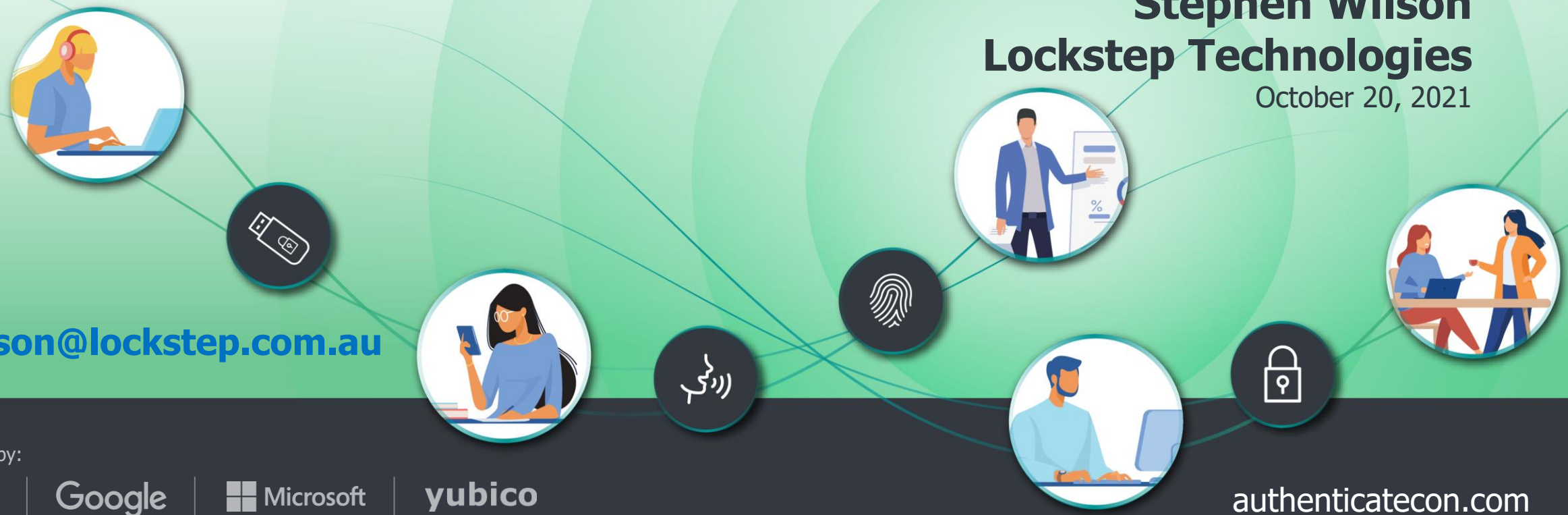
authenticate

The Identity of Things: We're Gonna Need a Smaller Idea

Stephen Wilson
Lockstep Technologies

October 20, 2021



swilson@lockstep.com.au

THE IDENTITY OF THINGS?

The "identity of things" seems like a natural extension of identity and access management techniques, and with connected devices expected to far outnumber human actors, we certainly need the means to tell devices apart. But let's be careful extrapolating from the digital identity of people. We have made a mess of digitizing "identity" of the sorts of actors who actually have identity. Let's take this opportunity to carefully rethink what we need to know about inanimate actors in the IoT.

"We are getting nowhere on digital identity"

— Dave Birch

"If these problems were easy to solve, we wouldn't be debating some of the same issues we were discussing 30 years ago"

— TechVision Research

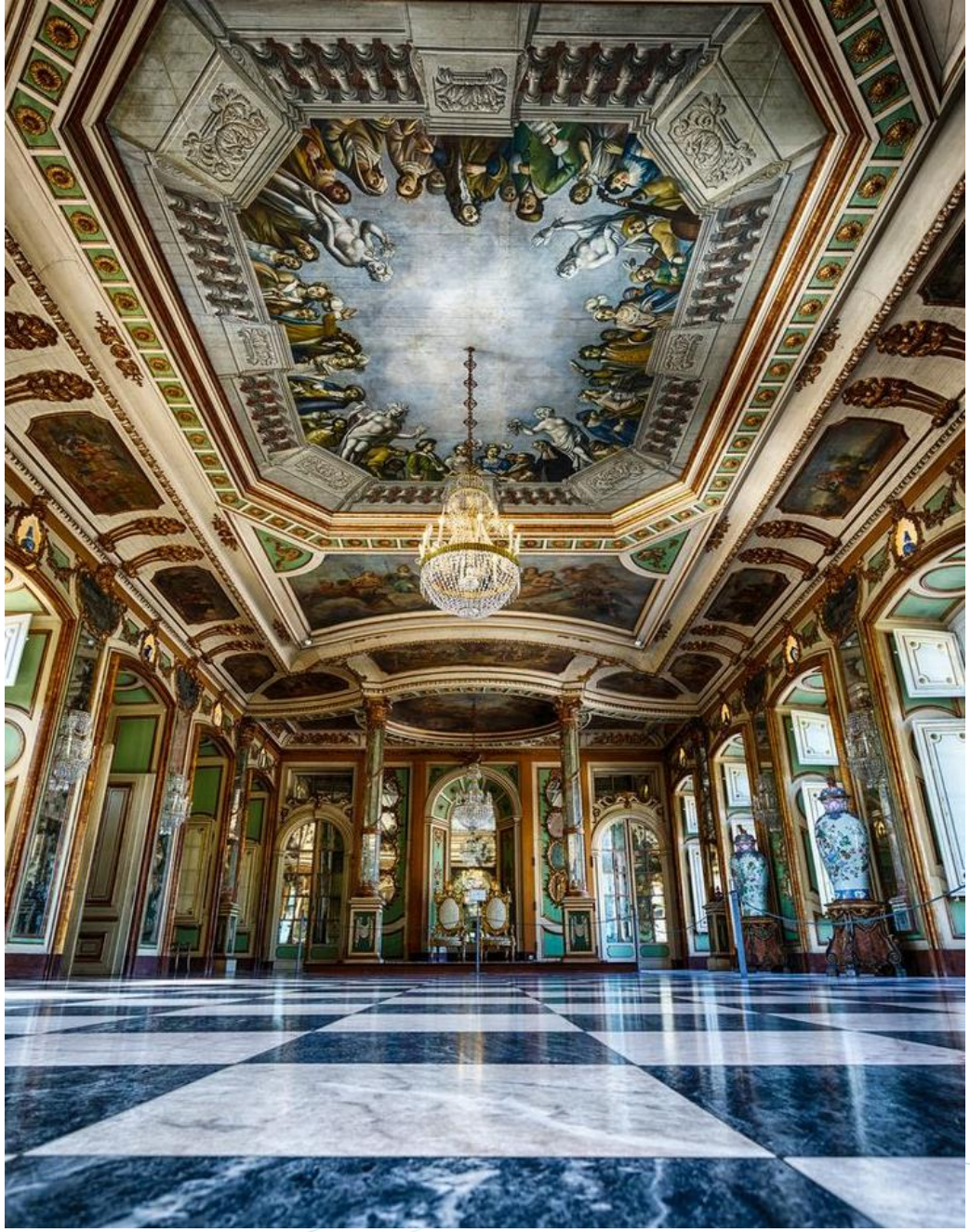
Complexity

"With self-sovereign identity, users have complete control over how their personal information is kept and used"

— TechTarget

We have a habit of complicating "identity" when we could be focusing more intently on the protection of credentials and authentication signals. For instance, the preeminent Self Sovereign Identity movement seeks to weaponize identity against big business and government in the fight over data. It's a critical contest for sure, but we must pick the right tools and methods, and we must frame the problem properly. What would it mean to "control" our information? When it comes to algorithmic outputs, analytics, health data and genetics, whose information is it anyway?

The Internet of Cars demonstrates the complexity of information flows and the granularity of device data ...



Complexity in IoT

Cars are becoming 'networks on wheels'. Passengers almost always carry connected devices—phones, games, even toys which now come with privacy policies—all liable to try to connect to the vehicle. The driver might use her watch to start the car, which in the near future will likely check her smart driver licence, or medical devices where relevant. Phones already share location with maps and traffic apps. Who "owns" these different data streams? Who could hope to "control" them? Self Sovereign Identity is not going to bring order to this chaos; indeed, the identification of things is only a small part of the challenge.

In the full-blown 'Internet of Cars', vehicles, car parts, road infrastructure, supply chains and stakeholders will work together for improved safety, congestion and energy efficiency. A key question in all these potential exchanges is what is relevant exactly? What will authorize a toy to connect with a car, or a car to interrogate a medical advice?

Informatic grey goo

"Vehicle data is more profitable than the car itself"

— Francois Fleutiaux, COO, T-Systems

The quote from one of today's IoT leaders echoes the famous words of former Citibank CEO Walter Wriston who said in the 1980s that information about money is as important as money. And thus it is the demand for information that really propels the Internet of Things.

With nanotech comes a vivid fear that the world could be chewed up and spat out by self-replicating molecular robots. Similarly, unconstrained hyperconnectivity could lead to informatic "grey goo" where devices radiate data about every other device—and every human being—they're connected to. To head off this privacy and security nightmare, we need precise organisation of device authentication, according to the principles of the Need to Know and Collection Limitation.

Design thinking for Authentication

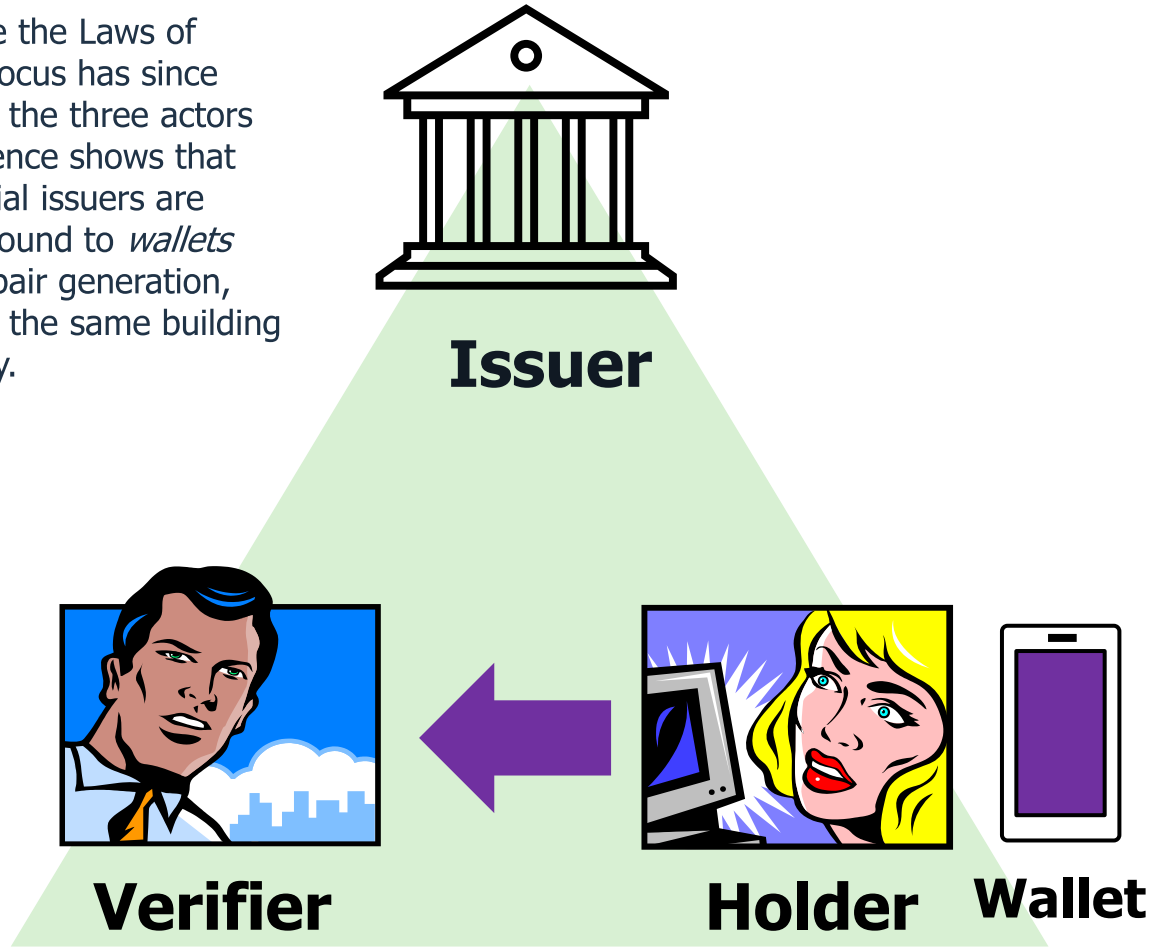
Careful authentication design should not start with "identity" but rather a set of precise questions:

1. ***What does one party need to know about the other?***
2. ***Where will the relying party get that data?***
3. ***How will the relying party know that it's true?***

Consider credit card processing. For a merchant to be securely paid, only the customer's primary account number (PAN) needs to be collected. Over different generations, the PAN has been handled using different card technologies: firstly paper, then mag stripe, and now chip. In many places now it is *mandatory* for the merchant terminal to read the PAN from a Chip-and-PIN card. And the truth of the data is established through digital signatures (a static signature of the issuing bank on the PAN loaded to the chip, and a dynamic signature applied by the chip to each transaction). These security features make the Chip-and-PIN card one of the first cryptographically Verifiable Credentials.

Authentication pattern & tools

There has been a common pattern in most authentication situations ever since the Laws of Identity gave us the actors *Subject*, *Relying Party* and *Identity Provider.* The focus has since shifted from open ended or abstract "identity" to very specific credentials, and the three actors are now often termed *Credential Holder, Verifier* and *Credential Issuer*. Experience shows that "identity" as such can't actually be "provided" but on the other hand, credential issuers are commonplace. Best practice has always been for Verifiable Credentials to be bound to *wallets* (and private key stores) and digitally signed by the credential issuer. The key pair generation, private key storage and transaction signing primitives used for VCs are exactly the same building blocks leveraged by FIDO protocols. These are core to IoT security and privacy.



Verifiable credentials

- Provenance of the credential
- Proof of Possession
- Provenance & state of the device.

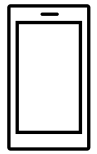
Adjacent to FIDO

- Strong private key storage
- User control
- Transaction signing.

IoT and infostructure

The *Holder / Verifier / Credential Issuer* pattern generalizes in the IoT, where many holders are inanimate devices, and credentials are properties or specifications held within secure elements. Verifiers will be other devices or control systems. A huge range of formal pieces of information will be transmitted and received & verified across the IoT.


Holder


Wallet

Date


Verifier

Country

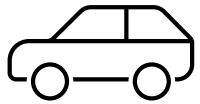
Type


Food

Maker


Appliance


Apparel

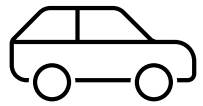

Thing

Rating

Efficiency

Serial No.

Part No.


Thing

Date


Verifier

Author


Appliance


Appliance

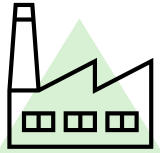

Issuer


Issuer


Verifier

Compliance

Warranty


Issuer

State

Version


Issuer


Verifier

Age

Quals

Rating

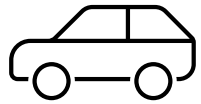

Medicine

Purity

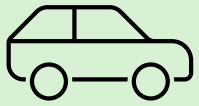
Passed

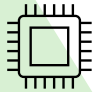
Model

Certified


Thing


Verifier


Thing


Secure Element

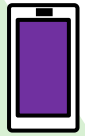
Location

Grade

Rating


Verifier


Holder


Wallet

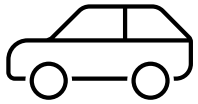
Registration

Service

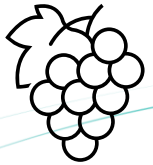
Test


Verifier

Rating


Thing

Weight


Food


Verifier

Compliance

The ~~Identity~~ Information of Things

of the things

for the things

by the things.

So let's think beyond identity, to leverage embedded cryptography, FIDO protocols and Verifiable Credentials technology to enable autonomous things to transact reliable information about themselves.

Stephen Wilson AuthenticateCon 2021 keynote - The Identity of Things (0.5.1) HANDOUTS

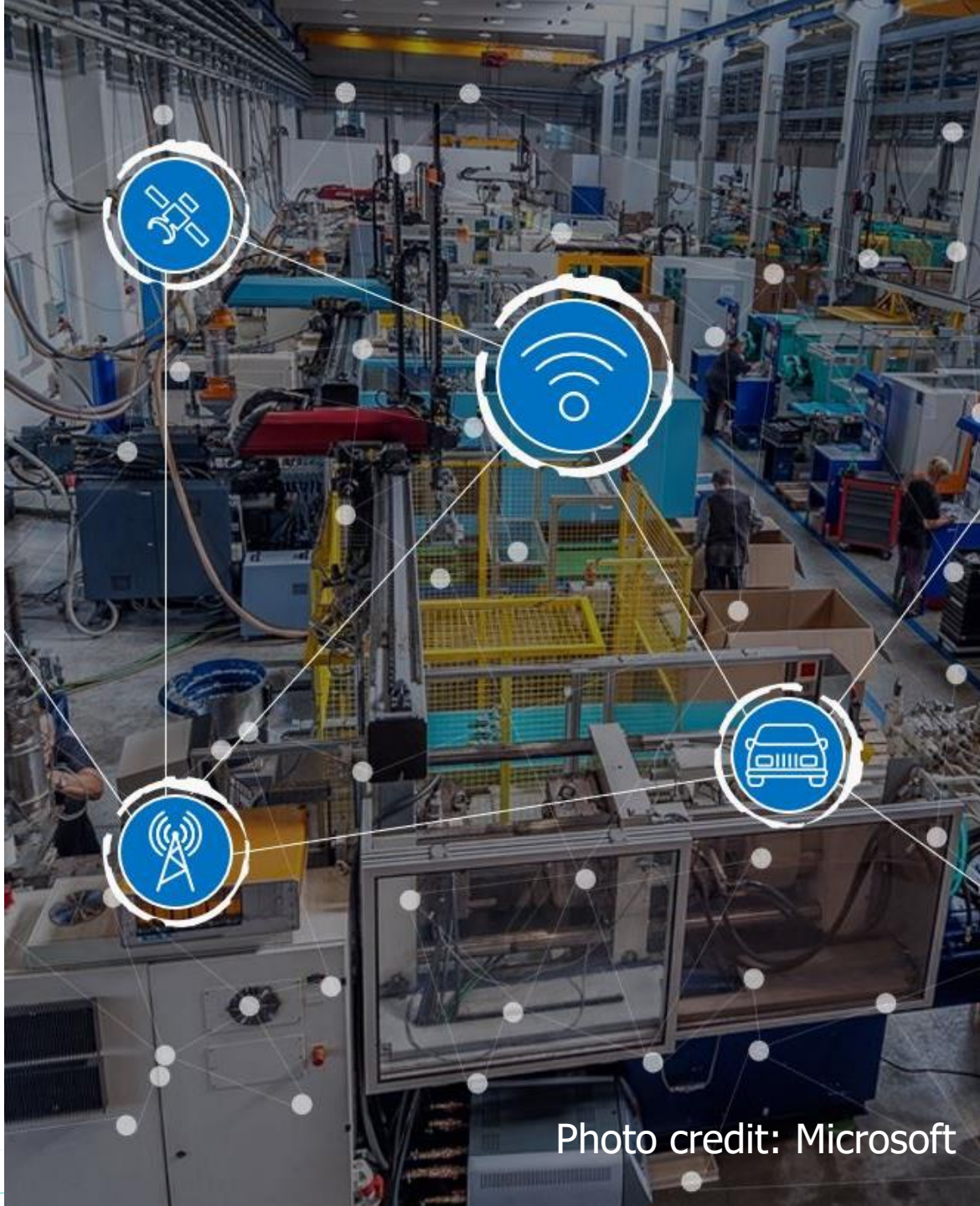


Photo credit: Microsoft