routine management	LOW Accept the risk Routine management	LOW Accept the risk Routine management	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review
	Unlikely	LOW Accept the risk Routine management	LOW Accept the risk Routine management	MEDIUM Specific responsibility and treatment	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review
	Possible	LOW Accept the risk Routine management	MEDIUM Specific responsibility and treatment	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review	HIGH Quarterly senior management review
	Likely	MEDIUM Specific responsibility and treatment	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review	HIGH Quarterly senior management review	EXTREME Monthly senior management review
	Almost certain	MEDIUM Specific responsibility and treatment	MEDIUM Specific responsibility and treatment	HIGH Quarterly senior management review	EXTREME Monthly senior management review	EXTREME Monthly senior management review

Risks can be assessed using existing risk management frameworks.

The next three steps will quantify the required controls to reduce the security risk to tolerable levels.

5. Determine what controls are best applied to reduce likelihood or lessen impact by seeking technical guidance from experts qualified in the at-risk components of the IoT solution. For example, the guidance for wireless radio communication for transmitting IoT sensor data is a specialist skill and intersects with applicable regulatory requirements such as radio frequency spectrum plan compliance. See the Recommended sources box at the end of this article for guidance, and work with implementation partners to assess possible solutions.
6. Estimate the cost and effort required to implement and maintain security controls to reduce risk to tolerable levels; this can be done in partnership with stakeholders and solution providers. Remember controls may be managerial, operational, and technical. The right balance for someone else may not be right for you.
7. Having identified potential risks, recommend and get a solution sponsor to agree to include applicable security requirements as minimum standards for the IoT solution.

The security requirements can now accompany functional requirements as well as other non-functional requirements to inform a tender for the selection and implementation of an appropriate IoT solution.

City councils should consider reviewing all risks regularly throughout the project and after implementation as the security threat landscape for IoT is one that changes rapidly. It is good practice to review risks and assure security requirements in the solution design phase, during technical implementation, and again during final quality assurance tests to confirm controls are working as intended. Vulnerability scans, penetration tests, and ethical hacks can be effective quality assurance measures, ensuring that your IoT rollout goes smoothly and avoids any nasty surprises when your smart city solution goes live.

Recommended sources

If you want to learn more about IoT security and platform selection, we recommend:

The IoT Alliance Australia Internet of Things Platform Selection Guideline: https://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA_IoT-Platform-Selection-Guideline-V1.1-July-2018.pdf

Securing the Internet of Things for Consumers Code of Practice, from the Department of Home Affairs: https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

A guide to the top ten security risks of IoT, from OWASP: https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet

The US National Vulnerability Database: https://nvd.nist.gov

Summary of IoT security guidance

- IoT deployments underpin smart city operations.
- Non-functional requirements, including security, are a critical part of the procurement process for IoT, and need to be evaluated early and often.
- Security controls should be based on strong risk assessment principles and should be planned out with stakeholders before implementation begins.
- IoT is both information technology and operational technology, and the consulted stakeholders need to reflect that.
- Risk assessment should be done regularly as IoT security threats change constantly.

ACS
International Tower One
Level 27, 100 Barangaroo Avenue
Sydney NSW 2000

P: 02 9299 3666
F: 02 9299 3997
E: info@acs.org.au
W: acs.org.au

About the Australian Computer Society

The Australian Computer Society (ACS) is the professional association for Australia's Information and Communication Technology (ICT) sector. Over 48,000 ACS members work in business, education, government and the community. The Society exists to create the environment and provide the opportunities for members and partners to succeed. The ACS strives for ICT professionals to be recognised as drivers of innovation in our society, relevant across all sectors, and to promote the formulation of effective policies on ICT and related matters.

Visit **www.acs.org.au** for more information.