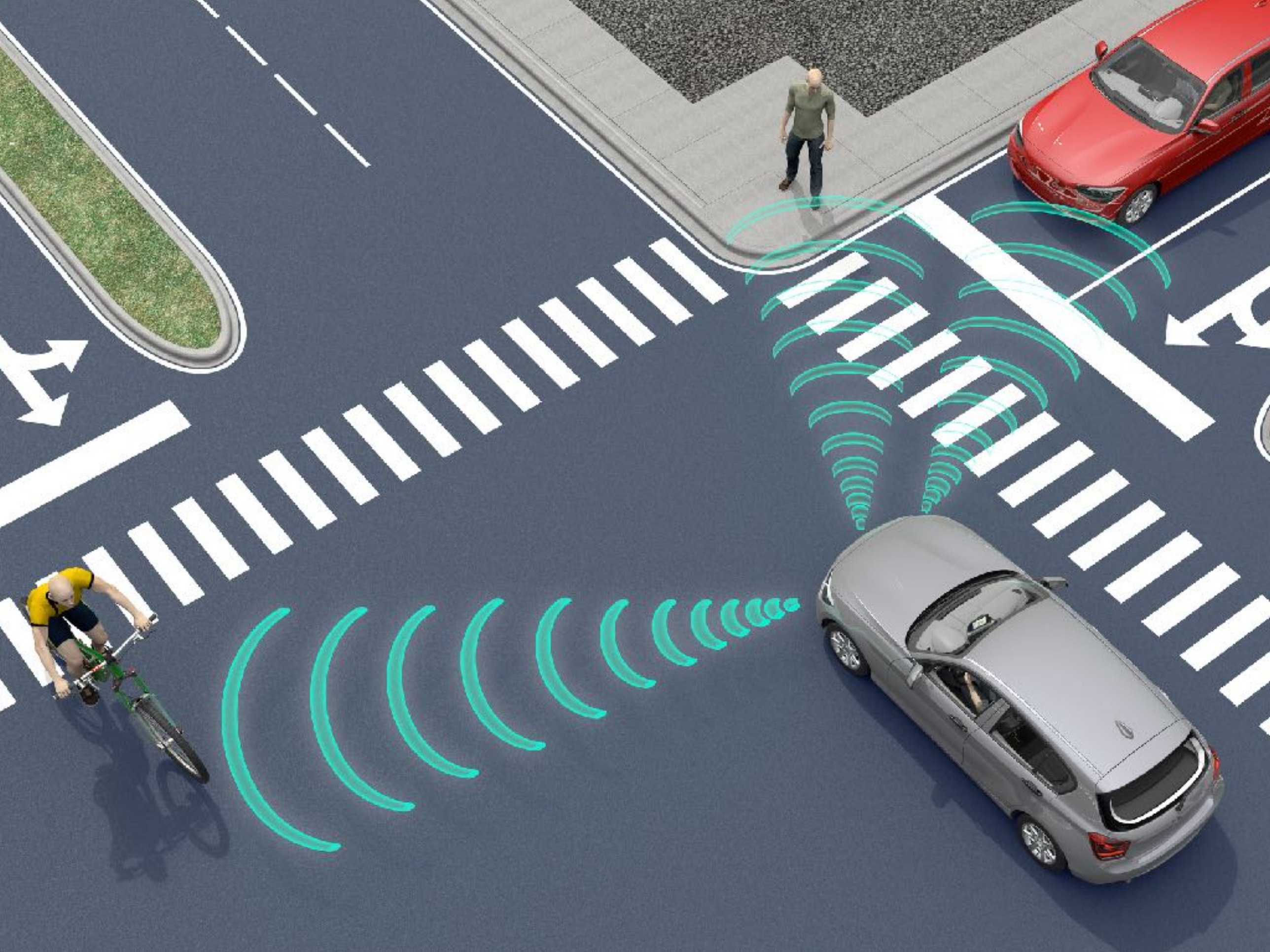
Threat modeling IoT

Grega Prešeren

Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/411
root/00000000	Panasonic Printer	https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek	RealTek Routers	
admin/1111111	Samsung IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdipc	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI
admin/smcadmin	SMC Routers	http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb	Toshiba Network Camera	http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt	Ubiquiti AirOS Router	http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor	VideoIQ	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>	Vivotek IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111	Xerox printers, et. al	https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521	ZTE Router	http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html

Source: krebsonsecurity.com



External interfaces

APIs, SDKs and gateways that act as interfaces for 3rd party systems (e.g., ERP, CRM)

Analytics

Algorithms for advanced calculations and machine learning

Additional tools

Further development tools (e.g., app prototyping, access management, reporting)

Data visualization

Graphical depiction of (real-time) sensor data

Processing & action management

Rule engine that allows for (real-time) actions based on incoming sensor & device data

Device management

Backend tool for the management of device status, remote software deployment and updates

Connectivity & Normalization

Agents and libraries that ensure constant object connectivity and harmonized data formats

Database

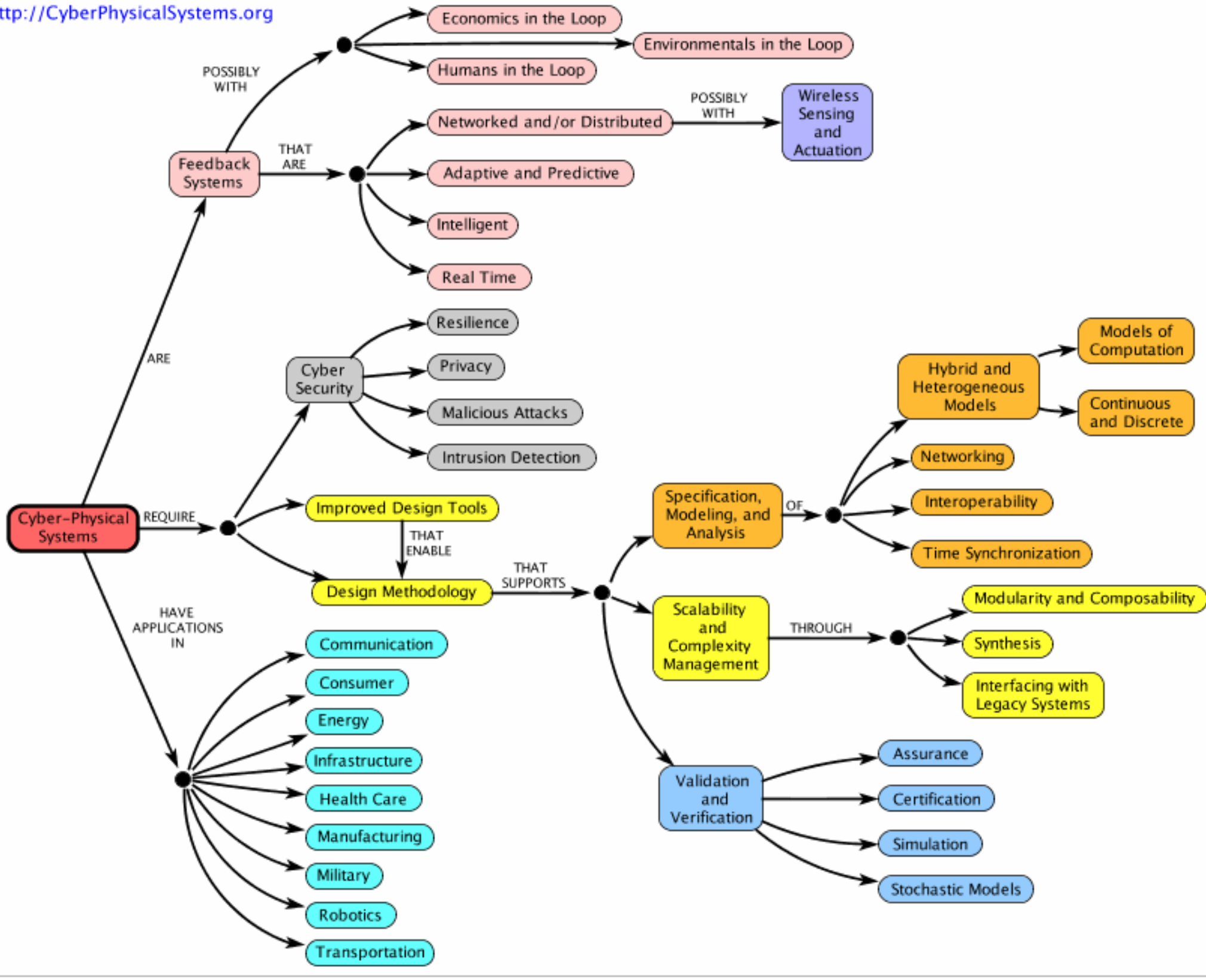
Repository that stores the important data sets

Source: iot-analytics.com

Cyber-Physical Systems – a Concept Map

See authors and contributors.

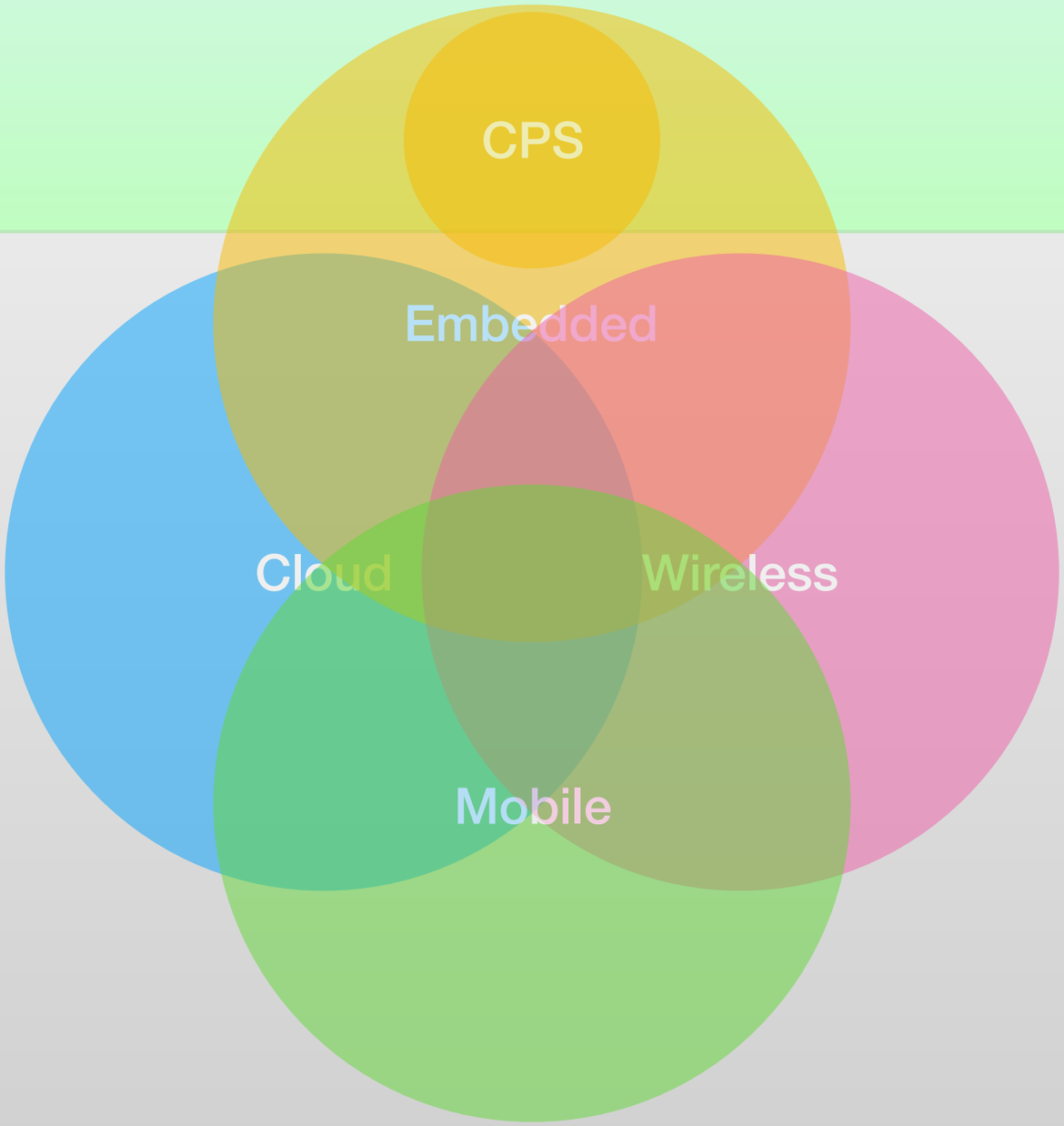
http://CyberPhysicalSystems.org



Source: cyberphysicalsystems.org

Physical

Cyber



SECURITY

BY DESIGN

START TO FINISH

END TO END

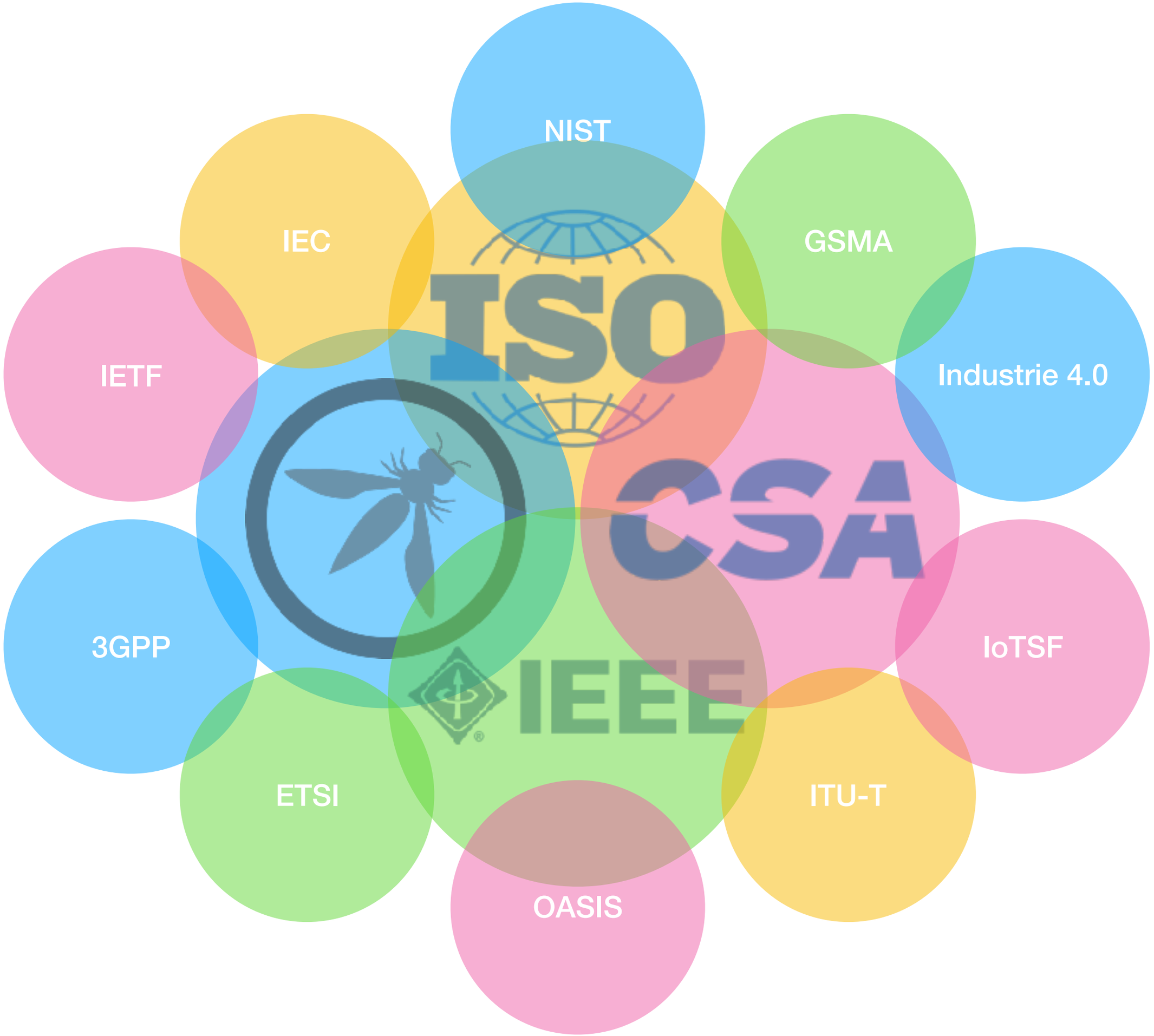
DEFENSE

IN DEPTH

START TO FINISH

END TO END


delete
enter


NIST
IEC
GSMA
IETF
ISO
Industrie 4.0
CSA
3GPP
IoTSF
IEEE
ETSI
ITU-T
OASIS

OWASP IoT Top Ten

I1 Insecure Web Inter

I2 Insufficient Authen

I3 Insecure Network S

I4 Lack of Transport P

I5 Privacy Concerns

I6 Insecure Cloud Inte

I7 Insecure Mobile Int

I8 Insufficient Securit

I9 Insecure Software/

I10 Poor Physical Security

A1 Injection

A2 Broken Authentication and Session Management

R1 Accountability and Data Ownership

R2 User Identity Federation

R3 Regulatory Compliance

R4 Business Continuity and Resiliency

R5 User Privacy and Secondary Usage of Data

R6 Service and Data Integration

R7 Multi Tenancy and Physical Security

R8 Incidence Analysis and Forensic Support

R9 Infrastructure Security

R10 Non Production Environment Exposure

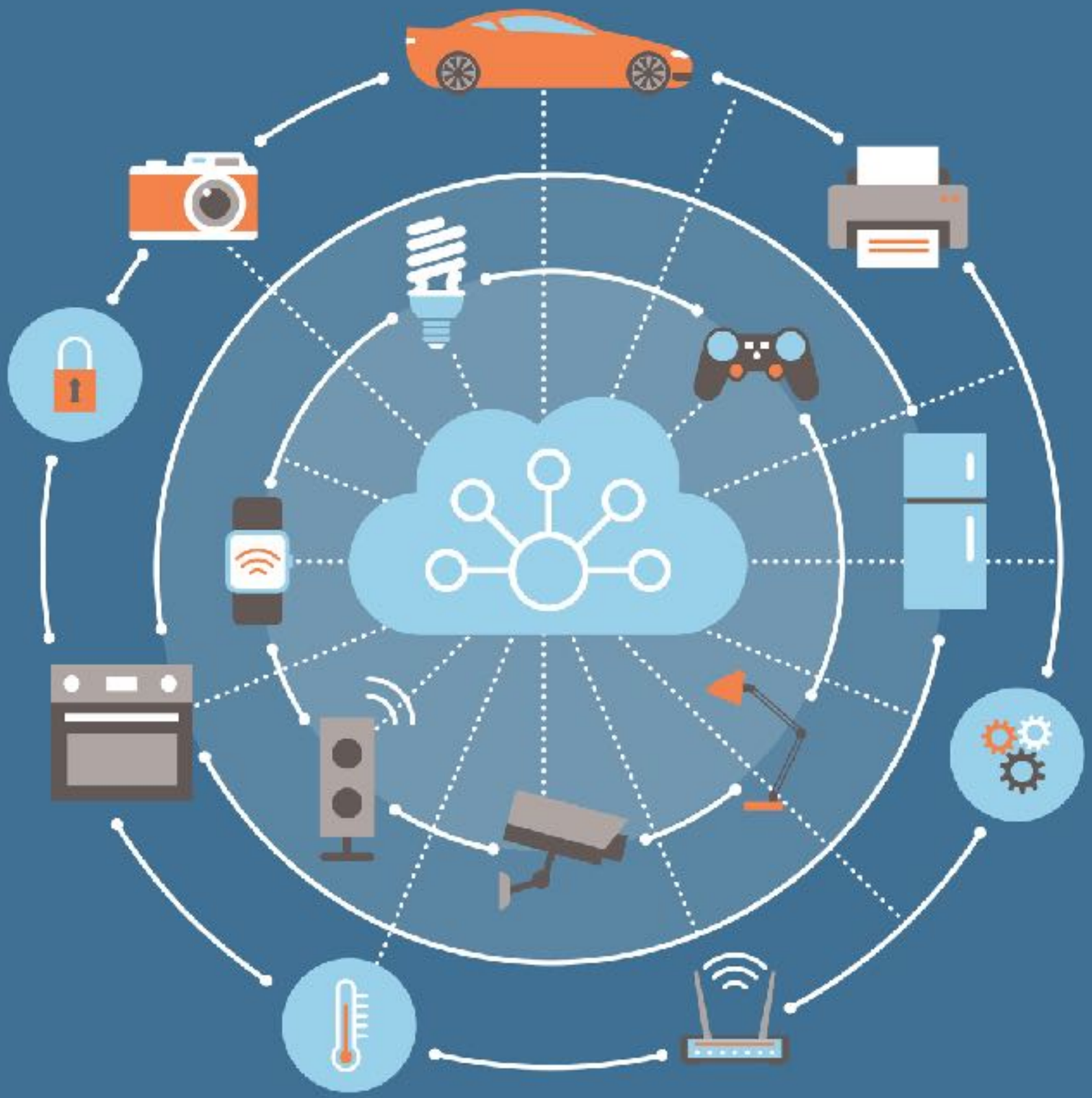
Internet of Things security architecture

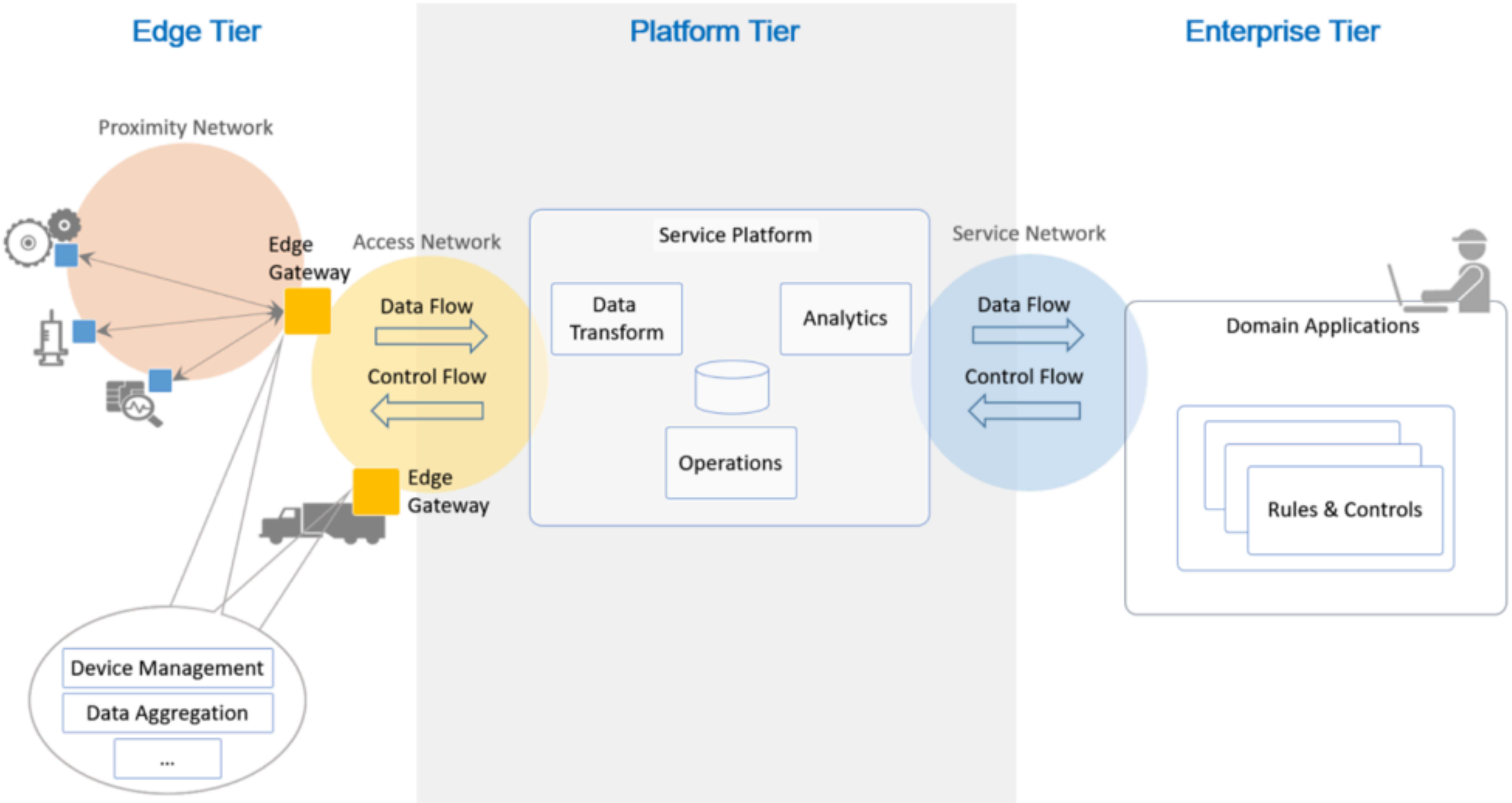
07/03/2017 • 24 minutes to read • Contributors

When designing a system, it is important to understand the potential threats to that system, and add appropriate defenses accordingly, as the system is designed and architected. It is particularly important to design the product from the start with security in mind because understanding how an attacker might be able to compromise a system helps make sure appropriate mitigations are in place from the beginning.

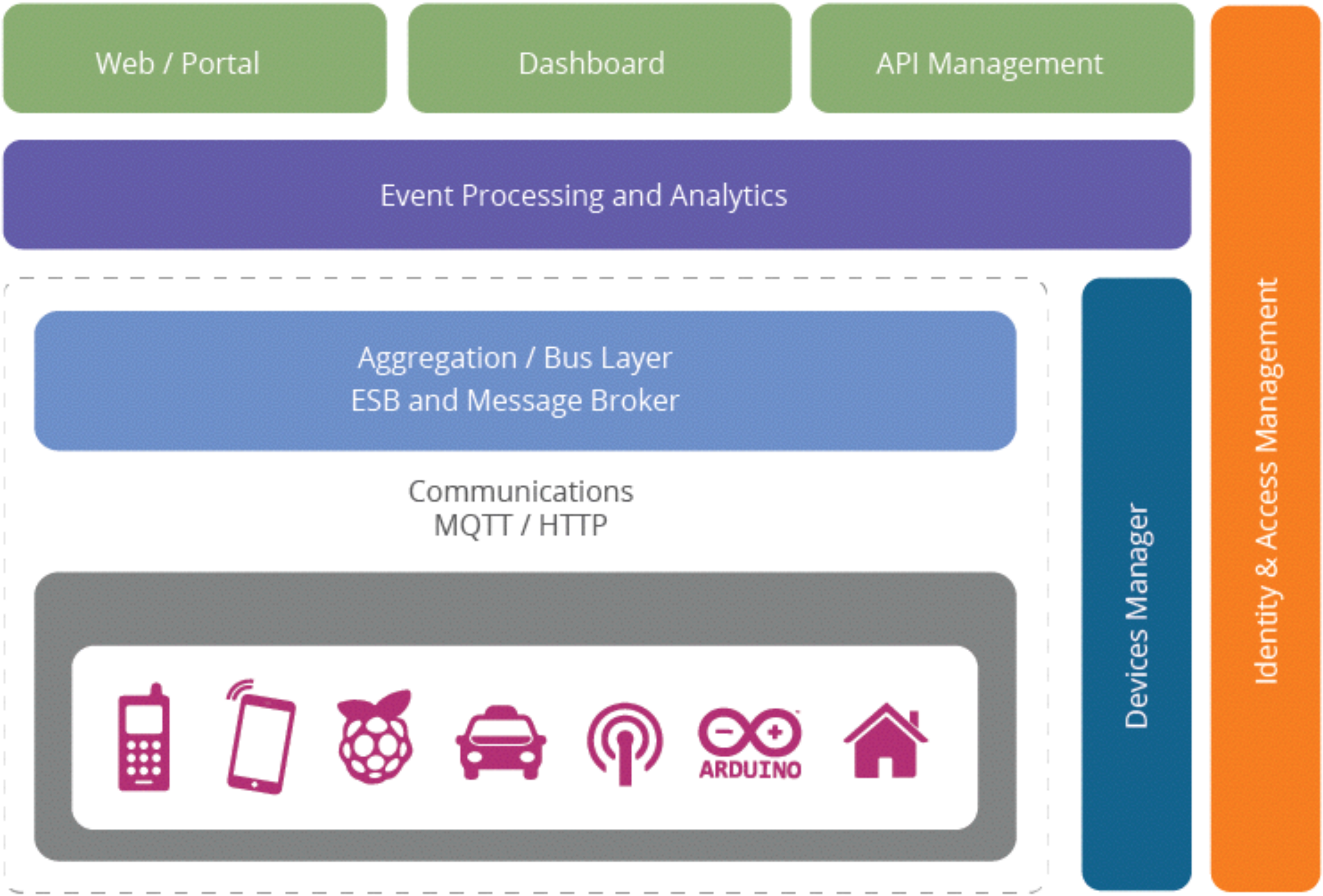
Security starts with a threat model

Microsoft has long used threat models for its products and has made the company's threat modeling process publically available. The company experience demonstrates that the modeling has unexpected benefits beyond the immediate understanding of what threats are the most concerning. For example, it also creates an avenue for an open discussion with others outside the development team, which can lead to new ideas and improvements in the product.

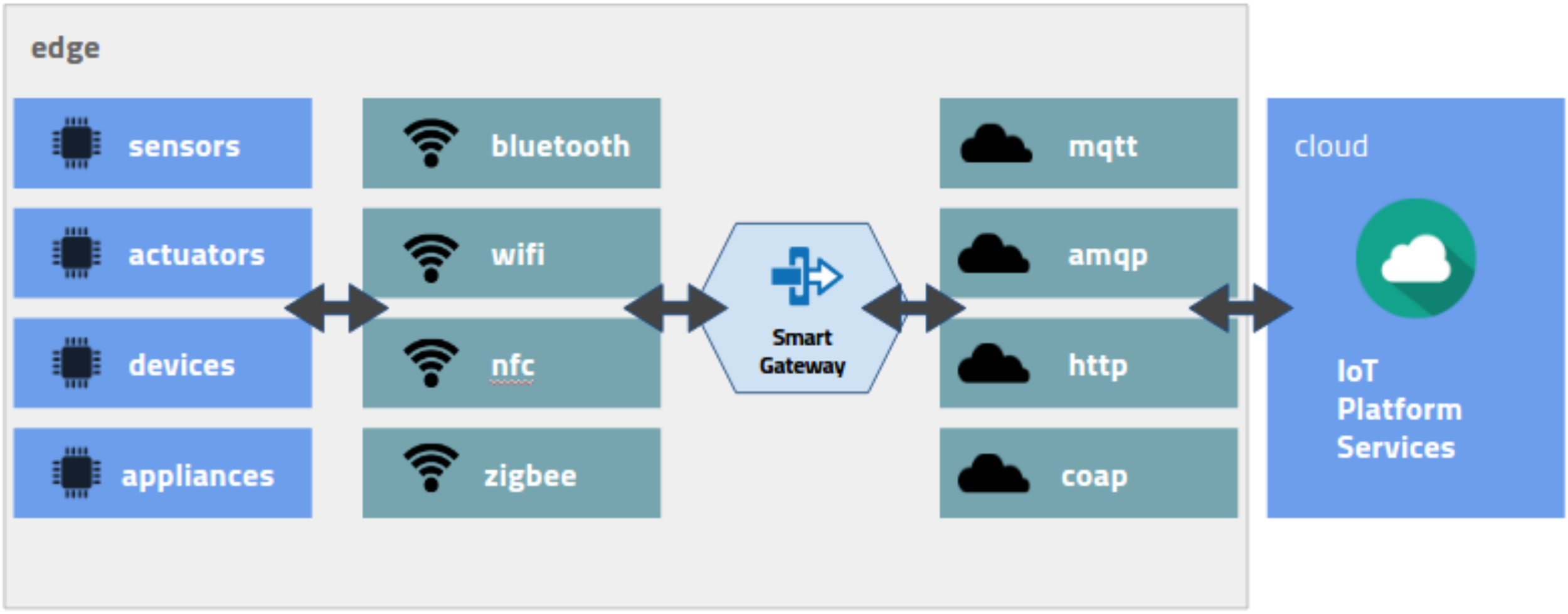




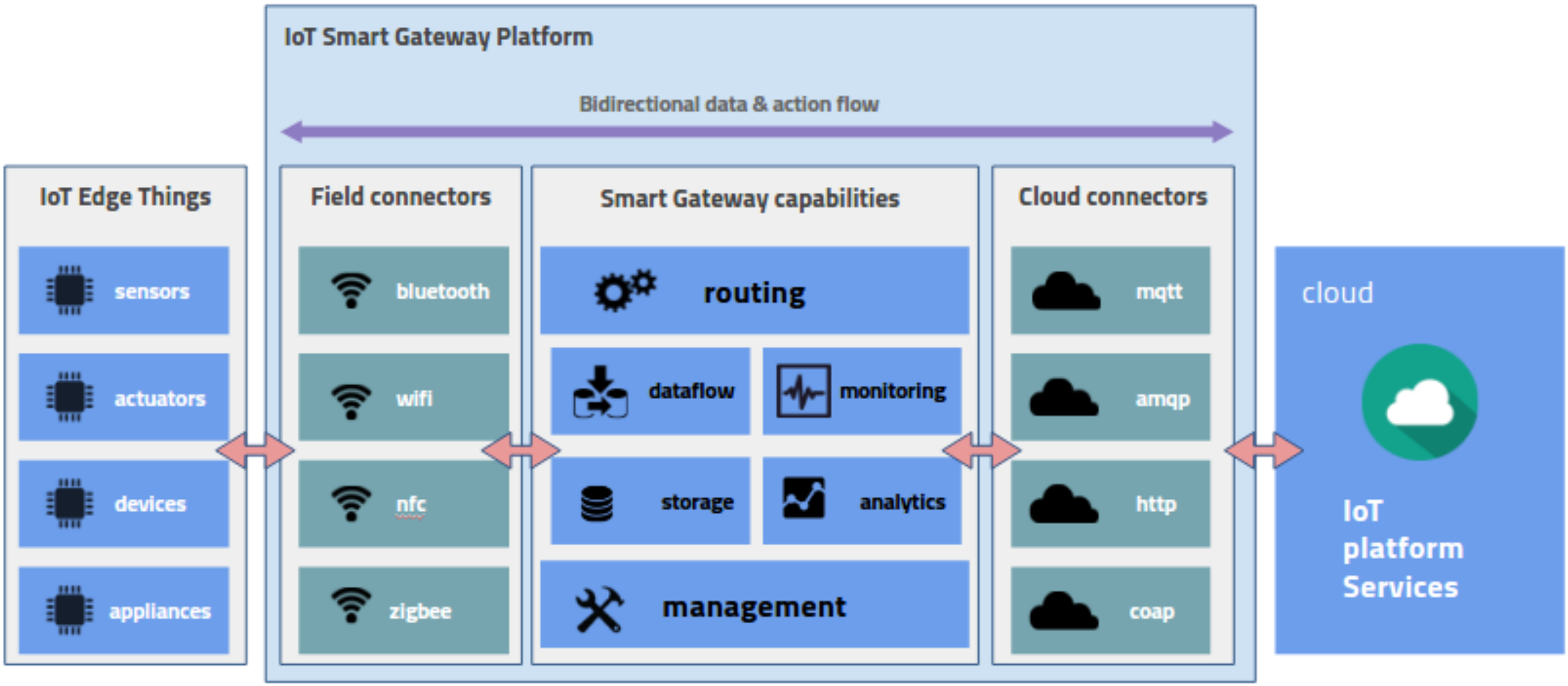
Source: iiconsortium.org



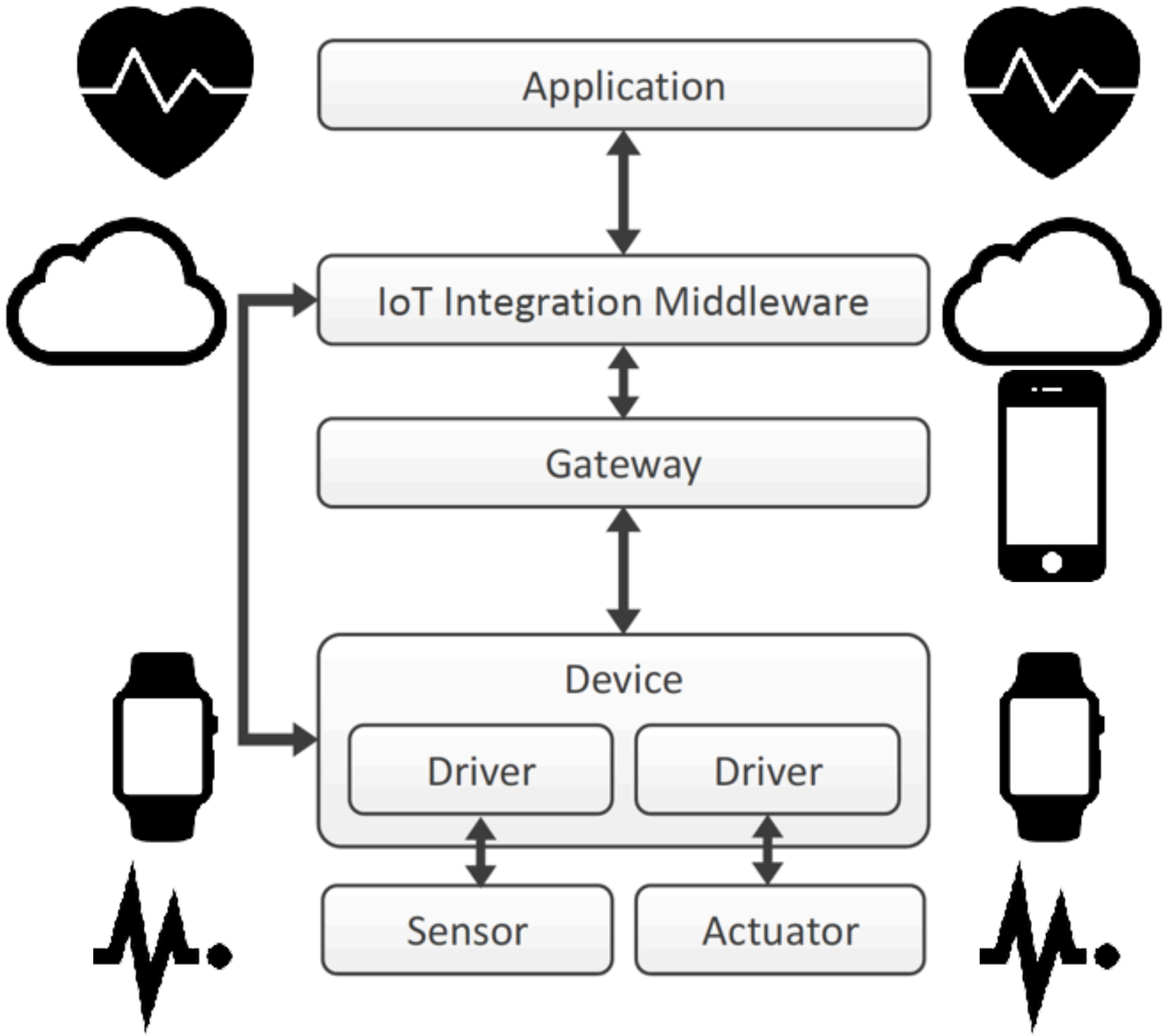
Source: wso2.com



Source: linkedin.com



Source: [linkedin.com]



Source: ieee.com

BRUCE WAYNE/BATMAN'S THREAT MODEL

ASSETS

BAT CAVE

ALFRED

EMAILS

TEXTS

PROTECTION

SECURITY SYSTEM

HIDE LOCATION

ENCRYPTION

THREATS

POLICE

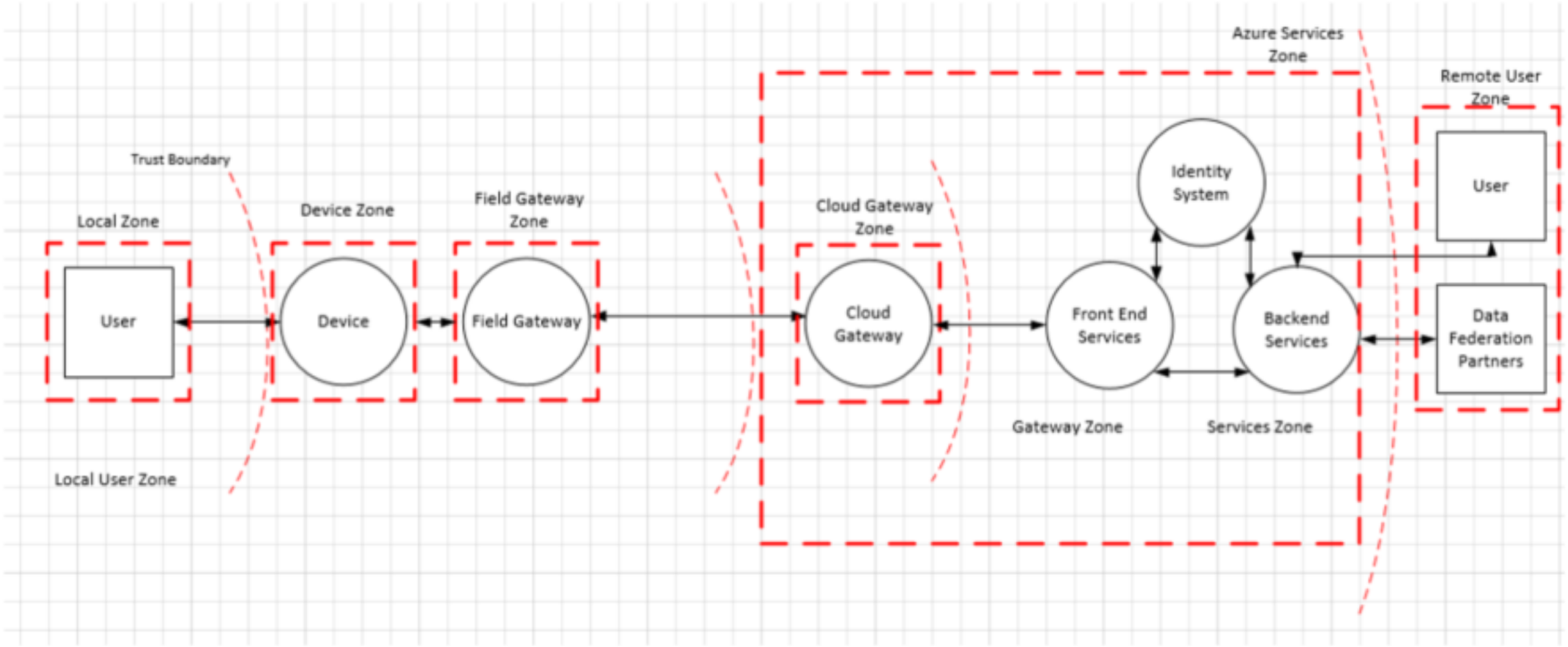
THE JOKER

JOURNALISTS

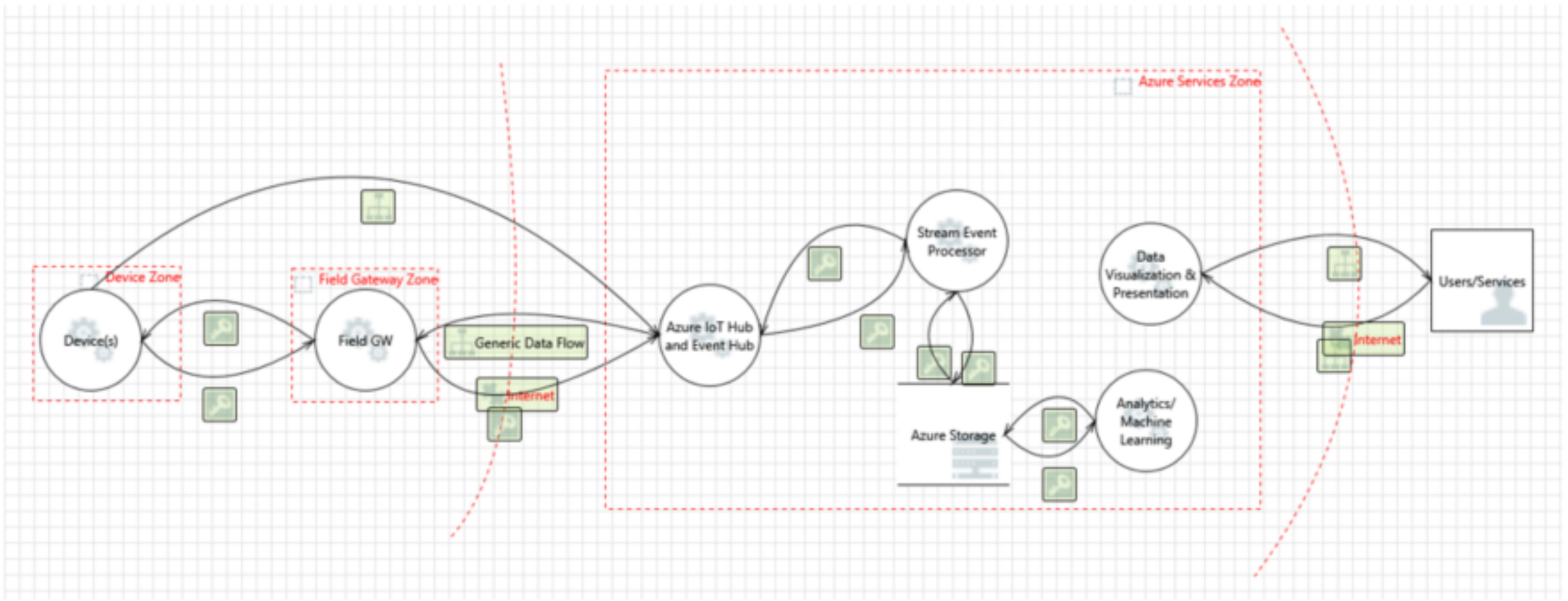
LOW RISK

MED RISK

HIGH RISK



Source: [microsoft.com]



Source: [microsoft.com]

EDGE TIER

PLATFORM TIER

ENTERPRISE TIER

Sensor
Actuator

Device
Thing
Controller

Gateway

Middleware

Application

PROXIMITY NETWORK

PROXIMITY NETWORK

ACCESS NETWORK (Internet)

INGESTION

STORAGE

AI / ANALYTICS

MANAGEMENT

VISUALIZATION

SERVICE NETWORK (Internet)

ENTERPRISE