MANUFACTURING:
AN INTRODUCTORY GUIDE TO 5G & SECURITY

UK 5G Innovation Network

INTRODUCTION

Network security is of the utmost importance for manufacturers. But as the world goes digital by way of open platforms and mobile networks, the industry understandably has its concerns. 5G, however, has security and resilience as part of its standards. AI and automated security tools can also be layered over the top for greatly enhanced security.

Manufacturers can therefore migrate to wireless connectivity with confidence. Connecting everything from enterprises, smart factories and critical public safety infrastructures, a 5G network guarantees communication service providers the ability to serve these use cases with secure and resilient connectivity alongside increased agility and flexibility.

This guide has been designed to explain how to outline 5G's security credentials —identifying the latest insights, the importance of authentication and introducing the zero trust model.

We don't claim to have all the answers here, indeed this forms only one part of a wider body of content produced by UK5G to help guide the manufacturing industry through how to deploy 5G—and, of course, each case is unique.

It is also important to note that, though this paper focuses on manufacturing, this information should be applicable to a range of sectors.

Network security is of the utmost importance for manufacturers.

5G has security and resilience as part of its standards. AI and automated security tools can also be layered over the top for greatly enhanced security.

5G'S SECURITY ARCHITECTURE

Building an inherently secure 5G system requires a holistic effort, rather than focusing on individual parts in isolation. This is why several organisations such as the 3GPP, ETSI, and IETF have worked together to jointly develop the 5G system, each focusing on specific parts. Below, we present the main enhancements in the 3GPP 5G security standard, all of which can provide assurance to manufacturers that devices connected to a 5G network, and the data they transfer, are secure.

a/ New authentication framework

- A central security procedure in all generations of 3GPP networks is access authentication, which is used to protect the communication between the device and the network and is typically performed when a device is turned on for the first time. It is well established and widely used in IT environments.
- One advantage is that it allows the use of different types of credentials besides the ones commonly used in mobile networks and typically stored in the SIM card. This flexibility is a crucial enabler of 5G for both factory use-cases and other applications outside the telecom industry.
- The support of the Extensible Authentication Protocol (EAP) also facilitates secondary authentication, allowing the operator to delegate the authorisation to a third party.

b/ Enhanced subscriber privacy

- Security in the 3GPP 5G standard significantly enhances the protection of subscriber privacy against false base stations, popularly known as IMSI catchers or Stingrays. In summary, it has been made very impractical for false base stations to identify and trace subscribers by using conventional attacks like passive eavesdropping or active probing of permanent and temporary identifiers
- In addition, 5G is proactively designed to make it harder for attackers to correlate protocol messages and identify a single subscriber. The design is such that only a limited set of information is sent as cleartext even in initial protocol messages, while the rest is always concealed.
- Another development is a general framework for detecting false base stations, a major cause for privacy concerns. The detection, which is based on the radio condition information reported by devices on the field, makes it considerably more difficult for false base stations to remain stealthy.

c/ Service-based Architecture & Interconnect Security

- In a service-based architecture (SBA), the 5G core network functions support state-of-the-art security protocols at the application layer to ensure that only authorised network functions are granted access.

REALISING ZERO-TRUST IN NETWORKS

Cybersecurity is a key consideration for any organisation and when it comes to deploying advanced connectivity solutions, many manufacturers are adopting zero trust models. By starting from the assumption that the attacker is already inside the network, a zero trust approach enhances security by both blocking unauthorised access to network resources and preventing internal lateral movement by an attacker.

The architecture is built on an identity-centric approach. Facilitating secure network access to resources (data, devices and services) that are limited only to authorised and approved subjects (users, devices and services) mitigates both the risk of an external attacker getting a foothold in the network as well as the risk of lateral movement, in the case of an (unlikely) security breach. Essentially, it assumes the worst at all times to offer the greatest protection.

There are three key security features in 5G that are of most significance in terms of enabling zero trust architectures: secure digital identities, secure transport and security monitoring.

a/ Secure digital identities

- These play a fundamental role in building trust and securing communication between entities across security domains and with 5G, each and every subject and resource is uniquely identifiable.

b/ Secure transport

- 5G's additional improvements include enhanced protection of subscriber privacy against conventional attacks such as passive eavesdropping or active probing of permanent and temporary identifiers

c/ Security monitoring

- 5G supports detecting threats, measuring network assets' security posture, and compliance with security policies. Monitoring and evaluation of subjects, resources compliance, trustworthiness and state are important when deciding whether to permit access to resources.

THE LINK BETWEEN SECURITY AND SAFETY

When it comes to manufacturing particularly, there is an undeniable interplay between security and safety. In the event of a security breach, manufacturers may find safety is compromised; a situation that is simply not acceptable in a heavily regulated industry.

A dropped connection or attack from bad actors could jeopardise a worker's well-being, with potentially fatal consequences. Security and safety are undoubtedly linked: but, for manufacturers, where should the focus lie and how can you balance the two? Read our discussion below.

David Lund, Founder of Safenetics and a contributor to the Factory of the Future project, said: "The safety context is that we don't want a rogue robot kicking people as it walks along the factory floor. We incorporated the safety element in some of our security risk assessments"

He added: "Safety is a cross-cutting key value as we go forward with research in 5G and of course, 6G. Safety is absolutely the right way to go with this and cybersecurity is part of that."

Toby Rhodes of Perform Green and 5G CAL, said: "There was a significant emphasis on safety within the 5G CAL project. Obviously, when you're driving around a 40-tonne truck, there has to be. It's a live industrial site as well, this was not an experimental zone. There was a huge amount of work over the past few years therefore on safety but also, as a result, cybersecurity. If someone were to take over the communications guiding the truck, for example, that would create a huge safety risk."

Giedre Sabaliauskaite, Associate Professor at Coventry University explained how the 5G CAL project mitigated the risk by putting in a physical line of defence: "Implementing a safety driver was the solution that we decided to proceed with. This meant that if there was an attack on our network or a failure, we had a person who could take control. In another manufacturing scenario, where there is no need for a safety driver, it would become really critical to look more seriously into the degradation of safety and security."

Wholly integrating security and safety is unlikely to be practical—each has its own ways of thinking, processes and structures—but in any instance where a breach of the integrity of a communications system impacts personnel, there is likely to be a relationship that needs to be understood.

Considering how exactly security—and any degradation in security—impacts safety during the concept development phase of any 5G deployment is key. Coventry University recommends establishing synchronisation points so, at set stages in the process, safety and security teams can come together to review interdependencies and identify if there are any issues arising.

Do private networks offer greater security?

Private 5G networks can be a fantastic connectivity solution for manufacturers, offering guaranteed coverage and capacity exactly where it's needed and the ability to configure the network according to specific requirements, for instance with a focus on uplink over the downlink. One of the benefits often touted is the enhanced security, but are private networks really any more secure?

The answer is yes… and no. The enhanced security credentials of 5G outlined in this guide are present on both public and private networks: 5G is inherently more secure by design and public 5G networks are secure. There are certain advantages associated with private networks however that can offer security-conscious manufacturers greater assurance.

Firstly, with dedicated SIMs for whitelisted devices, only devices you know and permit can connect to your private network. Secondly, your data is not 'in the field'. For aerospace manufacturers, or others operating in security-critical sectors, knowing your data is not leaving your domain can be a notable benefit both to satisfy your own internal policies and those of your customers.

Today, the majority of public 5G networks are non-standalone, meaning they rely on 4G infrastructure. In order to maximise the coverage available to customers, public networks will roam over to other networks when moving out of 5G coverage, or if for instance 5G is jammed. This would mean your connection passing to 4G or even 3G where networks are not as inherently secure. This may present an unacceptable risk to manufacturers which can be mitigated by using a standalone 5G network.