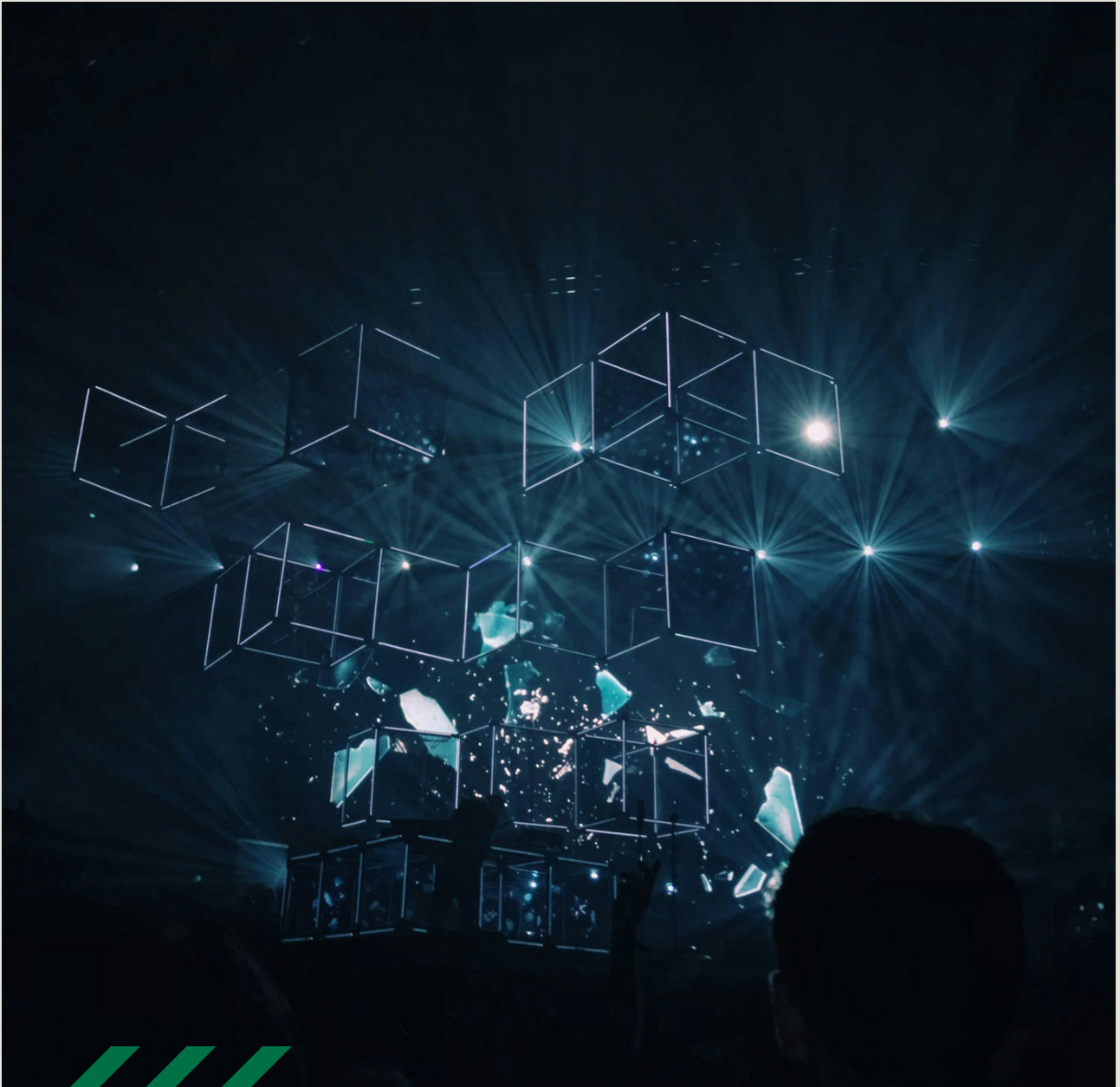


INNOVATION IMAGINATION  
TECHNOLOGY FORESIGHT



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

armasuisse

THE FUTURE OF

# Internet of Things

FOR MILITARY ENVIRONMENTS



# Disclaimer

---

This strategic foresight document is the result of a research project funded by the technology foresight program of armasuisse Science and Technology. It is a thematic research on the future of the Internet of Things at the technological level and its implications for security and defence.

The purpose is to get prepared to anticipate new technological solutions that might pop-up somewhere in the future, based on some of today's knowledge. Great care has been taken to consider only unclassified public information, avoiding any intellectual property unauthorized disclosure.

Conflict of interest: The author declare that he has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this document.

Federal Office for Defence Procurement  
armasuisse  
Science and Technology  
Feuerwerkerstrasse 39  
3602 Thun

ISBN: 978-3-9525890-8-3

contact: [quentin.ladetto@armasuisse.ch](mailto:quentin.ladetto@armasuisse.ch)

© armasuisse – Bern, 2024

# Foreword

---

For decades, the concept of the Internet of Things (IoT) has steadily transitioned from a futuristic vision to an everyday reality. When combined with military environments, IoT promises to revolutionize defence strategies, operational efficiency, and battlefield dynamics.

While the topic of IoT is not new, we explore in this document transformative intersections, revisiting both the foundational elements and emerging trends that will shape the future of military IoT. Coming back to the basics presenting and analysing core IoT components – semiconductors, sensors, energy, antenna, cyber-security, edge-computing - we aim to better understand how developments in artificial intelligence, machine learning, and wireless transmissions will enhance military capabilities.

Peppering the report with «what if» situations, we hope to project readers into different possible futures. These speculative elements challenge conventional thinking and inspire a forward-looking mindset. They encourage readers to envision how dual- or multiple-use products or functionalities might reshape military operations in unprecedented ways.

Join us on this journey through the past, present, and future of IoT in military contexts, where each technological breakthrough holds the potential to redefine our approach to security, efficiency, and reliability in the digital age.

This document is brought to you by the technology foresight research program of armasuisse Science and Technology. The program aims to inspire, inform and instruct the armed forces and its various stakeholders about the opportunities and threats brought about by the use of technology. Through its products and activities, it contributes to a collaborative and participative endeavour that strengthens Switzerland's defence capability.

We wish you an inspiring read.

Foresightfully yours,



Dr. Quentin Ladetto  
Head of Technology Foresight  
armasuisse Science & Technology

<https://deftech.ch> | <https://armasuisse.ch>

# Purpose

---

Information has always been at the center of warfare. Sharing real-time information between sectors is a critical aspect involved in managing the battlefield.

Many innovative tools, protocols and algorithms overwhelm the present of the IOT\*. Shaping the futurs with all of them is like resolving a Rubik's multicahedron\*\* with n particles on each side. By chance, several patterns already exist between the sides, improving the chances to trace a path that'll lead somewhere.

IOT is a complex mix of interdisciplinary domains like mobile computing, software architectures, embedded firmware, wireless communication technologies, security, networking, sensing technologies, energy efficiency, information management, data analytics and artificial intelligence.

As the society adapts to an increasingly complex security environment, it is imperative to understand how to harness the power of technological improvements and what to operate within new geopolitical contexts. Investments in C4ISR systems and infrastructure to analyze and disseminate data is how advanced military organizations will make the difference.

Fasten your seat belts, we're engaging in a fascinating road-trip. From vision to execution, from chip to solution, get ready. The world of augmented possibilities gets available to shape our Futurs.

Olivier Desjeux

July 2024

olivier.desjeux@advancedvalueglobal.com

---

*"The past is a present for the future."*

*André Malraux*

\*Since this publication is about IOT, it is assumed that the reader understands, or at least associates once for all this acronym with "Internet Of Things".

\*\*Multicahedron, plausible word describing a geometrical shape with multiple faces, the multiple being presumably a large figure. By the way, n is most likely also a large figure.

---

*"Diving into the IOT universe shares  
common grounds with science-fiction  
UNTIL IT GETS REAL."*

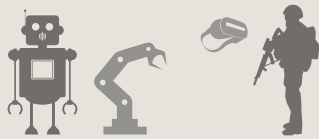
# Taxonomy

The IOT covers a very wide range of equally important expertise. The purpose of this document is to dive into the technology subsystems required for the success of a complete IOT system.

## PLATFORMS



Unmanned Vehicles



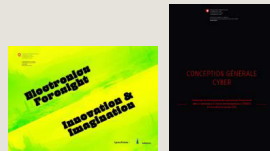
Robotics

Augmented Soldier



Supply-Chain

## TECHNOLOGIES



Semiconductor



Sensor



Energy



Edge-Computing

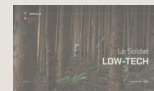


Cyber-Security



Antenna

## ENABLERS



Data



Standards



Cloud Computing/  
Storage



Networks

**EFFICIENT  
PLATFORMS**

rely  
on

**TECHNOLOGIES**

and

**ROBUST  
ENABLERS**





# Table of Contents

---

## I. Context

Internet of Military Things	14
Warfare of Things	15
Safety, Reliability, Risk	16
Remembering the Origins	18

## II. Technology Subsystems

Semiconductor	22
Antenna	34
Energy	40
Sensor	46
Cyber-Security	54
Edge-Computing	60

## III. Future Trends and Innovations

Build your own	66
Technology at Play	67
What if...?	70

## IV: Appendix : More about

1. Mobile Communications from its origins	74
2. Symmetric vs. Asymmetric cryptography	76

## V. Glossary

79

## VI. Sources

83





CHAPTER I  
**Context**

# Context

## IOT EXPECTATIONS

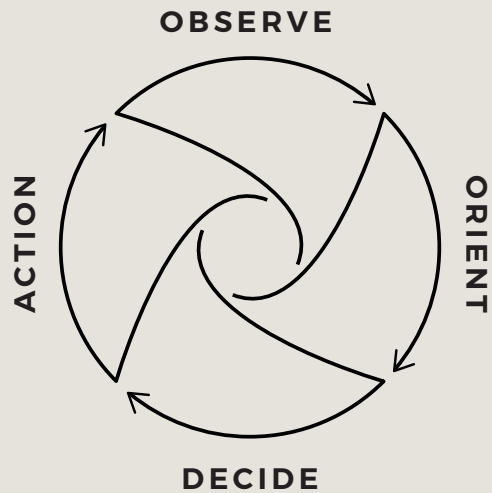
---

IOT solutions carries tremendous potential in modern warfare systems, able to handle great quantity of signals within in depth and intense combat situations, in the heart of the battlefield, on the friend or foe side.

### IMPROVE SUPERIORITY

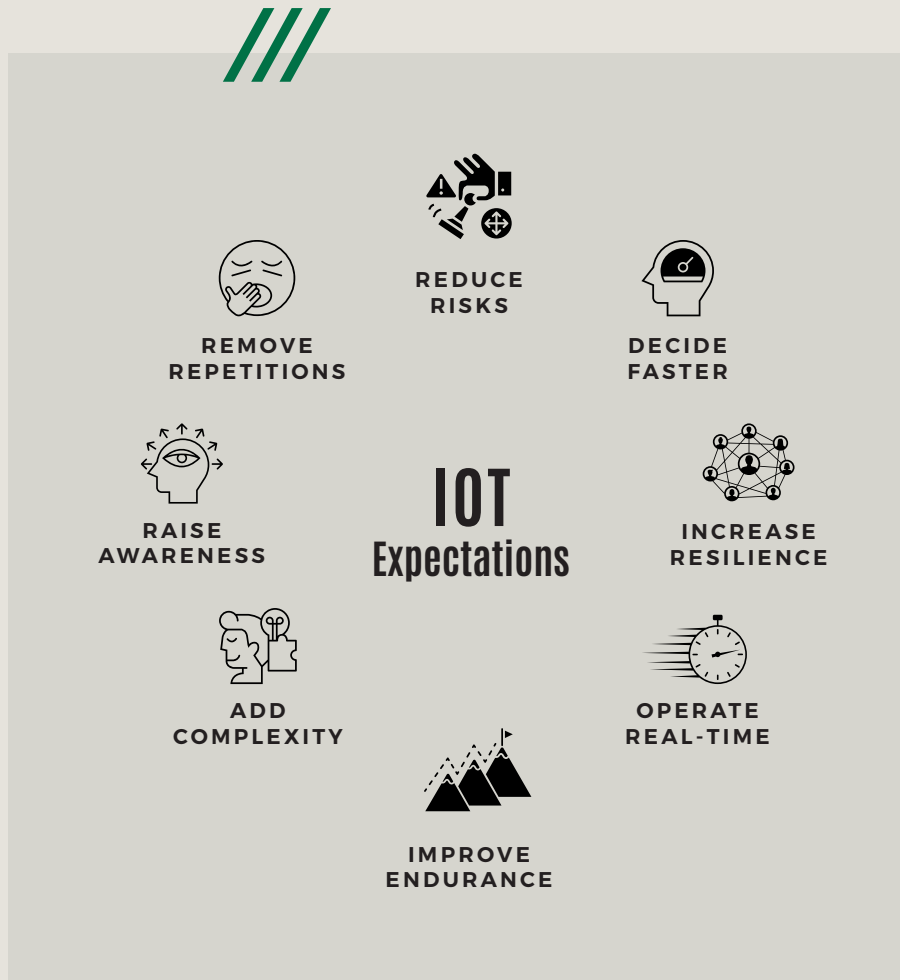
- Technological
- Temporal
- Spatial

Move **Faster** and with **Greater Precision** along the OODA Loop.



Exposed to the light of defence expectations, the requirement for IOT implementation is to provide strategic advantages for warfare superiority. Within the context of foresight analysis, the items of the taxonomy are individually considered, looking-out for the drivers and identifying trends having the potential to alter the course of the futurs.

The possible combination of drivers and trends of individual technologies should not be taken for granted. However this combinatory game is a way to stimulate the disruption along the course of linear evolutions. Playing with ideas, What If innovative practices could be generated?



*"The skillfull leader subdues the enemy's troops without any fighting; he captures their cities without laying siege to them; he overthrows their kingdom without lengthy operations in the field... Without losing a man, his triumph will be complete."*

*Sun Tzu, The Art of War*

# Internet of Military Things

COHESIVE NETWORK IMPROVES SITUATIONAL AWARENESS,  
RISK ASSESSMENT AND RESPONSE TIME

## IOT Sensing

Used to **Observe** information from the field, sensors commonly operate off-grid to nurture the **Orientation** with the following key drivers:

- Mobility
- Miniaturisation
- Ultra Low Power

## IOT ACTUATING

The actuators are executing the orders coming from either the algorithm or the operator. They transform a **Decision** into an **Action** with the following key drivers:

- Mobility
- Real-Time
- Low Power

## WHAT IF...

*... smart-dust sensors could be spread disseminated and self-organize their reports. Purpose: provide real-time data to complement situational awareness?*

## Common Drivers

Non negotiable features required for IOT components operated in the military and defence context:

- Safety
- Security
- Reliability

## WHAT IF...

*... the cornerstone of actuators relies on the order received commonly by wireless activity. Bio-mimicry suggests protein activation to convey messages?*

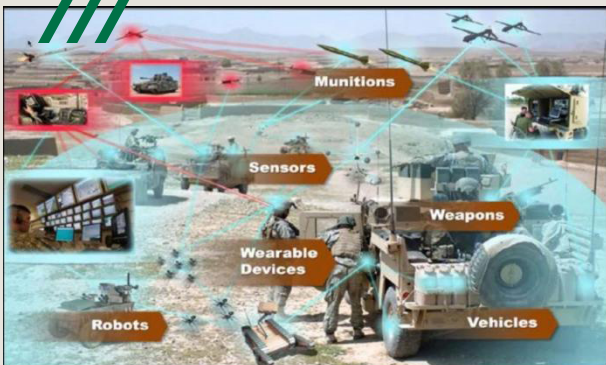


Photo credit U.S. Army, Internet of Battlefield Things (IoBT) Collaborative Research Alliance (CRA) Opportunity Day, March 27, 2017

# Warfare of Things

---

## PRIVATE SECTOR ORIGINS

In the past, the technology was driven by military innovations, especially when dealing with radiofrequency equipment. Today, most, if not all, of current IOT equipment and applications are driven by the private sector, with the military lagging behind in everyday operations. The military sector has an opportunity to capture the experience from existing IOT by partnering with the private sector. The adoption of IOT enabled practices that consider the technological particularities of tactical systems has become a key factor of success in the Internet of Military Things. However, military operations require operational specificities. Security, safety, robustness, interoperability challenges get challenged for adoption of new IOT systems.

IOT enabled data is useful for establishing advanced situational awareness in the area of operations.

The decision makers activity is based on real-time observation and analysis generated by integrating data from unmanned sensors and reports from the field.

The decision makers benefit from a wide range of information supplied by sensors and cameras dispatched on the battlefield and surroundings, also dispatched on manned or unmanned vehicles or soldiers.

These equipment capture the mission landscape and feed data to a forward base, where it can be merged with data from other sources.

## INTELLIGENCE IOT OSINT

Artificial intelligence (AI) and specifically machine learning (ML) improvements present significant opportunities to capitalize on the value of open-source intelligence (OSINT). Technologies such as IOT contribute to maintaining an Intelligence superiority. However, the risks in the open source domain, including the provenance and validity of collected information must be carefully scrutinized. Concurrently, the Defence must re-imagine its relationships with industry and academia to leverage the capabilities applied in the private sector. Because of the unclassified nature of open source information, OSINT presents a unique opportunity to explore new partnership models to speed the adoption of new tools, bearing in mind the risk to have bad or corrupted data.

# Safety, Reliability, Risk

IOT equipment for military applications often find their inspiration from the private sector, with a preference for products and systems designed for constrained applications. Specific methods have been developed in a set of standards under the umbrella of IEC61503 in Europe. They describe the process to apply, design, deploy and maintain automatic safety-related systems.

**/// The fundamental concept is that any safety-related system must work correctly or fail in a predictable (safe) way.**

The Safety Integrity Level (SIL) is a classification for such system. A higher SIL Level means a greater process hazard and a higher level of protection required. Applicable on request by the procurement to products or systems like IOT solutions, the minimum military requirement sits between the level 2 and 3. Requiring the level 4 is possible, however, procurement exaggeration might lead to unbearable costs and restrictions of usage.

Frequency	5	SIL 3	SIL 4	X	X	X
	4	SIL 2	SIL 3	SIL 4	X	X
	3	SIL 1	SIL 2	SIL 3	SIL 4	X
	2	-	SIL 1	SIL 2	SIL 3	SIL 4
	1	-	-	SIL 1	SIL 2	SIL 3
		1	2	3	4	5
	Severity of Consequence					





Source Unsplash

## Risk

***"The effect of uncertainty on an organization's ability to meet its objectives."***

*Definition from ISO31000*

---

Central to the standard are the concepts of probabilistic risk for each safety function. The risk is a function of likelihood of the hazardous event and its consequence severity. The outcome is the risk assessment matrix pictured on previous page.

**1. What can go wrong ?**

**2. How likely is it to go wrong ?**

**3. If it does go wrong, what are the consequences?**

# Remembering the Origins

---

*"If we had computers that knew everything there was to know about things – using data they gathered without any help from us – we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory. RFID and sensor technology enable computers to observe, identify and understand the world without the limitations of human entered data."*

*MIT AutoID Lab, Kevin Ashton 1999*

**This bold statement from Kevin Ashton was definitely visionary, carrying flavors of utopia. Let's imagine today's desirable future of IOT.**



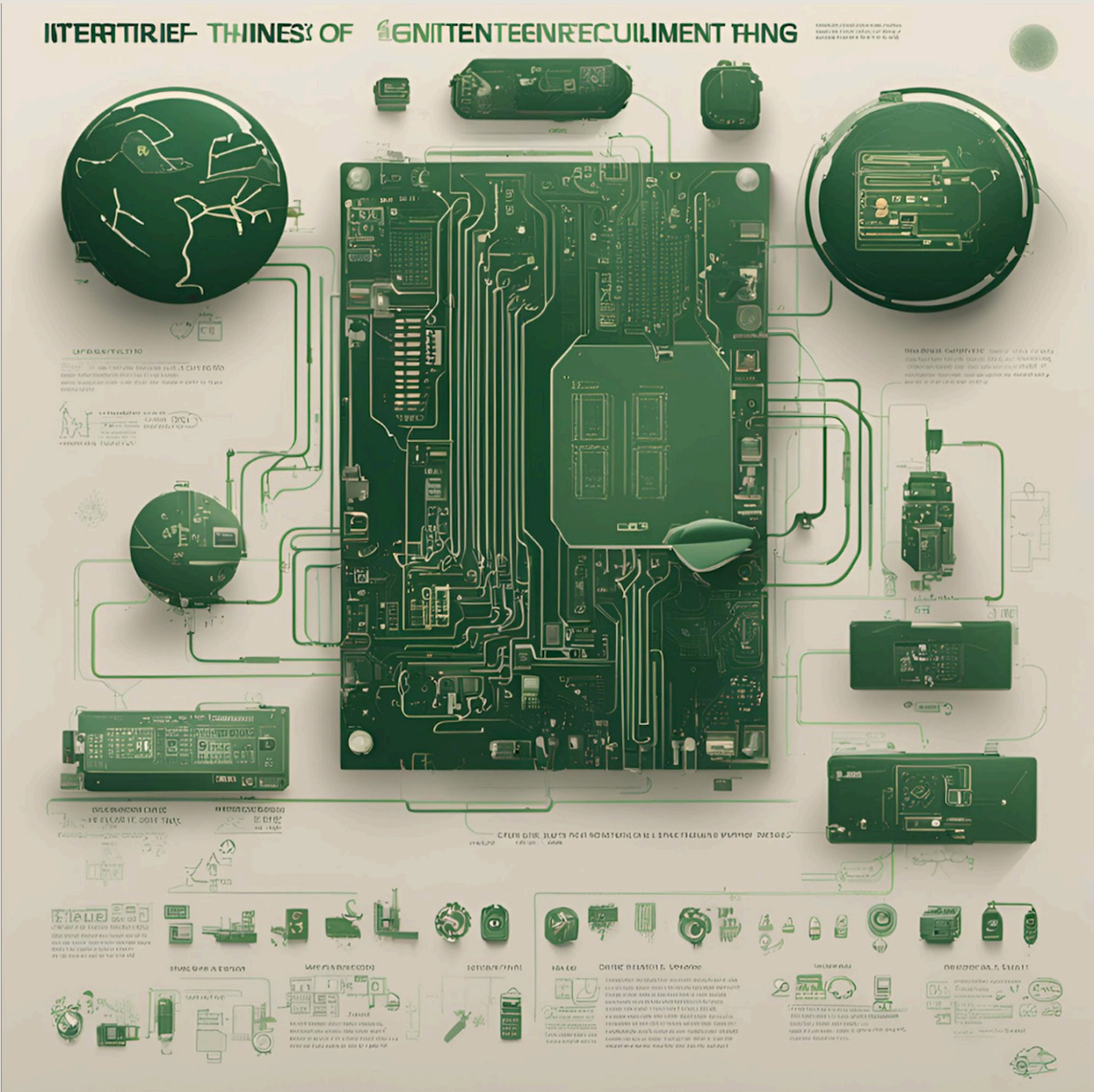
## Rewind the clocks, back in the early 2000's :

---

- **WWW** Companies just started operating static web sites
- **PTT** Former national Post and Telecommunication operators just became private (in Switzerland, from PTT to Swisscom)
- **GSM** The mobile network standard in Europe just commercially launched GSM 3G

Connecting to a WiFi hotspot when travelling was a difficult, techy, and ultimately expensive experience.





CHAPTER II

# Technology Subsystems

# Semiconductor Technology

## DRIVERS

## Driven by 3 Industries

COMPUTATION, WIRELESS, AUTOMOTIVE

**1  $\mu$ m**  
4"

**0.5  $\mu$ m**  
6"

**0.18  $\mu$ m**  
6"

**65 nm**  
8"

**SEMI CONDUCTOR FEATURE SIZE**  
wafer diameter



**1G**



**2G**



**3G**

**VOICE CALL**

**1980**

**SMS**

**1990**

**INTERNET 1.0**

**2000**

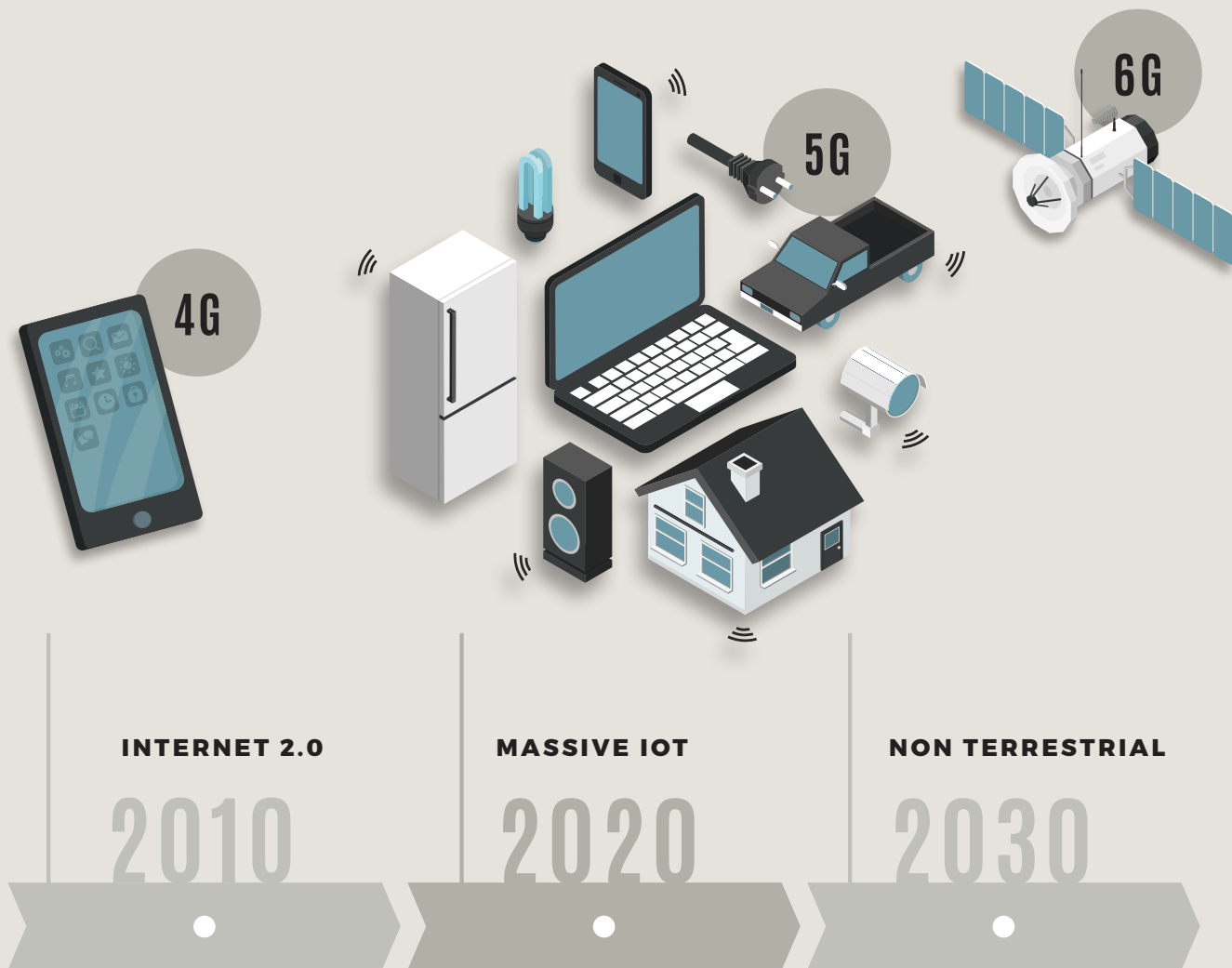
**40 NM**  
12"

**22 NM**  
12"

**5 NM**  
12"

**2 NM**  
12"

**SUB-NM**  
510 x 515

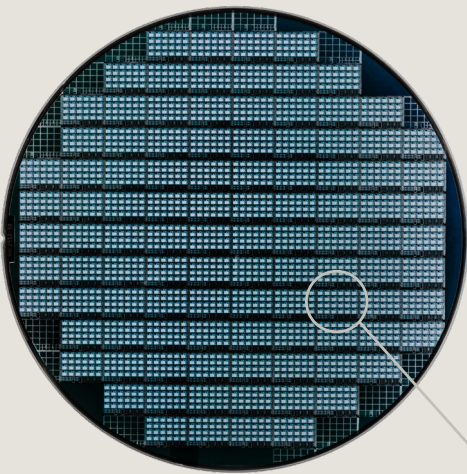


# From Wafer to Chip...

BY THE WAY, WHAT IS A "CHIP"? WHERE DOES IT COME FROM?  
HOW IS IT UTILIZED?

## Wafer

Slice of pure silicon\*



Diam. 12" = 300mm

## QUIZ

How many dies on this wafer?

Total number of dies if the production batch had 12 wafers, with a yield of 98%?

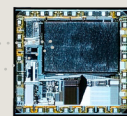


## USAGE

Typical chip found in a commercial IOT equipment



Feature size



4 x 4.7 mm

## Semiconductor

Chip = Die = Integrated Circuit = IC

Photos credit from the author



# ...From Chip to Solution

Semiconductor chips stand at the heart of complex IOT Solutions.

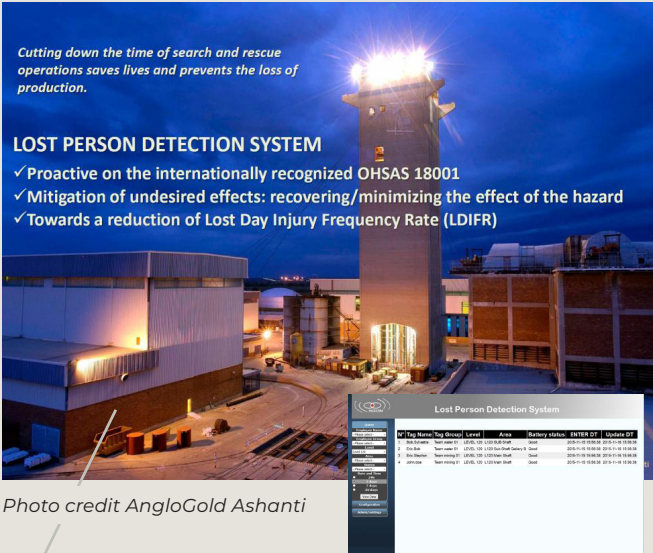
Each chip includes Millions of transistors frequently combined with analog functions.

### IOT Solution

*Cutting down the time of search and rescue operations saves lives and prevents the loss of production.*

#### LOST PERSON DETECTION SYSTEM

- ✓ Proactive on the internationally recognized OHSAS 18001
- ✓ Mitigation of undesired effects: recovering/minimizing the effect of the hazard
- ✓ Towards a reduction of Lost Day Injury Frequency Rate (LDIFR)

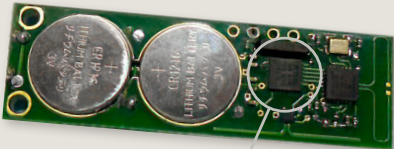


ID	Name	Tag	Status	Level	Area	Battery Status	ENTER DT	Update DT
1	John Doe	12345	Active	1	Plant	Full	2023-10-27 10:00:00	2023-10-27 10:00:00
2	Jane Smith	67890	Active	2	Warehouse	Low	2023-10-27 09:30:00	2023-10-27 09:30:00
3	Mike Brown	11111	Inactive	1	Plant	Full	2023-10-26 15:00:00	2023-10-26 15:00:00
4	Sarah White	22222	Active	3	Office	Full	2023-10-27 08:00:00	2023-10-27 08:00:00

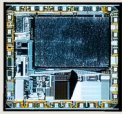
Photo credit AngloGold Ashanti



**Packaged IOT Product**



**Printed Circuit Board (PCB)**

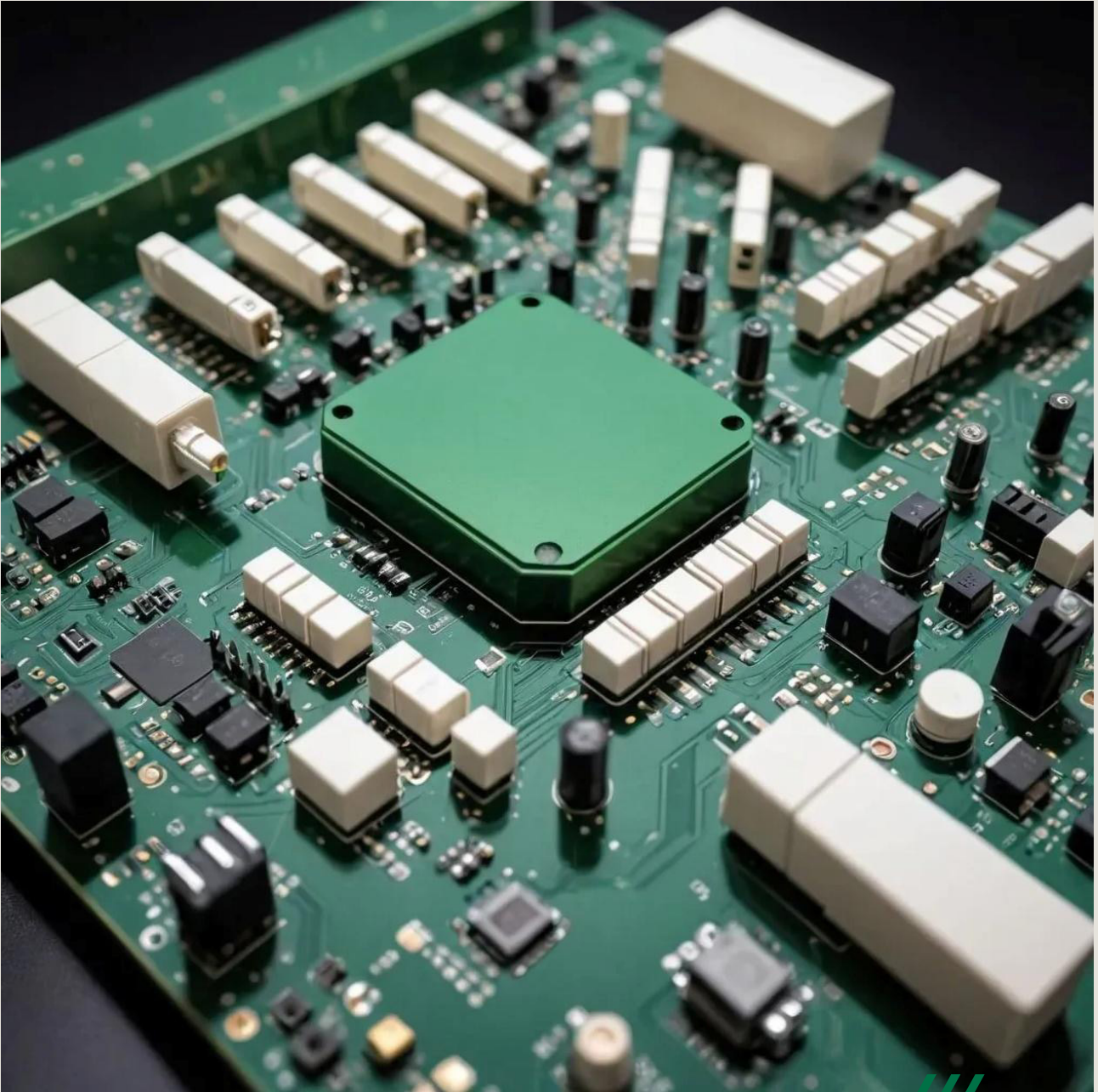


4 x 4.7 mm

### Semiconductor

Chip = Die = Integrated Circuit = IC

Photos credit from the author



Source photo.ai



**Silicon\***,  $\text{SiO}_2$ , has semiconductor properties. It is the eighth most common element in the universe by mass.

Slit in thin slices, called wafers, from single-crystal ingots, the pure silicon becomes the substrate for microelectronic components.

Complex and long processes are used, such as doping, ion implantation, etching, thin-film deposition of various materials, and photolithographic patterning to build as many as possible identical Integrated Circuits (IC), originating from the same design.

Ultimately, the individual Chips are separated by mechanical sawing. The operation is called Dicing.

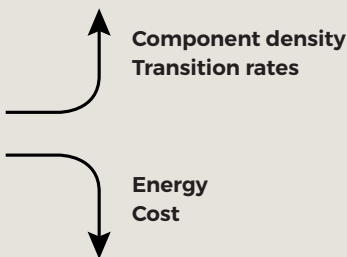
# Semiconductor

## DRIVERS

---

### Smaller

Since the early days of semiconductor, the feature size\* has always been a major driver of industries roadmaps, enabling:



Today's most competitive roadmaps target sub-nanometer\*\* feature size before 2030.

### Faster

While processing time is still a dominant driver as an answer to increasing complexity of algorithms and massive amount of data, reducing bottlenecks at memory access and inter-chip data transmission is actively considered.

### Low-Power

Dennard's scaling theory stated that the energy consumption of a chip would stay in proportion to its size. Shrinking feature sizes allows to increase computing capabilities without consuming more energy. Architectural solutions have become increasingly important and will play a larger role in the future.

*\*In the early days the Feature Size corresponded to the smallest feature on the chip. The gate length was often considered as the smallest feature. For example the 0.18um technology of early 2000's. Nowadays, the Feature Size is also called Node. With the 3D geometry of semiconductor structures and feature size getting below atomic dimension, the Node generation gets closer to a marketing name, even though it still relates to a feature.*

*\*\*Structures smaller than the electron coherence length (x100nm) are already produced. The semi-classical theory set in Boltzmann's equation, which served for more than half a century, is no longer in use. Increasing density towards atomic feature size requires quantum description, starting with formalism for non-interacting electrons.*

# Semiconductor

## IC OPTIONS

---

### ASIC, MCU Or FPGA ?\*

#### Let's go to the construction area.

The comparison is far from perfect but highlights several key differences:

#### ASIC

is like building a dream-house with specific bricks, custom made doors and windows. It is a very complex and unusual long work. At the end of the day the house perfectly matches the dreams.

Comparison's limits: while a dream-house is unique, ASICs are meant to be produced in multiple millions.

**Example:** an ASIC inside hearing aids discriminates the desired sound from the ambient noise, provides also wireless capabilities to interface with TVs or mobile phones.

#### FPGA

Lego bricks, doors and windows are used to shape the structure. They come in various shapes and colors and it is always possible to disassemble and rebuild part or all of the house.

**Example:** FPGAs are used in missiles for applications including guidance, control, targeting, and communications. Typical functions can be motor control, sensor inputs, signal processing and more.

#### MCU

Pre-built panels and wiring are brought to the construction site.

They are quickly assembled and configured. The house is functional, the owner can select a limited quantity of options and the construction time is unbeatable.

**Example:** Drone flight controller unit runs the speed of each motor and stability of the airframe.

---

Takeaway from the recent armasuisse Deftech Days about *Mission-Critical*: Defence equipment shall also take advantage of massively produced non DO-254 lightweight low-cost components, for improved agility and adaptability.

From electronic perspective, this statement suggests migrating from expensive FPGA based products towards highly integrated low-cost Micro-Controllers (MCU), or moving to ASICs.

Unlike FPGAs, an MCU or an ASIC may include the peripherals required to operate the final unit.

- Low-Power optimization
- Include external components
- Reduced geometrical volume
- Reduced weight

\*The abbreviations are described in the last section

	ASIC	MCU	FPGA
<b>NRE* Cost</b>	Red	Green	Yellow
<b>Time to Release</b>	Red	Green	Green
<b>Analog blocks</b>	Green	Yellow	Red
<b>Real-Time Operation</b>	Green	Yellow	Green
<b>Parallel Processing</b>	Green	Red	Green
<b>Energy Efficiency</b>	Green	Yellow	Red
<b>Finished product dimension</b>	Green	Yellow	Red
<b>Field re-programmable</b>	Yellow	Green	Green
<b>Typical quantities (Units)</b>	x 10M	In between	x 100

Generic table, exceptions can occur, depending on the application and type of MCU.

\*NRE: Non-Recurrent Engineering: Research and Development, engineering and tooling, cost and duration

# Semiconductor

## TRENDS

---

### eFPGA

The embedded FPGA (eFPGA) is an IP core integrated into an ASIC that offers the flexibility of programmable logic without the cost of FPGAs. Programmable logic is especially appealing for accelerating machine learning applications that need frequent updating.

An eFPGA provides the coverage required to launch products who will require onsite updates. Embedded FPGA helps programs consume less power and run faster.

### ADVANCED EDGE COMPUTING

With one of the key drivers being the very low-power of operation, combined with ultra fast processing time, the Edge Machine Learning is meant to play a pivotal role in the future of IOT. The increase of hardware processing density together with the algorithm optimization paves the way to tiny machine learning chips meant to provide microwatt powered artificial

intelligence capability directly at the physical sensor level.

The goal of On Device Learning (ODL) is to make sensors smarter and more efficient, observing changes in data collected, self-adjusting the sensor's operating model, and conveying through the network only the vital resulting information.

This trend is particularly strong for photonics sensors, prone to generate heavy loads of data. Edge AI saves wireless data communication and energy. Many algorithms will be transferred from cloud to edge.

### ADVANCED SECURITY

The proliferation of tiny nodes with autonomous capabilities provides countless entry points to potential cyber threats. What was initially the secret area of advanced hobbyists has become the playground of professional predators.

Advanced security is of utmost importance to preserve the integrity of the network and consequently the infrastructure within which the IOT takes place. Even a cyber attack on a single node may carry fatal casualties. Very capable advanced cryptographic functions are available at the hardware or embedded firmware level.

The trend is the early integration of appropriate security mechanisms in the architecture as one of the key requirements of the specification.

Advanced Edge Computing participates to data privacy, avoiding to convey loads of personal information on the network.

Source Pixabay



## ADVANCED TECHNOLOGIES

The progress in component density finds its limitation in the integration of analog components, who don't scale like digital transistors.

Moore Law focuses on shrinking the size of physical components while improving density and performance.

However, geometric scaling will eventually reach its limits as chips approach atomic levels of scale.

Samsung claims that "its 3 nm GAA process can achieve 45% reduced power usage, 23% improved performance and 16% smaller surface area compared to 5nm process".

The best way to think of these technologies is as more advanced technologies that enable smaller design features on a chip to the point where we will soon be reducing them to the size compared to single atoms.

*"The escalating demands for more memory, performance, and data rates necessitate groundbreaking progress in packaging technologies, process technology, and materials."*

*Bill En, AMD*

## ADVANCED MATERIALS

Silicon is the industrially preferred semi-conductor substrate material, with a stable native oxide (SiO<sub>2</sub>), which happens to be a good insulator prone to receiving positive (P) or negative (N) doping elements to create P-N semi-conductor junctions. However, one of the limitation to higher performance is the poor electron hole mobility in silicon. Also, silicon performance degrades at high temperatures, and exhibits limited photonics properties.

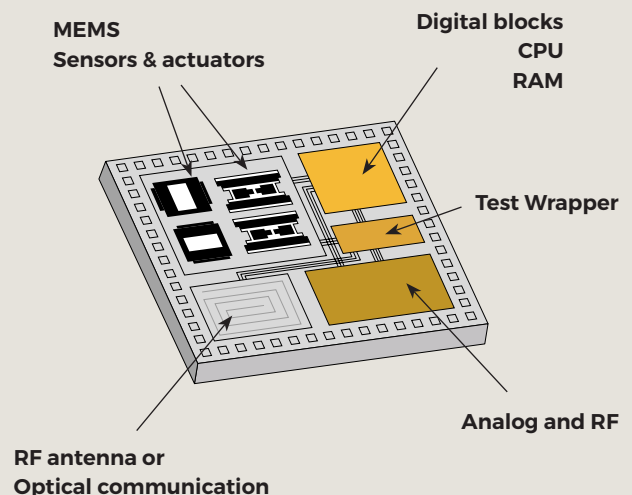
While industry stretches towards higher processing speed, higher interfacing speeds and/or higher power circuits, advanced materials are required to push-back its intrinsic limits.

The use of compound materials expands silicon's initial performances. Tracks like Synthetic Diamond offer promising futures for power electronics. Graphene, as a single sheet of carbon atoms, is explored for ultra-high conductivity semiconductors.

## ADVANCED ASSEMBLY

Besides the obvious volume saving interest, network on chip provides:

- Performance improvement, with a reduced dimension and controlled connection between terminals. New developments envisage to use photonics to speed-up the inter-chip communication rates.
- Reduced mechanical stress with a tighter package.
- Security enhancement as inter-chip probing probability gets highly reduced.



*Image credit techovedas.com*

# Semiconductor

## WHAT IF ?

### BIO-SEMICONDUCTORS

Bio-semiconductors are expected to exhibit characteristics similar to organic semiconductors. However, they are not in application yet.

## WHAT IF...

*...light and flexible cellulose-semiconductors, built with renewable natural compounds, would combine its characteristics to interfere directly with microorganisms?*

*...biosensors and disease diagnostic could trigger the appropriate treatment implants to anticipate the curing mechanism before symptom occurrence?*

### QUANTUM SEMICONDUCTORS

The qubit is the smallest possible unit of quantum information, which state is being continuous-valued, but cannot be fully measured, copied, deleted, delivered to multiple recipients and cannot be hidden. The conventional software rules of digital computing are reshuffled, but carries tremendous processing power. Today, most of research programs are international and collaborative.

## WHAT IF...

*... trade restrictions would limit the usage of quantum super powers to several happy few?*

Quantum computers promise to deliver tremendous computation power and execute algorithms unreachable to classical computers. Several hardware quantum computing platforms compete. The technology who will prove most successful is still unknown. The leading schemes are based on superconducting circuits or trapped-ion technologies.

Silicon-based quantum processors are on the way to industrialization within all-CMOS industry made qubits. While photonics has often been considered impractical because of difficulties in generating the required quantum states. However, this method could turn out to be the dark horse.

## WHAT IF...

*... the semiconductor integration comes to the point where quantum personal computers with its operating system, gets massively released?*



**PRINTED ELECTRONICS**

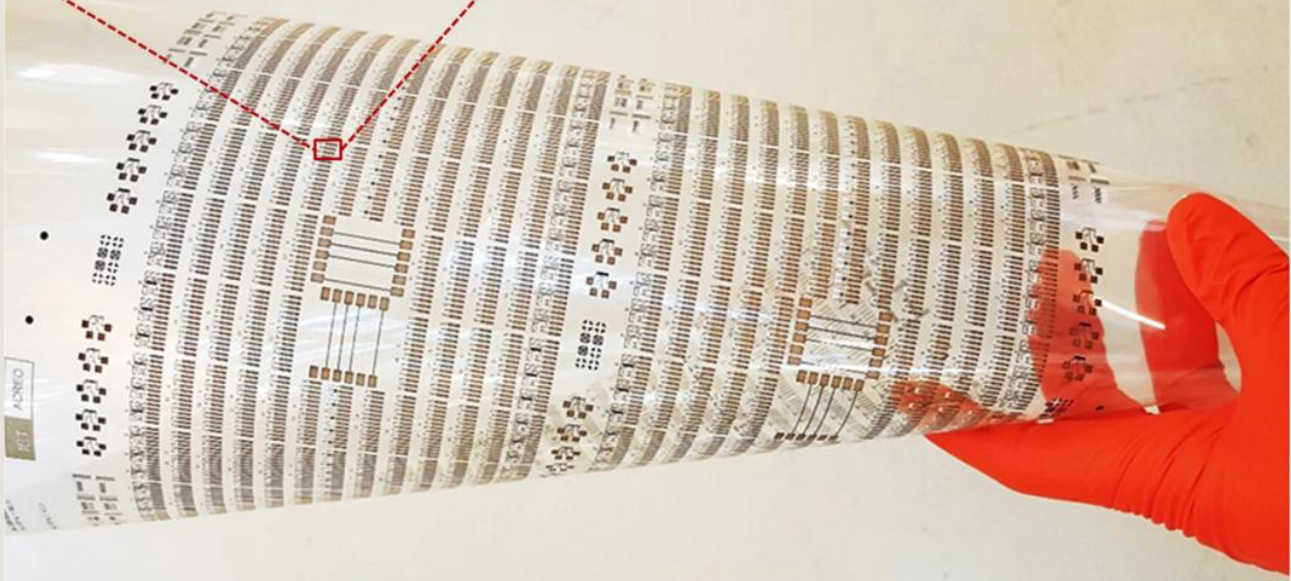
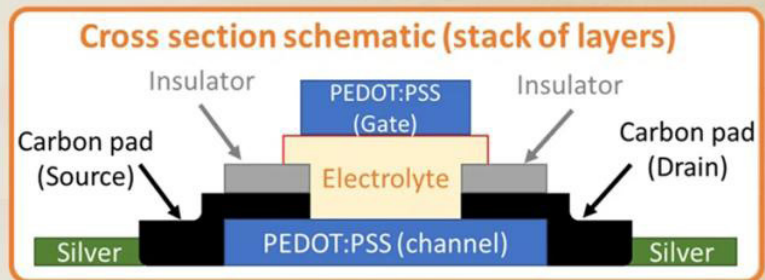
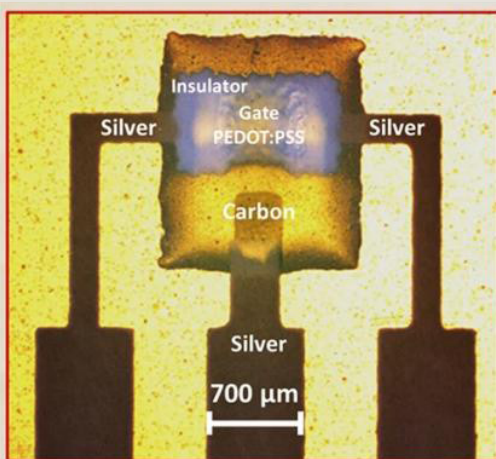
Inkjet printing technologies are considered as promising approach for the manufacturing of novel flexible and large area electronics, as the base substrate doesn't need to be of semiconductor type.

Glass or passive polymer does the job. So far, printing methods do not allow the manufacturing of electronic chips with high number of transistors. This figure is much lower compared to established conventional methods based on photolithography.

**WHAT IF ?**

*Will the augmented soldier benefit from disposable skin patch to monitor his operational ability?*

Instant energy consumption, power reserve, physiological ability to perform are decisive parameters on the battlefield.



Source [nature.com/articles/s41528-020-0078-9](http://nature.com/articles/s41528-020-0078-9)

# Antenna

## OPTIONS

---

### INFRASTRUCTURE ANTENNA

Generally part of the network section, infrastructure antennas are built to sustain harsh environment conditions. Modern designs make usage of enclosures in which one or several elementary antennas take place.

A basic rule for installation of any antenna is “the higher the better”.

**Reminder valid for any antenna:** its volume size is inversely proportional to the wavelength. In other words, the higher the frequency, the smaller the antenna size.

### EXTERNAL ANTENNA

More often used on IOT actuators, external antenna provides a false sense of security to its designer.

If the environment in which it is operating is most likely free air, the users have a tendency to hide it. Hiding the antenna has the same meaning from the electromagnetic perspective. In such case the IOT actuator will exhibit degraded performances due to its hidden antenna. In order to perform correctly the external antenna must be placed in a visible, open space.



4 External antenna WiFi router

*Photo credit Synology*

Infrastructure antennas of different formats, frequencies and purposes on a rooftop.



*Photo credit from the author*

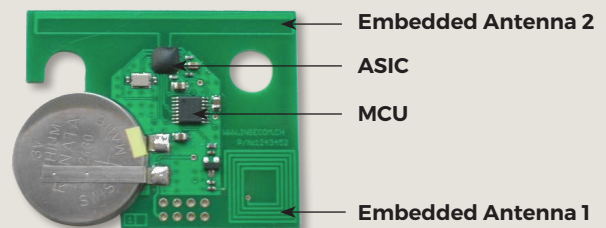
### EMBEDDED ANTENNA

IOT sensors are often cost, size and shape constrained.

Embedding the antenna directly on the sensor is the preferred choice of the designers.

Presented as the simplest solution, its performance might be strongly impacted by the environment in which it is operating.

The same IOT sensor will display excellent range capability when affixed on an empty container, and very poor performance while this same container gets filled with liquid.



*Photo credit from the author*

# Antenna

## DRIVERS

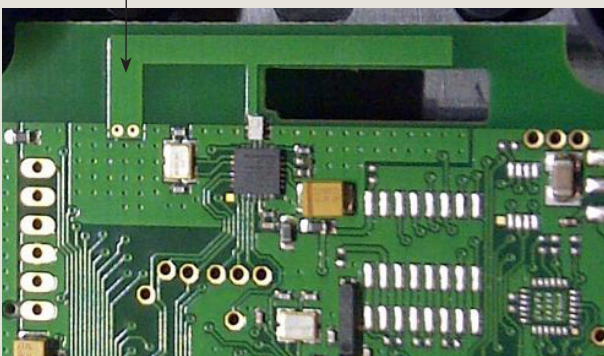
---

The antenna is a passive element whose role is to convert electrical energy into radiated energy, and vice-versa. Given that the transformation is linear, it is totally reversible. The transmit antenna is the same as the receive antenna.

Often overlooked during the design of an IOT system, the antenna should carry the greatest attention as it is the center piece of all the wireless communications.

A passive matching network is often required to minimize electrical losses between the electronic transmitter or receiver and the passive antenna. A good antenna design is reached when integrating all the surrounding elements.

Embedded Antenna



*Photo credit from the author*

## BANDWIDTH

As wireless IOT are principally derived from civilian applications, they are operating within a strictly regulated spectrum of frequencies,

making them vulnerable to adverse threats like jamming, eavesdropping or spoofing, just to name a few.

Military IOT will attempt to escape with the utilization of different frequencies. But the antenna must be able to cope with this spread in spectrum.

## COST

While the antenna cost in civilian IOT is of utmost importance to reach market fit, it is not as severely impacting for military budgets.

## GAIN

The Gain of an antenna is the concentration of radiated power into a particular solid angle of space. There's no increase in total power above that delivered from the power source. The power increased in a specific direction is balanced by power reduced in other directions.

## SIZE

The reference size of an antenna is a dipole, where both elements of the dipole are a quarter wavelength dimension. For IOT equipment operating at 2.45GHz (Bluetooth, WiFi), it means an optimum dipole dimension of 6cm long. It is possible to circumvent this physical law by using specific materials like ceramics. Other than that, the size reduction is detrimental to its performance.

# Antenna

## TRENDS

### ACTIVE BEAM-FORMING

The integration of beam-forming technology carries the potential to unlock innovative features. Antenna beam-forming is a technique used to control the directionality of an antenna array. It consists of the organization of phase and amplitude of the radio waves emitted by each individual antenna element in an array to produce the requested radiation pattern. Focusing the antenna's radiation energy in a specific direction creates a beam of radio waves that can be aimed at a target.

Beyond the benefit of spectrum occupancy optimization, a reduced amount of energy is required to achieve the same result. Ultimately, privacy is the 2nd order winner as eavesdropping gets more difficult.

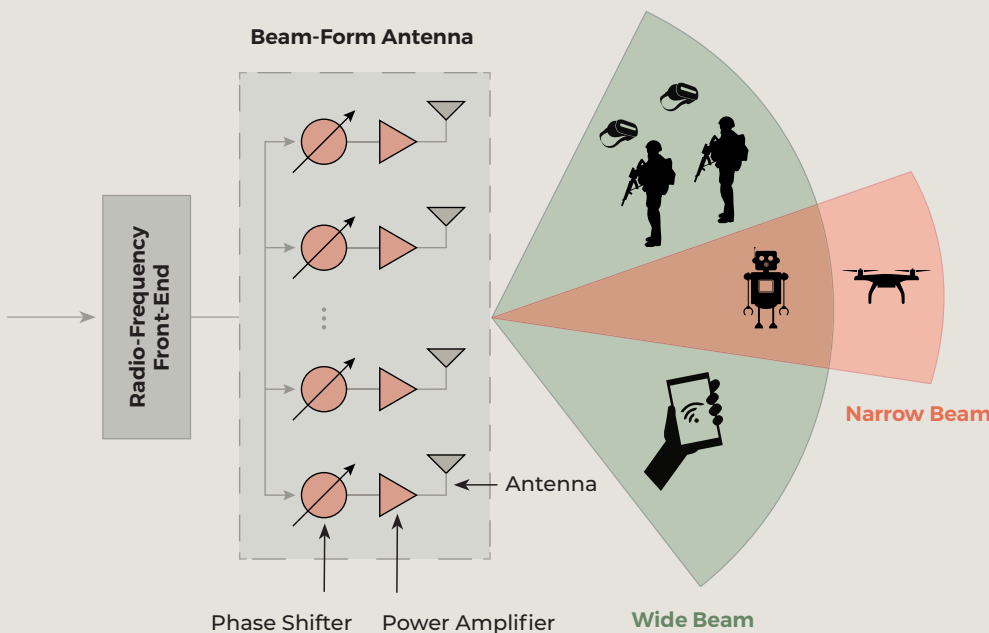
### ADVANCED MATERIALS

The antenna design's first consideration is its operating frequency and bandwidth required. An embedded antenna design is constrained by the mechanical geometry of the product. The designer is usually required to adapt and shrink the antenna to fit inside the space allocated.

Advanced Materials like artificial metamaterial are here to help. They provide properties like negative permittivity and permeability that improve critical parameters of the antenna.

The emergence of epsilon-near-zero materials exceptionally allows for an infinite wavelength of electromagnetic waves.

Special ceramics are used as a way to reduce the overall antenna size. Artificial metamaterials are pushing the boundaries further.



## RECONFIGURABLE INTELLIGENT SURFACES (RISs)

RIS are used to expand the capacity and coverage of wireless networks by smartly reconfiguring the wireless propagation environment. Based on beam-forming principles combined with applications of machine learning, RIS are intelligent reflecting surfaces, with capability of proactively modifying the wireless communication environment.

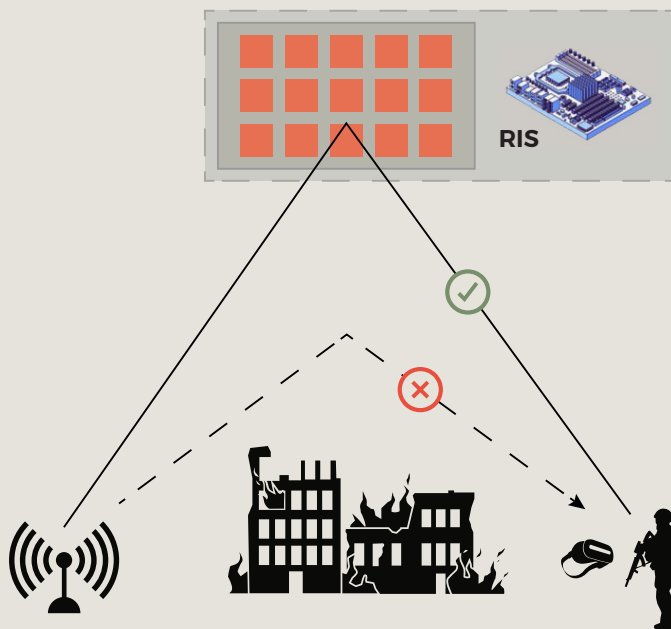
However, RIS only reflect the electromagnetic waves, therefore doesn't require the complex and expensive electronic required to amplify and forward.

The RIS comes in usage when the radio Line of Sight (LoS) gets blocked by obstacles. Since RISs compose a software defined wireless environment, it provides enhancements of the received signal-to-interference-plus-noise ratio (SINR).

## RECONFIGURABLE ANTENNAS

While miniaturized design having low weight and size is required especially for IOT sensors, miniaturized antenna designs have a drawback of a lower gain. While this drawback can be partly compensated by advanced materials, another difficulty arises, when the requirement for multiple frequency band operations happen. In the military context, spreading the spectrum is vital to escape adversarial threats.

Switching are applied to antenna structures by incorporating PIN diodes, acting as 'on' or 'off' switches to achieve frequency configuration. Several layers of metamaterial superstrates can be combined over the patch antenna, controlled by the PIN diode switches to operate at the requested frequency.

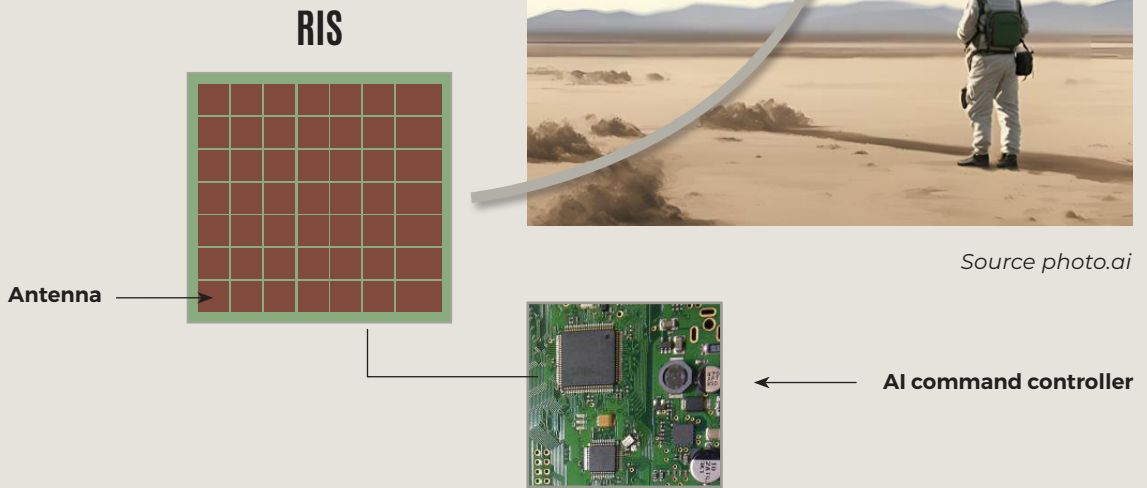


# Antenna

## WHAT IF ?

### STRETCH THE LINE OF SIGHT (LoS)

Reconfigurable Intelligent Surfaces (RIS) provides an economical way to stretch wireless communication capacity beyond the Line of Sight (LoS). A limited amount of hardware and energy can reconfigure any surface into some sort of mirror of millimetric radio waves.



Source photo.ai

## WHAT IF...

... fixed wing Unmanned Aircraft Vehicles (UAV) would carry RISs affixed under the wings? Those RIS UAVs could be orbiting above the terrain for which an extension of the LoS is required, providing a superior telecom advantage.

The RIS technology doesn't disclose the radiofrequency characteristics. A UAV RIS captured by hostile forces won't divulge any compromising information.

## ACTIVE BEAM-FORMING

When an aircraft gets grounded in hostile territory, his pilot is under threat. Whilst equipped with a Personal Locator Beacon (PLB), his activation exposes him to being localized by the hostile forces. (Ref.: *Revue Militaire Suisse*).

Instead of 360° radiation pattern, the downed pilot could be localized faster, with greater precision, while reducing the probability of being detected by hostile forces. As time runs against the victim, such a feature would greatly improve chances of being localized.

## WHAT IF...

... the Personal Locator Beacon could concentrate and direct the transmission to a specific area?



**Personal Locator Beacon**  
360° radiation pattern

Photo credit from the author | US Navy Search and Rescue exercise – SH60B, San Diego bay

# Energy

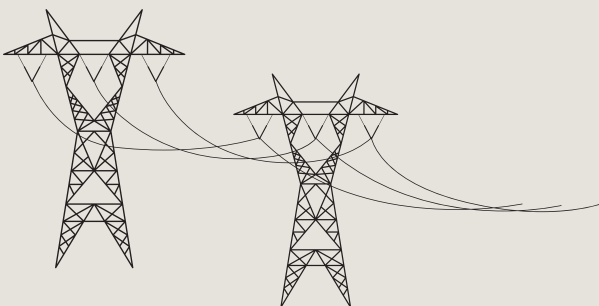
## OPTIONS

---

The IOT intrusion in warfare is still in its infancy. The projected growth is skyrocketing, raising the question about how its energy supply will follow. The battlefield's harsh and unpredictable nature is such that, deployed IOT equipment must operate with high performance and without interruption for potentially extended time periods. Energy must be efficiently conserved throughout the operating lifetime of a defined application. While growing pressure is placed on IOT sensors to deliver increasing quantity of data, the energy management reminds that it comes at the expense of adversary factors such as

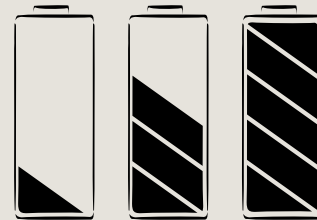
- **Increased weight**  
More data is more power is more weight and volume to store the required energy.
- **Stress over the supply chain**, whether for battery replacement or recharging.

Multiplying the sensors across the battlefield and its surroundings is only a question of time. The energy management will unfortunately act as a retainer against this multiplication.



### ENERGY MANAGEMENT

Proactive and systematic monitoring, control, and optimization of all the equipment's energy consumption to ensure their operational function.



Monitoring an estimate of the power reserve of each equipment is a good practice. Converting it into remaining lifetime is vital to organize the energy supply chain.





# Energy

## DRIVERS

---

The energy source, its management and usage require careful consideration for the optimization of all IOT equipment. The profile of the mission leads the equipment's specification. Its energy strategy derives from the required operational lifetime.

Many complex factors affect the outcome of warfare. Ultimately, the energy is at the center of all the contingencies. The party able to

- Collect more and better data,
- Run intense and faster AI computer algorithms,
- Decide and activate better and more powerful actuators,

exhibits warfare superiority, especially if resilient on the long run.

Mastering the energy strategy is critical for the success on the battlefield.

---

## STORAGE DENSITY

The storage density is the ability to pack as much energy as possible inside a given volume. But the energy must be manageable without requiring excessive engineering, or exposing to unnecessary risks.

## SAFETY

Loads of battery related casualties are commonly reported on the civilian market. In a

military context the consequences may carry critical outcomes. Great caution must be exercised handling energy related considerations.

## EFFICIENCY

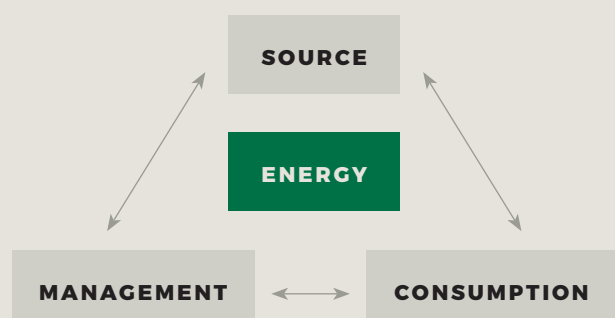
The operational lifetime's primary contributing factor is the energy consumption of the equipment. Huge energy savings would occur if a monitoring camera could sense and pre-analyze one picture every minute, and self determine the opportunity to resume or transmit the following video frames.

## AVAILABILITY - DRAIN

An IOT sensor can remain in deep sleep mode, with near to zero energy consumption during a long time. Sudden activation for sensing and wireless transmission will require an abrupt and intense peak of energy from its source.

The battery's specification fits well with the global requirement of energy. But the brutal and intense peak requirements may exceed its electrochemical capabilities.

The energy management must organize the availability in an efficient way.



# Energy

## TRENDS

### MATERIAL RESEARCH

While lithium is today's undisputed primary component, the volatility of its supply chain triggers intense research activity. Sodium (Na) is already a replacement challenger but other materials are on the spot.

Since decades, most anodes use graphite to hold the lithium ions. Alternatives based on silicon are expected to improve energy density and reduce the charging duration.

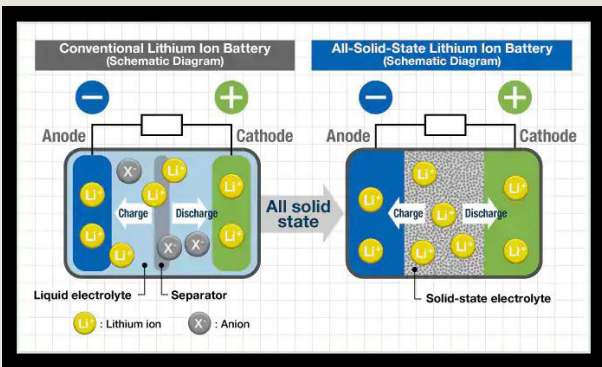


Image credit TDK.com

### SOLID STATE ELECTROLYTES

Lithium-ion batteries and related chemistries use a liquid electrolyte that shuttles charge around.

Solid-state batteries replace this liquid with ceramics or other solid materials, opening the path to:

- Improving the energy storage density
- Reducing the fire risk
- Canceling any chemical leakage occurrence

- Faster charging time
- Reduced sensitivity to temperature
- Enabling novel geometries

The architecture allows also to use lithium metal as the anode, which provides higher capacity than the graphite anodes used for liquid electrolytes.

Solid-state materials take advantage of robust production capacity such as lithography for layer deposition, opening the path to massive capabilities.

### MICRO-BATTERIES

With limited capacity, micro-batteries can play a significant role, just keeping alive the minimum vital part of an IOT equipment.

A prompt and efficient wake-up is provided by the smart energy management, transitioning to unlock additional energy sources.

Energy harvesting and micro-batteries combine well when smartly managed.

Small footprint and high energy density oppose each other.

Micro-batteries built with thin film stacks offers the capacity of being massively produced. On-chip batteries offers monolithic integration capacity, such as surface mount placement, with other components on a printed circuit board structure.

## GEOMETRIES

Solid-state electrolytes paves the way to novel battery shapes. The traditional cylindrical shaped battery cell is dictated by the sealing of the container, required to prevent leakage of the liquid electrolytes.

With no worries about leakage, the solid-state battery's geometry can accommodate the shape required by the user.

The layer deposition of solid-state electrolytes paves the way to flexible structures. New geometries can be imagined with flexibility in mind.

## EXPAND TEMPERATURE RANGE

For proper operation, liquid electrolyte batteries must operate within a temperature range such that the electrolyte remains... liquid. The processes limiting low-temperature characteristics is a decrease of ionic conductivity in the electrolytes, resulting in capacity loss.

A typical lithium-Ion electrolyte exhibits limits from  $-20^{\circ}\text{C}$  to  $+60^{\circ}\text{C}$ . Both low temperature and high temperature outside of this boundary will lead to degradation of performance and lifetime.

If low temperatures affect the performance and lifetime of the battery, exceeding high temperature limit causes irreversible damages, such as lithium plating and thermal runaway. exposes to increased risk of safety problems, including fire and explosion.

Extending the temperature range above the

current limitations improves the ability to operate safely within military operational conditions.

## ENERGY HARVESTING

Capturing enough energy from the surroundings to run the equipment fascinates as it provides a flavor of perpetual motion. However, for this dream to become true, the combination of two other forces are mandatory: Optimized energy consumption and smart energy management. Whether harvesting energy from sunlight, ambient radio-waves, mechanical vibrations, audio sound, temperature difference or from vegetables, the common ground is its scarcity. The trends are focusing on smart converters to extract the best of an energy source and make it available to an energy management system.

# Energy

## WHAT IF ?

---

### MATERIAL RESEARCH

Alternative material research for lithium replacement is running fast. So far the closest match is the abundant and cost effective sodium (Na), which unlocks new futures. The anode replacement by sodium (salt) doesn't increase the energy density of batteries but improves significantly its supply chain as it is considered as the sixth most abundant element on the planet. In addition, nanoparticles can be used in many different parts of batteries, including anode, cathode, and electrolyte. Using nanoparticles contributes to cleaning and decreasing environmental pollution.

### WHAT IF...

*... all the solid-state electrolyte material components be so abundant and harmless to the environment?*

Relieving the pressure on the IOT equipment supply chain is a strategic issue.

### SOLID STATE ELECTROLYTES

The solid-state intrinsic nature of the batteries is such that the toxic waste is difficult to recycle. By design, the coherent intricate assembly of polymers, oxides and sulfide based electrolytes is difficult and energy intense to separate for recyclability purpose.

### WHAT IF...

*... the composition of materials used didn't carry recyclability concerns?*

If the environment protection is not the first driver of military systems, aiming towards an eco-friendly design can only improve.

### MICRO-BATTERIES

The phantasm of micro-batteries solves all problems gets quickly confronted to the reality of their very limited amount of energy available. Such small volume batteries also carry the limitation of instant power availability: even if the theoretical amount of energy would be enough to cover the operational demand of the IOT equipment, its peak-power request exceeds the micro-batteries drain capacity.

### WHAT IF...

*... micro-batteries could shrink even smaller, carry more energy, supply all the peak-power request and be environment friendly?*

Dreaming of the holly grail doesn't hurt, as long as it doesn't convert into unrealistic promises.

## GEOMETRIES

IOT hardware electronic is always packaged inside a protective case, made of a material adapted to its purpose. The protective role of the case is of course mandatory, but contributes to increasing the weight and form factor of the equipment.

### WHAT IF...

*... the protective case consisted in total or partially of the solid-state structure of batteries?*

Impossible to do with the liquid electrolyte, let us imagine that the solid-state battery plays also the role of protective cover, therefore contributing to optimizing the overall weight and dimension of the equipment.

## ENERGY MANAGEMENT

Since the energy is at the root of operations of any IOT equipment it must be considered as a scarce resource. Great care must be exercised to avoid wasting to stretch the operational lifetime to its best capabilities.

### WHAT IF...

*... an AI aided energy management system could help optimize the energy conversion and distribution?*

The poly-factor environment of an IOT equipment is such that its operation may be adapted to the evolution of its context. The AI assistant would provide the ability to manage the energy appropriately, ensuring the availability of a power reserve for when required.

## ENERGY HARVESTING

Based on conversion principles, the energy harvesting design begins with a model of energy to be converted. Light energy is a good example, where the most efficient solar farms are adapting the elevation and azimuth of each solar panel. How does this efficiency translate to IOT equipment?

### WHAT IF...

*... the artificial intelligence could assist to identify precisely where and when to direct the energy harvester?*

# Sensor

## OPTIONS

Sensors are hardware components for detecting different parameters from the environment. They extend the eyes and the ears capabilities of the command and control system.

Most advanced sensors are fitted with pre-processing capability to summarize the parameters down to a certain level before transmitting data over a network. This network can be wired, but in a military situation the wireless option is predominant.

The data gets aggregated into servers and computers who compile and process, running software applications and analytics, commonly driven by artificial intelligence.

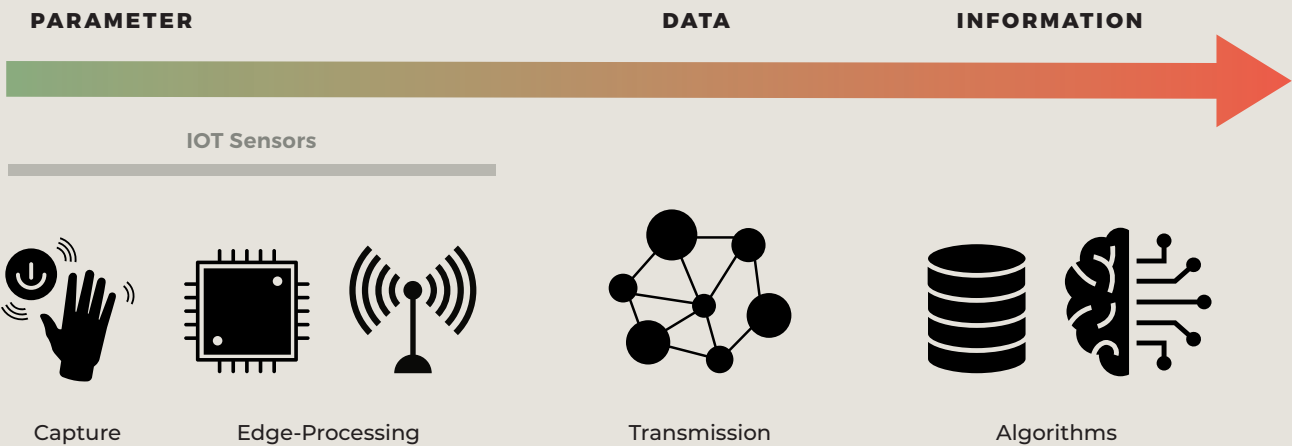
The information is the outcome of the chain.

In the CONTEXT section of this document, **IOT sensing** is used to differentiate the general sensing function of IOT equipment from the general **IOT actuating**. While the first one

provides data, the second one executes a command. Other parts of this document refer to **IOT sensor**, still in the general context of supplying data to a host. This section gets more into the details of a sensor as a **component, part of the IOT hardware**.

IOT sensors have the power to capture the real parameters of a situation. They are at the root of the real information. It is down the transmission and data analytics line that this true source gets exposed to manipulation and misleading representation. An IOT sensors is unbiased, by definition. The information, outcome of the global chain has already received several filtering and optimizations.

**IOT sensors play an increasingly important role in the Internet of Military Things.**



# Sensor

## DRIVERS

---

We like to think that sensors convert the measured parameters with High Fidelity (HiFi).

HiFi is one of those outdated marketing acronyms used to convey the feeling of emotions. Only specialists knew how to interpret the HiFi's characteristics, common to all sensors, or transducers.



Source Pixabay

Several characteristics are dominant during the selection of a typical sensor.

Example: a temperature sensor wouldn't require a fast reactivity unless used for monitoring gas leakages.

### SENSITIVITY

Data change response to change in measured parameter

### ACCURACY

Data on target



### PRECISION

Same parameter - Same data

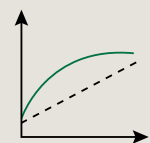


### RESOLUTION

Smallest change displayed from the measured quantity

### DYNAMIC RANGE

From min to Max, within Sensitivity, Accuracy and Precision



### LINEARITY

Accuracy and Precision over the dynamic range



### REACTIVITY

Duration required for the measurement

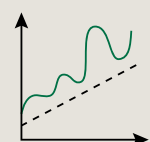


### JITTER

Short term stability around the parameter

### DRIFT

Divergence on the long run



# Sensor

## TRENDS

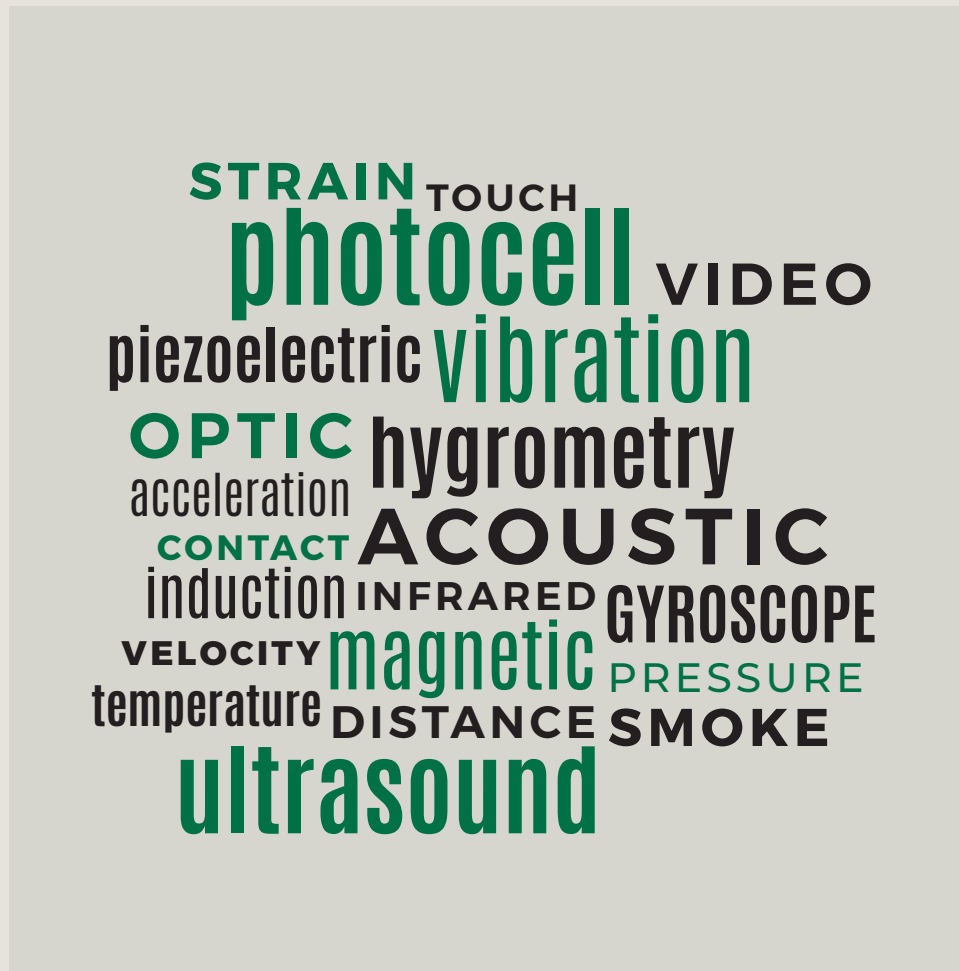
---

The trends follow the same lines as for semiconductor (page 27). Smaller, Faster, Low-Power is a common trend for all the sensors.

SMALLER

FASTER

LOW-POWER





## MOLECULAR BIO-SENSING

The abnormal concentration fluctuations of neurotransmitters are associated with brain-related physiological events. Monitoring the dynamics of extracellular neuro-chemicals in vivo can provide direct insight from the molecular basis of brain function.

In vivo electrochemical analysis is a promising tool for such tasks due to the merits of high spatial-temporal resolution and favorable sensitivity.

Photo-electrochemical sensing has been developing quickly in recent years, targeting in vivo applications.

Some small-molecule organic semiconductor based photo-electrochemical sensing makes use of the structural flexibility and readily tunable energy of the organic structure.

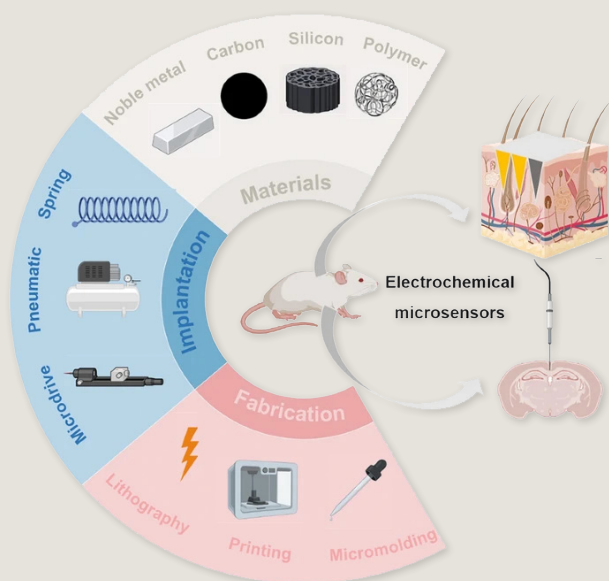
## QUANTUM SENSING

Quantum sensors exploit the fundamental properties of atoms and light for environment measurements. The quantum states of particles are extremely sensitive to the surroundings, which is a virtue for sensing.

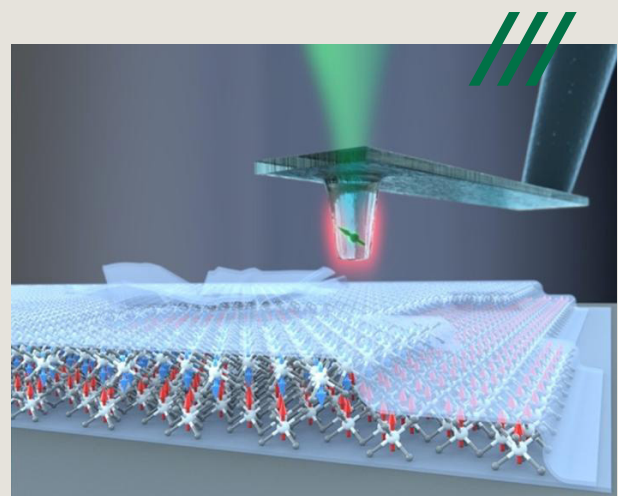
Quantum sensors using particles as probes will quantify acceleration, magnetic fields, rotation, gravity and the essence of time more precisely than any conventional technology.

Smaller and more accurate atomic clocks, cameras to see through fog and around corners, underground mapping structures are foreseen among others.

If their commercial promise still needs to be better appreciated, their military potential holds strong.



Source *Monitoring of Animal Physiological Information Nano-Micro Lett.* 16, 49 (2024)



Source University Basel, Switzerland

# Sensor

## WHAT IF ?

---

### NEURAL BIO-SENSING

Soft implantable electrodes have been used by EPFL researchers, combined with semiconductor ASIC design, running machine learning algorithms, to produce a neural interface that can identify and suppress symptoms of various neurological disorders. The system extracts and classifies a set of biomarkers leading to symptom prediction.

*“NeuralTree functions by extracting neural biomarkers – patterns of electrical signals known to be associated with certain neurological disorders – from brain waves. It then classifies the signals and indicates whether they herald an impending epileptic seizure or Parkinsonian tremor, for example. If a symptom is detected, a neurostimulator – also located on the chip – is activated, sending an electrical pulse to block it.”*

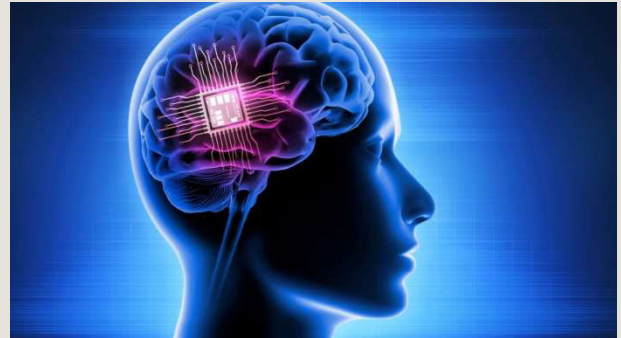
---

## WHAT IF...

*... the machine learning algorithms running behind the implanted electrodes could also reveal the soldier's biases in real time?*

### BRAIN ELECTRONIC SENSING

Human brain sends over a million different movement instructions to the body to operate both simple reflexes and complex behaviors,



Source Shutterstock

---

## WHAT IF...

*... the electronic brain interface could rehabilitate the altered motion functions?*

through the actions of large distributed neuronal networks.

With collection of nerve tracts running in the vertebral column, the spinal cord injury is often irreversible, causing partial or complete paralysis of arms, legs or both.

Soldiers are exposed to high-impact contacts with strong potential of spinal cord injury.

A digital bridge between the brain and the spinal cord is under exploration at the EPFL, in order to restore motor control of paralyzed limbs. Brain recording techniques such as electroencephalography (EEG), electrocorticography (ECoG) and intracortical recordings is used to decode the motor intention and translate into electrical orders for activation of the muscles.

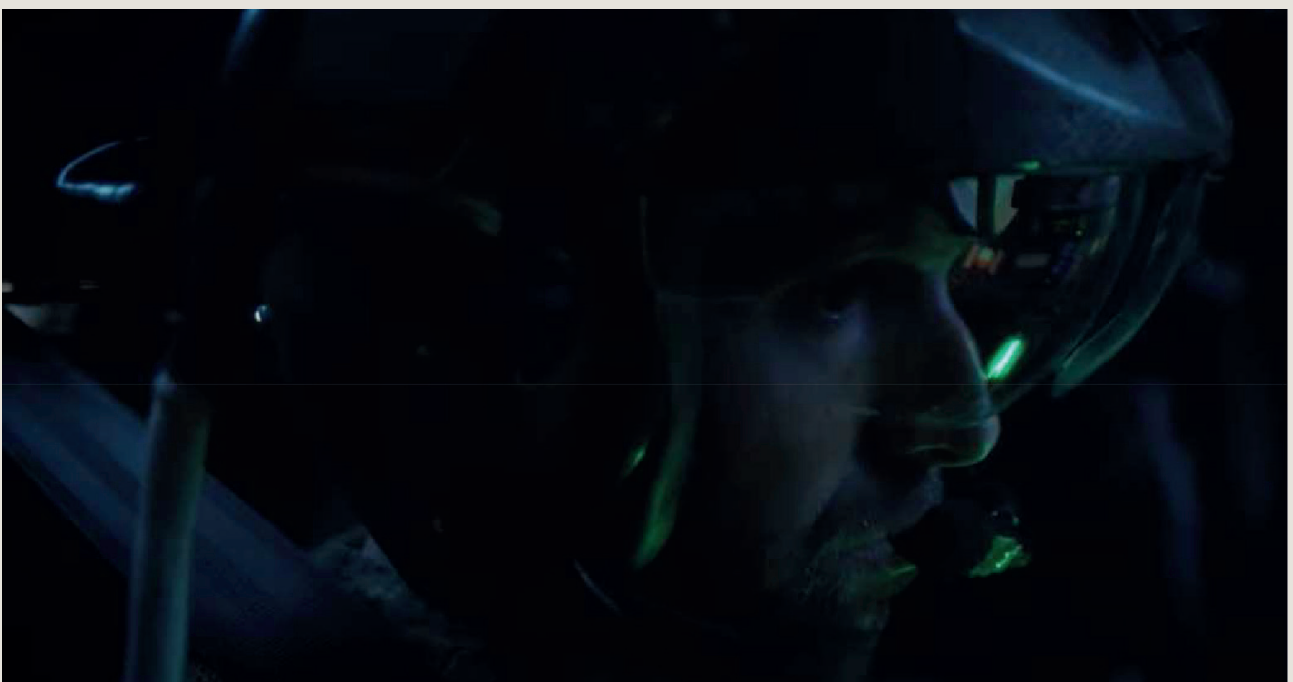
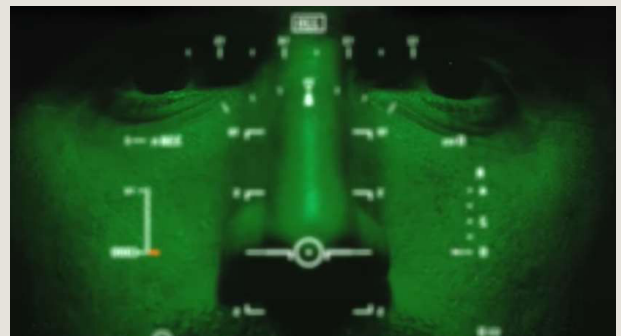
## SENSOR FUSION

A combination of sensors at the IOT level brings significant added value, especially with the advanced edge-computing power available nowadays.

A new helmet tracker is based on MEMS technology to sense angular rate of rotation, gravity and earth magnetic field along three perpendicular axes. On top of the 3 axis, x, y, z, the angular rates are integrated to obtain the orientation (yaw, pitch, and roll) of the sensor. This combination of sensors provides a 6 Degrees of Freedom (DOF) ideal for augmented and virtual reality inside-out applications. The hybrid optical-based inertial tracker (HOBIT) produced by Thales Visionix allows pilots to use their helmet-mounted cueing system for optimum symbology, sensors and weapons slaving.

## WHAT IF...

*... the sensor fusion also included non invasive brain electronic sensing so the pilot could activate the systems only with his brain interactions?*



Images source Thales Visionix

# Sensor

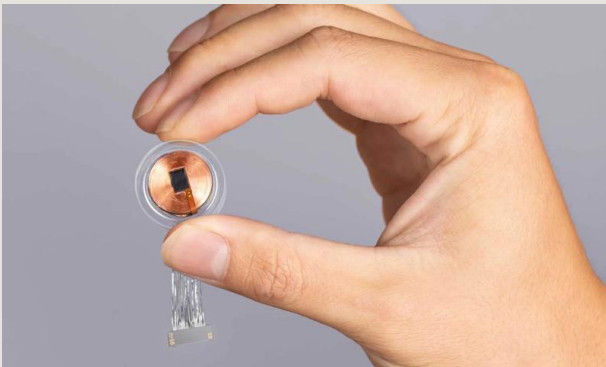
## WHAT IF ?

### MOLECULAR BIO-SENSING

During COVID era, Bill Gates was under fire, with very angry and aggressive accusations of dissimulating bio-sensors inside each vaccine dose, for the purpose of massive populations control.

Three years later, Elon Musk got elevated to the highest rank of visionary when Neuralink published on the success of Telepathy, announced as the first implanted Brain-Computer Interface (BCI).

The pictures below shows that it is still far from being diluted inside an injection fluid.



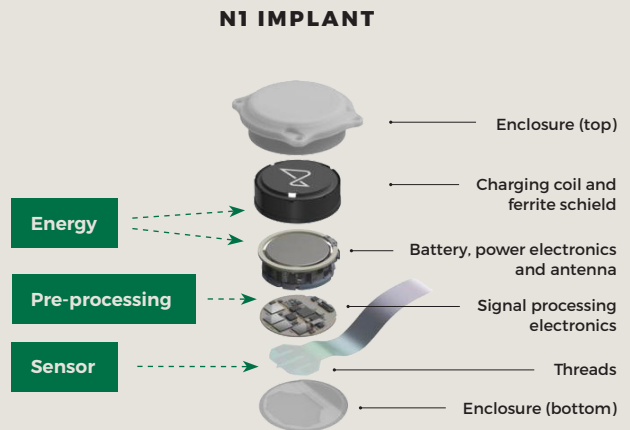
Source Neuralink

The picture reveals that the sensor consists of a network of fine threads reaching out to the brain.

Total thickness of this astonishing fine-art demonstration of electronic integration is 8mm. The energy section is the main contributor to this relative thickness.

All this work is still experimental, despite Noland Arbaugh's positive success. Since 2003,

fewer than 20 people in the U.S. have received a brain implant, mostly on a research basis. Today, the purpose of this experiment is to interface with various computer applications, like playing online chess and Mario Kart.



**Transpose to the military context, when the BCI will be smaller, massively implantable by robots.**

## WHAT IF...

... Error 404 – Not Found  
Self censorship in progress, governance issues foreseen.

## QUANTUM SENSING

Quantum sensing technology's capabilities in monitoring, imaging, navigation, and identification have the potential for disruptive impact. When atoms are used for quantum sensing, they carry intrinsic noise while shifting between energy levels. However, when they get entangled, the entanglement property is such that they all behave in unison. This is how entanglement reduces that noise.

Entanglement, which Einstein dubbed "spooky action at a distance", could theoretically sync particles all the way to the edges of the universe. Acceleration measurement is foreseen as the great winner of this physical property.

### WHAT IF...

*... quantum sensors with multiple entangled ions could overcome GNSS frequency jamming, retaining high accuracy timing and navigation capability on the battlefield?*

## MICRO-ELECTRO-MECHANICAL SYSTEMS

MEMS sensors integrates mechanical and electrical components at a micro-scale.

They are built for detection and measurement of physical parameters such as pressure, temperature, acceleration, gyroscope, magnetic field, vibration, and more.

As an example, MEMS pressure sensors integrate mechanical and electrical components on a micro-scale, utilizing the principles of MEMS technology to convert pressure into electrical signals.

### WHAT IF...

*... advanced sensing technology could reproduce the tactile perception and convert to relative sensation for remote sensing feedback?*

# Cyber-Security

## OPTIONS

---

The most favorable option states that a majority of battalions and companies would be equipped with the means to carry out actions in electromagnetic space, with:

- Decentralized cyber protection of infrastructures
- Mobile independent digitalization capabilities
- Dedicated focus on strong electromagnetic spectrum reinforcement
- Cyberspace targeting

The technical improvement of data transmission program via optical fiber and radio transmission is already on the way, as part of the project FITANIA, to support the air, ground operations as well as other capacities of the army.

In the mean time, the Internet of Military Things grows in importance. Agile wireless equipment with significant interest is showing up continuously.

## So what are the cyber-security options?

The hybridization between civil and military, and the massive growth of IOT equipment is such that the armed forces will interface with products operating from civil networks. From the security perspective mobile phone users trust the:

- Sole ownership of the phone number, Unique Identification
- Communication content privacy, Data protection

The Unique Identification (UID) is provided by the SIM card. The Data protection is provided by the network's standards. Other networks consider the security differently.

### **PUBLIC NETWORK, WAN**

SIM card + custom cyphering  
*3G, 4G, LTE, 5G NB-IOT*

### **PRIVATE NETWORK LAN**

MAC address + standard protocols  
*WiFi, Bluetooth*

### **PRIVATE NETWORK LP-WAN**

Custom Solutions  
*LoRaWan Symphony Link  
MAC on Time (MoT)*

# Cyber-Security

## DRIVERS

---

### PRIVATE WAN : SIM CARDS

Since 1991 Subscriber Identity Module (SIM) cards are connecting phones to the Global System for Mobile (GSM) world.

It all started with a full credit card size supporting the security SIM chip connected under a connector. As mobile phones shrink, so do the SIM card.

The coming generation is the embedded-SIM (eSIM), affixed directly on the phone's electronic circuit.

If IOT equipment can immediately take advantage of this feature, they can also elect to use dedicated IOT cellular chips with integrated SIM (iSIM) inside.

The close future is already available with a complete dematerialization of the SIM, that stores the 15 digit number International Mobile Subscriber Identify (IMSI) and the 128 bit value authentication key (Ki) related.

### PRIVATE NETWORK LPWAN : CUSTOM

One of the most secured LPWAN network, LoRaWAN, standardized its security principles, replicating some principles of public WAN networks. A combination of key exchanges, determine how security session context is generated and how the confidentiality, integrity, and authenticity of messages are ensured.

However, inherently to its stochastic operation and characteristics of the 868MHz band, LoRaWAN networks are not suitable for ultra-reliable services.

Specific dedicated private network LPWAN make usage of Secure Elements to assist elevating the global security of each transaction.



Source Freepik 

### THREATS : THE HATEFUL SIX

- Physical attacks
- Replay attacks
- Network traffic analysis
- Denial of Services (DoS)
- Spoofing attacks
- Man-In-the-Middle attacks

Other attacks, like beacon synchronization are not counted among them.

### WIRED VS. WIRELESS SECURITY

Wired protocols have an intrinsic higher level of security over wireless.

The highest levels of security, which faces any of the hateful six, is embedded into the called Secure Elements, typically in use for card banking applications used on a safe wired peer-to-peer transaction.

# Cyber-Security

## TRENDS

---

### QUANTUM COMPUTING

Compared to our fastest and most cutting-edge classical computers, quantum computers have the potential to solve complex problems orders of magnitude faster.

While symmetric keys like the AES are anticipated to be quantum resistant, the asymmetric encoding used typically to protect Unique Identification (UID) is exposed to the power of quantum computing.

The IMSI from SIM cards will theoretically be exposed to the power of quantum computing. The threat will become significant when quantum computers will become massively available.

### QUANTUM CRYPTOGRAPHY

The target of quantum cryptography is to “develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks.” (source NIST).

Based on the occurring and immutable properties of quantum mechanics, the quantum

cryptography carries the potential to extend by far the security, way above any previous types of algorithms. While conventional cryptography is built on mathematics, quantum cryptography is built on the laws of quantum physics.

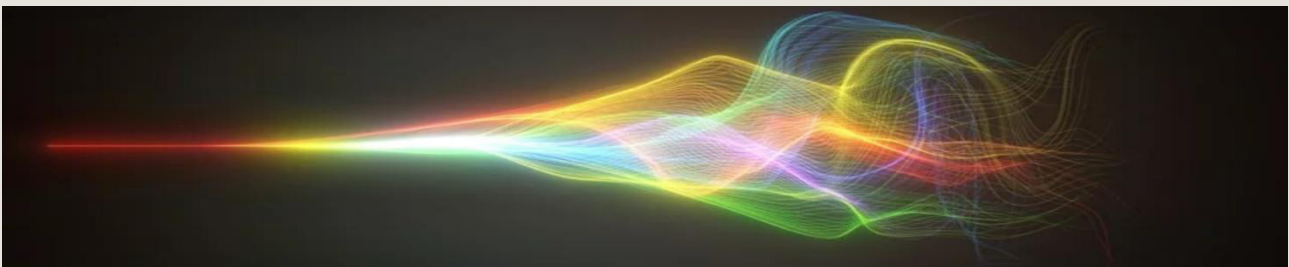
### QUANTUM KEY DISTRIBUTION

Quantum Key Distribution (QKD) works by sending individual photon light particles across a fiber optic cable. the sender's side change the physical orientation of each single photon to a specific position. A successful match of the received photon's specific position confirms that the key hasn't been intercepted.

Different types of quantum cryptography are under scrutiny by researchers, such as:

- Direct encryption,
- Digital signatures
- Position-based cryptography
- Device-independent cryptography
- Quantum coin-flipping (QCF)

using the property of quantum entanglement and other forms of quantum communications.



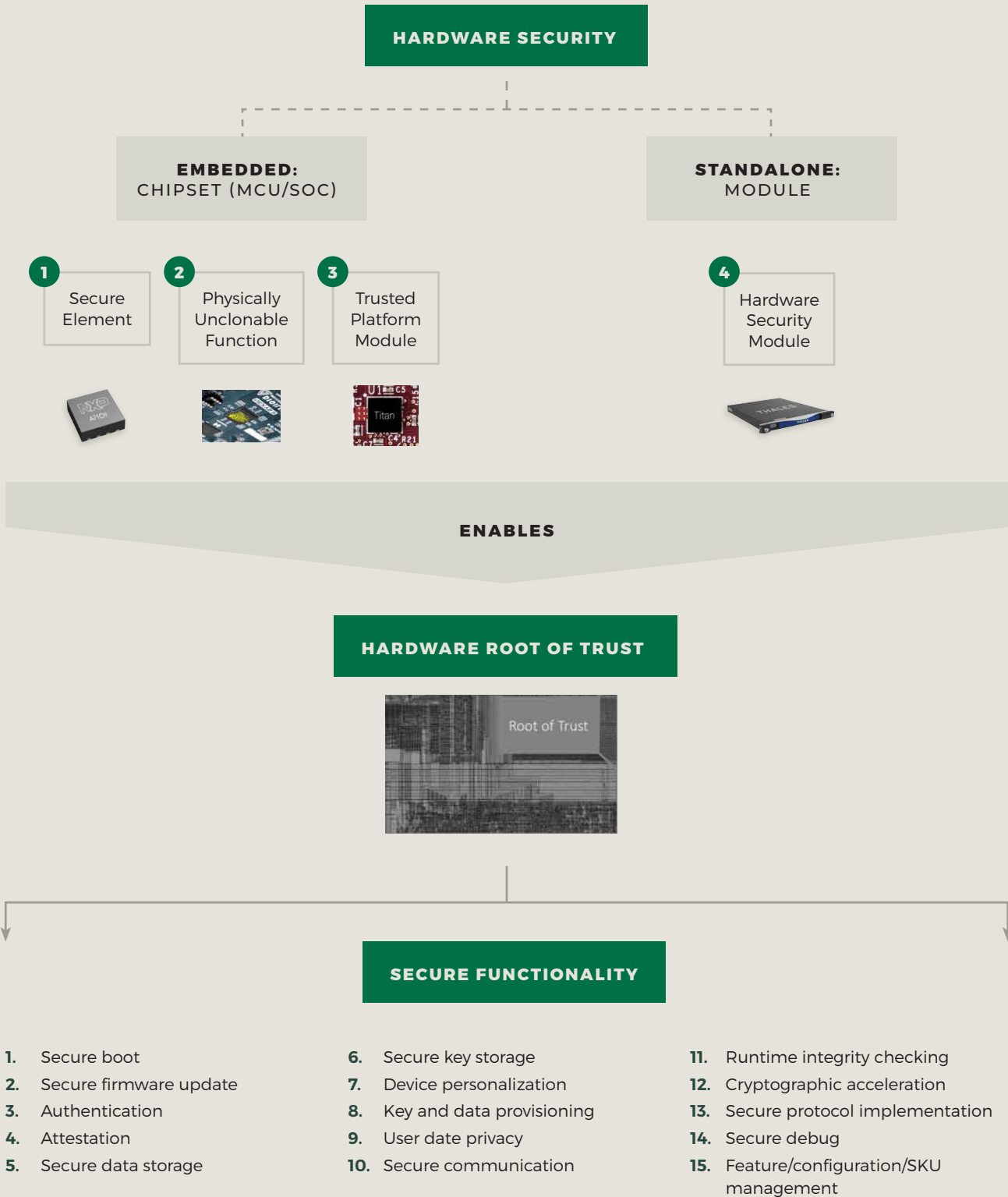
High energy particles flowing inside vacuum

Source [ibm.com](http://ibm.com)



# The makings of a "hardware root of trust"

Source IoT Analytics Research 2021



# Cyber-Security

## WHAT IF ?

---

### **PUBLIC WAN : SIM CARDS**

The SIM card emerged as a security reference when the GSM was born (ref. Appendix 1). Today's versions of eSIM is a dematerialized version. With up to 8 downloadable eSIM, its security level has raised to a higher level, removing any possibility to for a fraudster to steal a physical SIM.

Tomorrow's quantum computing might be standing on its way and to break the encryption that protects much of our personal data.

## WHAT IF...

*... the future quantumSIM could understand who we are, harness the power of AI and quantum computing safely to guarantee personal privacy?*

### **QUANTUM COMPUTING**

With quantum computing potential to compromise conventional cryptographic methods, quantum cryptography combined with machine learning are identified as perfect combination for next generation of security feature protecting digital identities.

### **ZERO TRUST ARCHITECTURE**

In the world of cryptography, key management and trust setups is unfortunately too frequently overlooked. Think about the security of all the apartments of a condominium having all their individual door keys gathered in the poorly secured lobby.

## WHAT IF...

*... the visibility of encryption keys could be hidden from the network. Adopting a zero trust architecture with separated network segments could reduce the visibility of cryptography key storage?*

## WHAT IF...

*... the combination of bio-electronics with quantum algorithms and machine learning would provide the ultimate link to our uncompromizable digital twin?*

## QUANTUM CRYPTOGRAPHY

While cryptography theories based on mathematical functions is widespread and understood by many, the physical principles of quantum mechanics reach a higher level.

### WHAT IF...

*... subversive minds took advantage of this difficulty to shape its own physics equations? Could the result be convincing enough to spread a parallel cryptography?*

### WHAT IF...

*... SIM cards could perform secure short-range wireless transactions by themselves, without requiring assistance from the smartphone's infrastructure?*

*Some innovations remain on the shelves. Despite first promising prototypes (picture below), this specific innovation never found its market.*



SIM cards production batch including wireless transmission features.

*Photo credit by the Author*

# Edge-Computing

## OPTIONS

---

The optional Edge-Computing stands between the Sensor raw parameter capture and the pre-processed data transfer. (Sensor, page 46)

The option to forward all the raw parameters via the network to the data-center places un-reasonable loads on the server. Even a simple pre-processing unit has the power to, at least, pre-filter the raw parameter and shape it in a friendly format for the data-center. Doing so removes a significant burden off the network, providing also energy savings: most of the power budget of an IOT sensor usually comes from the data transmission.

A sensor captures portions of the ambient noise when operating close to its best sensitivity. The pre-processing consists in filtering out the ambient noise in order to transmit only the valid information. A microphone able to capture whispers must remove the surrounding noise prior to transmitting the conversation.

Other sensors, like video cameras, capture loads of parameters, while only minimal information is really required from the user. A sophisticated edge-AI could, for example, count the number of people and transfer only this data.

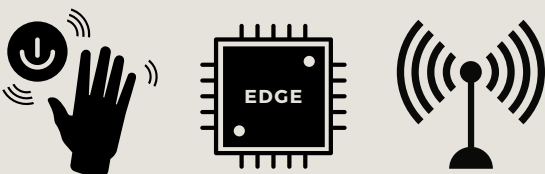
To carry out machine learning (ML), IOT data are typically transferred to the cloud, or centralized system for storage and processing. The resulting latencies and network traffic congestion become quickly detrimental to the performance of the overall system.

From simple mathematical operations all the way to complex sorting requiring the power of AI, the Edge-Computing:

- Removes traffic from network and load from data-center
- Alleviates energy requirement from the IOT sensor
- Improves real-time availability of usable data,
- Adds a security layer when avoiding data transmission.

Until recently, attention was brought to the limited MCU's pre-processing capability. Tremendous progress in semiconductor integration brings neuronal networks at affordable cost very close to the sensor.

## IOT SENSORS



# Edge-Computing

## DRIVERS

---

### **AUTOMOTIVE AND MOBILITY**

Zillions of data bytes generated from the network level is putting massive pressure on data processing and structural optimization. Simultaneously, the semiconductor industry is engaged in a frantic race towards faster, denser and lower-power integrated processing, driven by the automotive and the mobility requirements.

Resulting from this race are microcontrollers (MCU) of very high-performance and low-power designed to operate at the edge of the massive sensor parameter collection to offload networks and data-centers.

Vendors provide full catalogs of advanced components which include a set of integrated peripherals such as analog-to-digital converters and libraries of algorithms ready to produce decentralized intelligence enabled edge-computing.



Source photo.ai

# Edge-Computing

## TRENDS

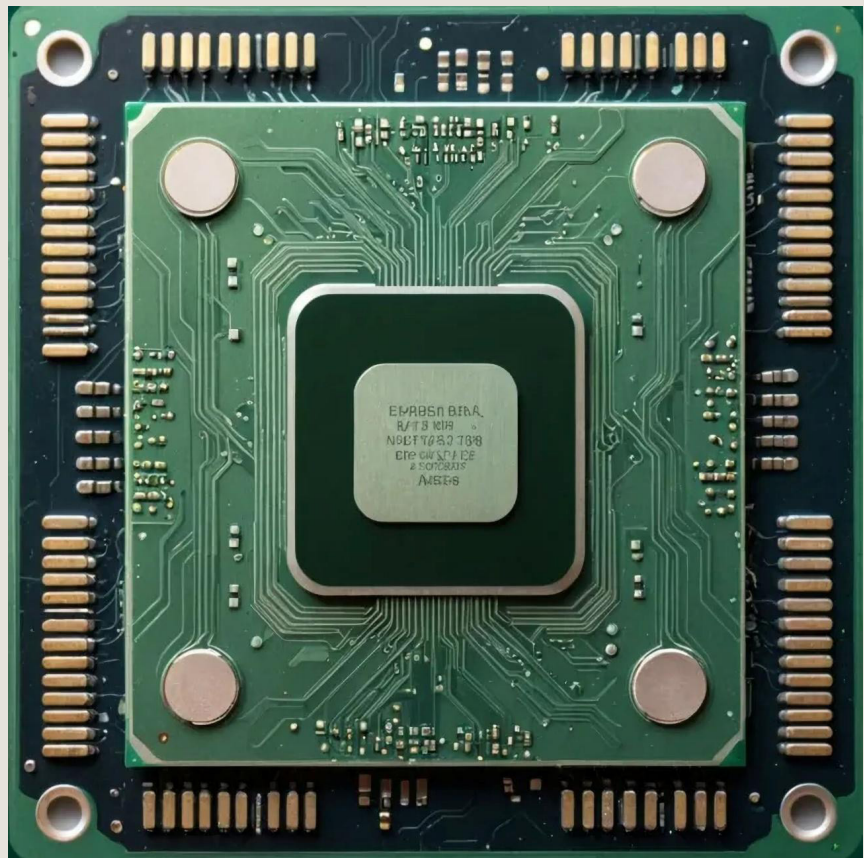
---

### HIGH-PERFORMANCE ASICs

The convergence of generative AI and IOT solutions is a global trend, harnessing the performance of latest generation processors for decentralized decision making.

Deep learning is of different formats, like Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs) or Generative Adversarial Networks (GANs). Striking breakthroughs are achieved in the segments of computer vision, speech recognition, and natural language processing.

It is a matter of time before ASICs with computational acceleration such as eFPGAs, Graphics Processing Units (GPUs), Tensor Processing Units (TPUs) and Neural Processing Units (NPU) get integrated with IOT sensing equipment, to the benefit of solving complex learning, planning, and decision-making problems.



Futuristics representation of a high-performance ASIC

Source photo.ai

# Edge-Computing

## WHAT IF ?

---

### AUDIO SENSORS

The combination of two or three tiny MEMS microphones into one same housing provides more data for an edge-processor to filter-out the ambient noise and even determine the spatial relative origin of incoming sound.

#### WHAT IF...

*... the Edge Machine Learning algorithm could contextualize the surrounding's noise to automatically transmit warning and critical threat data?*

### VIBRATION SENSORS

The raw parameters provided by a vibration sensor affixed to an axle, or its bearing, are filtered and classified by an edge-intelligence, so as to supply only two types of messages: the regular heart-beat, or the warning message.

### VIDEO SENSORS

Videos sources are the largest data producers. Vehicle classification is a priceless edge application as the machine learning algorithm instantly translates to Indication Friend or Foe (IFF), just like onboard fighter jets. However, deceptive tactics are able to lure the identification.

#### WHAT IF...

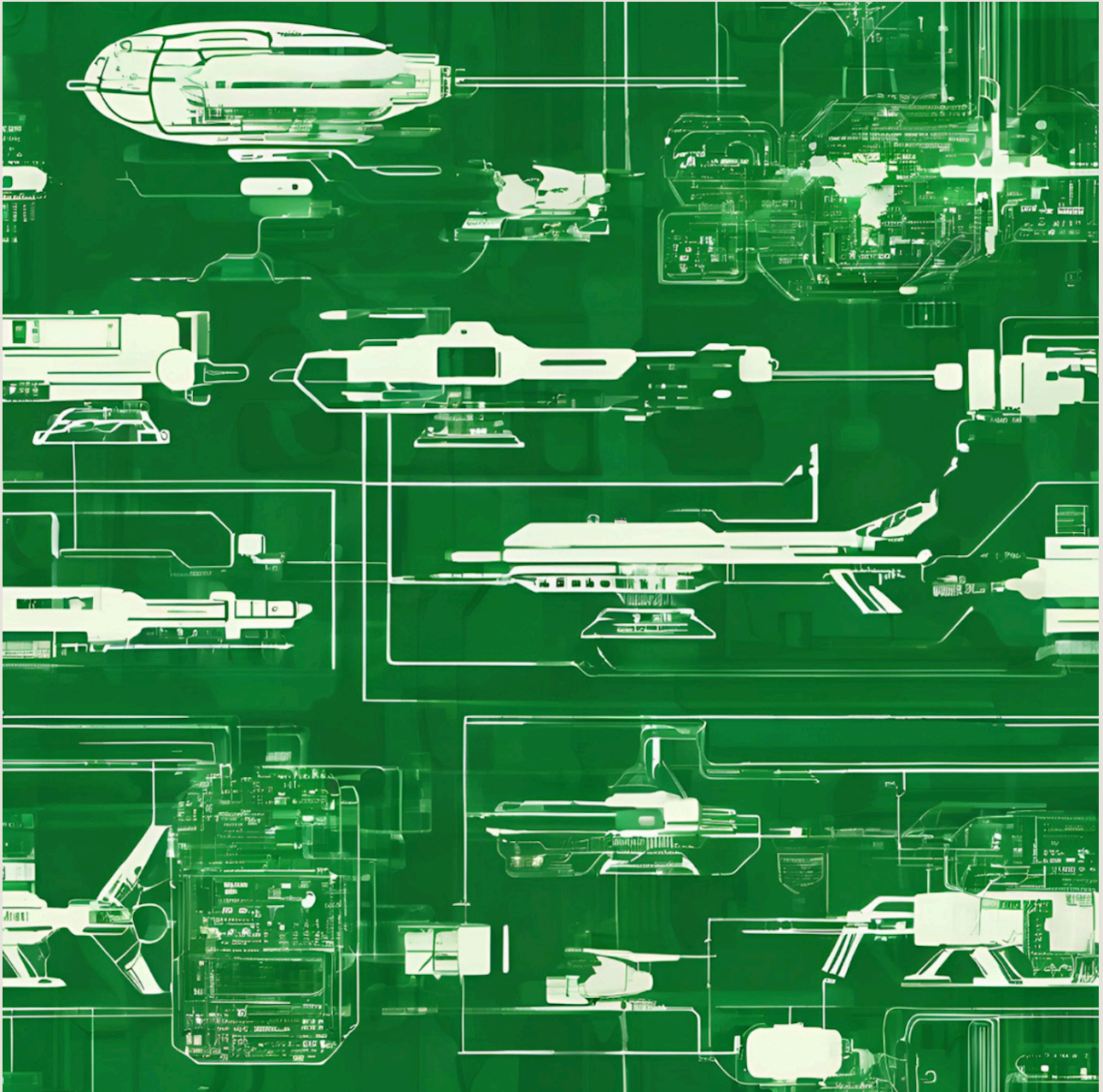
*... the Edge intelligence could also analyze the situation and context to provide a doubt index to the classification result?*

#### WHAT IF...

*... a hacker manages to break-in and generate random warning messages?*







CHAPTER III

# Future Trends and Innovations

# Build your own

CALL TO  
*Innovators!*

## INTERNET OF MILITARY THINGS

### IT IS YOUR TURN

The frontline of the battlefield has been defeated several times with the same scenario despite all the IOT sensors and actuators already dispatched.

Describe precisely the scenario (What, When, Where), figure out Why the IOT sensors or actuators fail, and Who is the right person/team to improve.

Answer as precisely as possible the questions below to prepare the future IOT. Use the options, drivers and trends of technology subsystems in chapter II to prepare the future IOMT. Try to keep the concept as simple as possible.

Start by selecting a relevant topic. Examples: Population, Education, Water, Cyber, Supply-Chain, Maintenance, Energy, Network. Unmanned, Robotics, ...

1

**Topic** .....

2

- IOT Sensor**
- IOT Actuator**

3

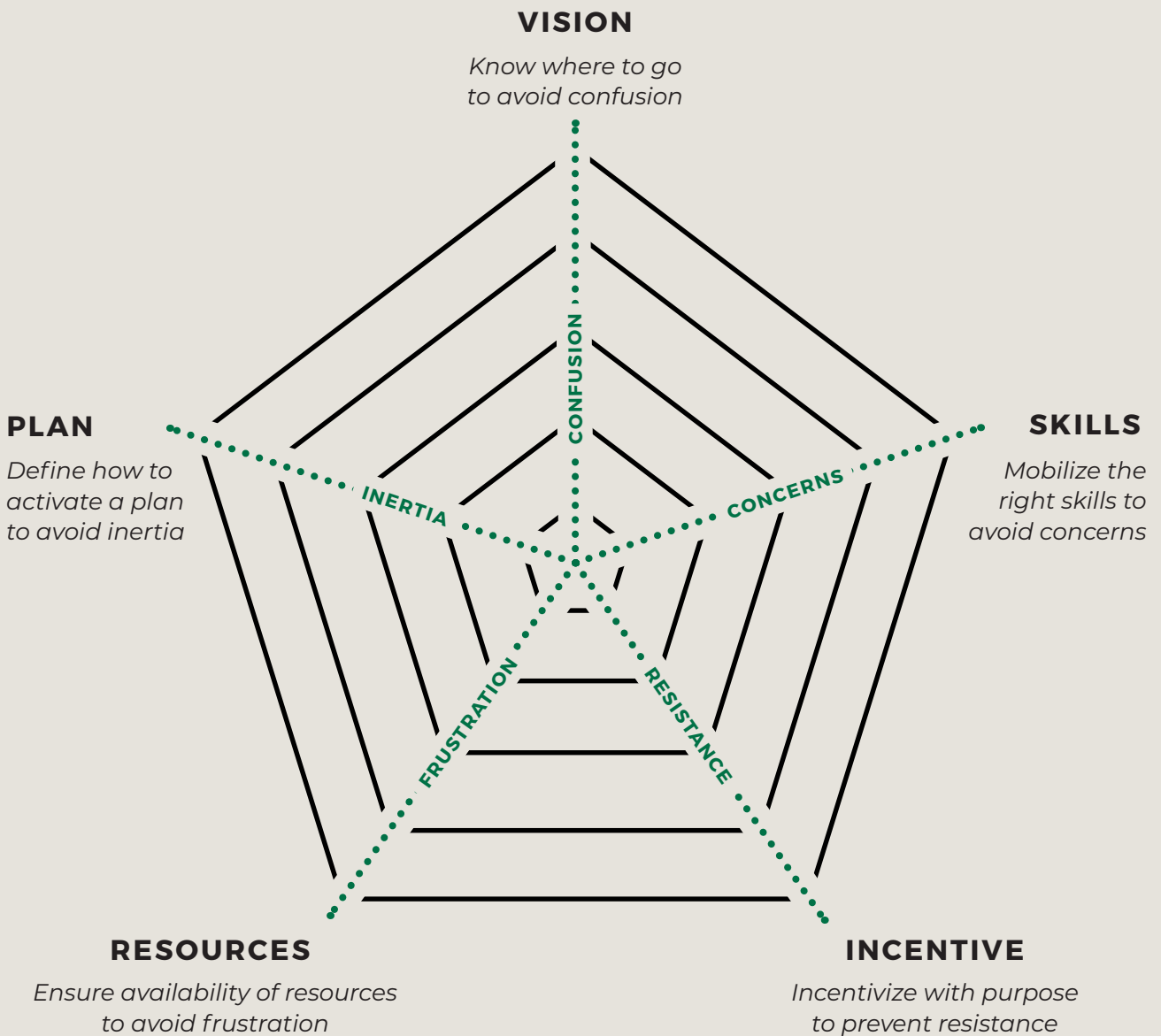
<b>Problem to solve</b>	What, When, Where, Why, Who
<b>Purpose</b>	My IOMT's purpose is to ...
<b>Function</b>	It has the ability to ...
<b>What's distinctive</b>	Compared to ..., it also ...
<b>Success factors</b>	To be successful, My IOMT will ...
<b>Components</b>	It will consist of the following components ...
<b>Characteristics</b>	Sensitivity, Protection, Lifetime, Range, Response time,
<b>Recyclability</b>	When done with its military purpose, it can be ...
<b>Upcyclability</b>	My IOMT can be done using existing ...

# Technology at Play

## FRAMEWORK

---

Using this framework provides a way to map the potential of the future IOT. Maximise his chance for it to become real.



# What is your

## INTERNET OF MILITARY THINGS

---

Imagine your Internet of Military Things, operating on terrestrial and non-terrestrial-network integrations (Space-Air-Ground-Sea Integrated Networks); think about quantum encryption, and bio-inspired IOT technologies for tactical, military, and civil protection applications.

**Problem to solve**

**Purpose**

**Function**

**What's distinctive**

**Success factors**

**Components**

**Characteristics**

**Recyclability**

**Upcyclability**

# Combine the Options

---

Semiconductor
Sensor
Actuator
Network
Security
Energy
Antenna
Edge-AI

## VERIFICATION

---

$$\text{IDEAL OUTCOME} = \frac{\text{BENEFITS} \uparrow}{\text{DRAWBACKS} \downarrow}$$

# What if ?

---

## Internet of Military Things

---

### WHAT IF

smart-dust sensors could be spread disseminated and auto organize their reports. Purpose: provide real-time data to complement situational awareness?

### WHAT IF

Bio-mimicry suggests protein activation to convey messages. What If the IOT sensors and actuators could convey the information using proteins instead of wireless radio transmission?

## Semiconductor

---

### WHAT IF

light and flexible cellulose-semiconductors, built with renewable natural compounds, would combine its characteristics to interfere directly with microorganisms?

### WHAT IF

trade restrictions would limit the usage of quantum super powers to several happy few?

### WHAT IF

Will the augmented soldier benefit from disposable skin patch to monitor his operational ability?

## Antenna

---

### WHAT IF

fixed wing Unmanned Aircraft Vehicles (UAV) would carry RISs affixed under the wings? Those RIS UAVs could be orbiting above the terrain for which an extension of the LoS is required, providing a superior telecom advantage.

### WHAT IF

the Personal Locator Beacon could concentrate and direct the transmission to a specific area?

## Energy

---

### WHAT IF

all the solid-state electrolyte material components be so abundant and harmless to the environment?

### WHAT IF

the protective case consisted in total or partially of the solid-state structure of batteries?

### WHAT IF

the artificial intelligence could assist to identify precisely where and when to direct the energy harvester?

## Sensors

---

### WHAT IF

quantum sensors with multiple entangled ions could overcome GNSS frequency jamming, retaining high accuracy timing and navigation capability on the battlefield?

### WHAT IF

advanced sensing technology could reproduce the tactile perception and convert to relative sensation for remote sensing feedback?

## Cyber-Security

---

### WHAT IF

the future quantumSIM could understand who we are, harness the power of AI and quantum computing safely to guarantee personal privacy?

### WHAT IF

the combination of bio-electronics with quantum algorithms and machine learning would provide the ultimate link to our uncompromizable digital twin?

## Edge-Computing

---

### WHAT IF

the edge machine learning algorithm could contextualize the surrounding's noise to automatically transmit warning and critical threat data?

### WHAT IF

the Edge intelligence could also analyze the situation and context to provide a doubt index to the classification result?

### WHAT IF

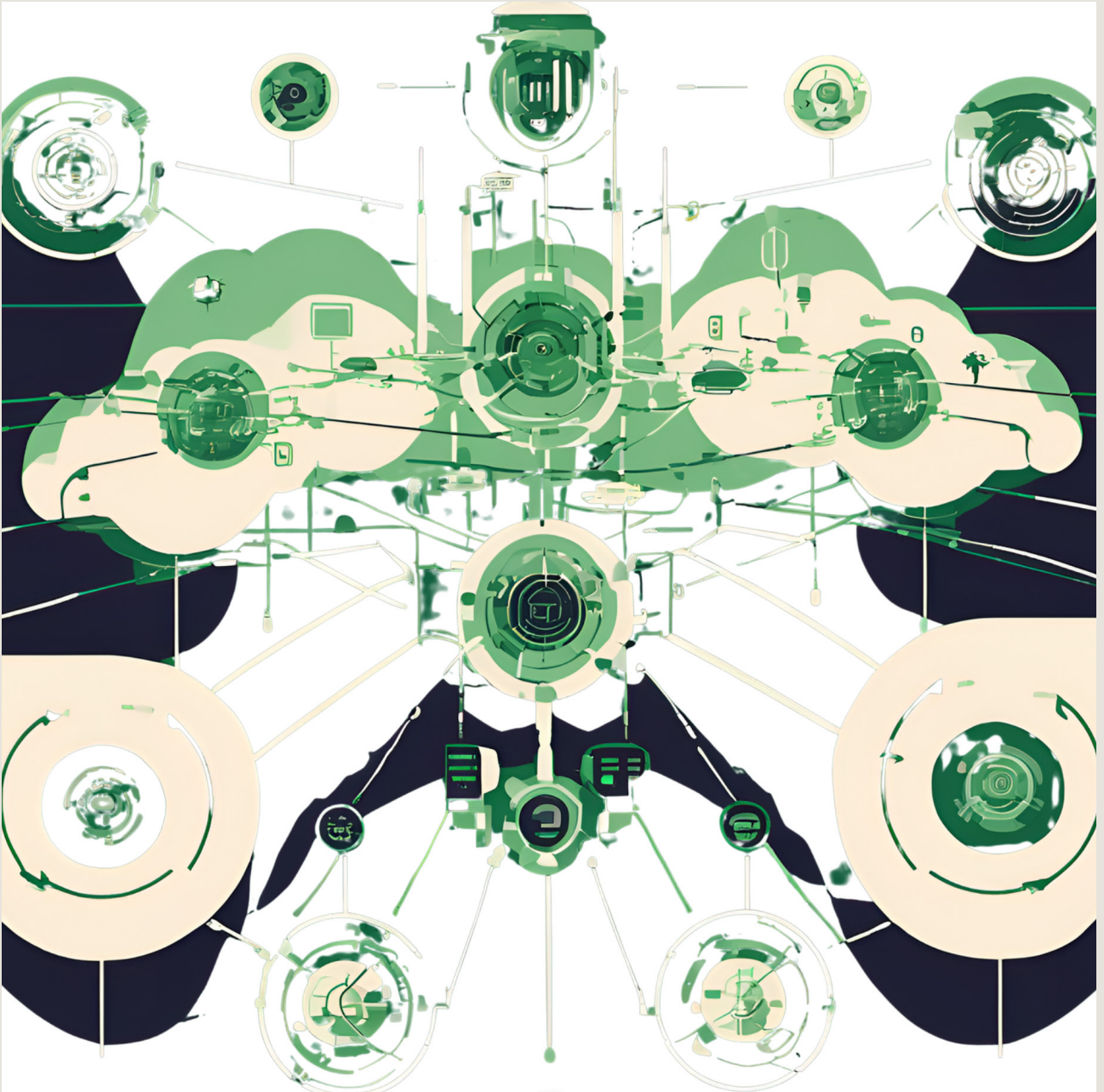
the visibility of encryption keys could be hidden from the network? Adopting a zero trust architecture with separated network segments could reduce the visibility of cryptography key storage.

### WHAT IF

a hacker manages to break-in and generate random warning messages?







CHAPTER IV  
**Appendix**

# Appendix 1

## MOBILE COMMUNICATION FROM ITS ORIGINS

### 1G

The 1980s saw several countries launching their own voice-communication network initiatives. The 1G networks were not necessarily compatible and interoperable between countries. The information was analog transmission, prone to many weaknesses. Among them, the clear over-the-air voice transmission that could be captured by any radio amateur suffered from the lack of privacy in conversations, the handover between cells suffered reliability, and the limitation of density with limited bandwidth and time switching mechanisms.

### 2G

Early 1990s, the GSM (Global System for Mobile Communication) standards were introduced for better interoperability between countries. The GSM 2G was based on Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA) as digital modulation techniques, with ability to carry both voice and short message services (SMS). Digital voice and data was introduced, offering improved security and privacy in telephone calls. With digital voice encoding, simple eavesdropping with a radio scanner on the transmission frequency became useless. The standard called for a specific signaling channel, data confidentiality and mobile station authentication with the introduction of the SIM card. Many services in use today are built on the grounds of the 2G standardization effort. Among them, SMS, in-

ternal roaming, conference calls, call hold, billing based on usage.

The 2.5G is the first data transfer connected to the internet network, developed between 2000 and 2003 based on technology evolutions. The GPRS (General Packet Radio Service) and EDGE (Enhanced Data Rates for GSM) were included in the GSM standards. With flexible data transmission rates, GPRS provides a continuous connection with the network resulting in users being charged for the amount of data transfer rather than connection time. The GPRS sets a strong milestone in the wireless as a service.

### 3G

In 2000, the 3G network was launched on the basis of 2G to offer communications and internet access at 2 Mbps. Services like web browsing was just starting to become wireless. TV streaming, or video streaming weren't accessible, but the digitalization of those services was still in its infancy. Security limitations of the 2G were improved, providing two way authenticating, resulting in Authentication and Key Agreement (AKA).

With 3.5G, faster data rates was achieved using High-Speed standards HSUPA, HSDPA, and EVDO. Those improvements started supporting high-quality video applications with higher data rates compared to prior generation.

## 4G

Launched in 2010, the 4G differs from the previous standards by bringing the Ethernet IP protocol to wireless radio. Consequently, the completely IP based system provides an extension to terrestrial internet services like high-speed, high-quality, and high-capacity services, VoIP and multimedia, with improved security. The 4G standard introduced packet switching as well as an all IP network in the Long Term Evolution (LTE) standard, carrying also the benefits of seamless handover from previous generations of infrastructure.

Notice that the 4G became the first truly internationally deployed mobile communication network worldwide. Before, there were still countries, like Japan, who were using their own proprietary, and very competitive, technologies.

## 5G

5G networks have started their expansion in the early 2020s. The primary promise of 5G is to radically increase the security and quantity of objects connected to the mobile network, with a much higher data throughput and reduced latency. High-quality of services is becoming ubiquitous with the spread of 5G, opening the path to new innovative usages and applications such as smart cities by connecting sensor networks, traffic management, connection to self-driving cars and other virtual and augmented reality applications. Its high-speed connections could enable better remote sur-

gery and other telemedicine, help companies automate their factories and offer businesses dedicated high-speed internet lanes. Security concerns over the 5G comes from the fact that, for the first time in modern history, China took the lead over occidental countries in the infrastructure development.

The 5G-NTN, for Non Terrestrial Network, is paving the way to 6G, which is intended to offer a worldwide satellite coverage of the mobile network, provided that the mobile equipment can be in view of the sky.

## 6G

Different initiatives are on the way for the definition of the 6G-NTN. Among them, the European Telecommunication Standards Institute (ETSI) has kicked-off the standardization project. The usage of artificial intelligence to sense and shape the network is foreseen to exploit the full potential of radio signals operating in the terahertz segment. The inclusion of sensing capabilities intrinsic to the network presents many opportunities and challenges. Also, the Non Terrestrial cell-free concept opens to vertical extension of the communication to both ground and airborne terminals.

## Appendix 2

### SYMMETRIC VS. ASYMMETRIC CIPHERING

#### SYMMETRIC CRYPTOGRAPHY

is used for file encryption or to encode data flows. It is the easiest to understand.

With symmetric cryptography the same key is used to cipher and decipher a message. Until today, the most secure algorithm is the AES256. AES stands for Advanced Encryption Standard, and 256 is the key length, expressed in number of bits. The United-States National Institute of Standards and Technology (NIST) has approved the AES256 for security usage within the Department of Defense.

However, since the same key is used for ciphering and deciphering of the message, its management is of highest criticality. The process consisting of generating, storing, sending to the distant party, the said distant party being also responsible for securing this key, must be under very careful scrutiny. It is advised to carry external audits to challenge the management of symmetric cryptographic keys.

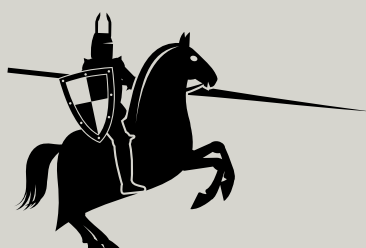
#### ASYMMETRIC CIPHERING

is used to encode small quantity of information due to the intense processing time. Asymmetric encryption is a set of mathematical operations that can be performed with one key and verified or undone with another key. The first is usually the Public Key, while the second is the Private Key.

A public key is distributed by the recipient, for the originator to cipher a message, the said message can only be deciphered by the secret key kept privately by the recipient. Picture the battle scene from ancient times. Generals A, B and C had to exchange messages for proper synchronization of their operations. Prior to the battle, they all agreed to share their public key, and retain for themselves their secret key. Assuming the messenger got captured while travelling from A to C. His ciphered message could not be read, AND could not be corrupted, AND only C could de-cipher the message, back to original.



**KEYS**  
**Secret A**  
*Public B*  
*Public C*



**INTERCEPTOR**

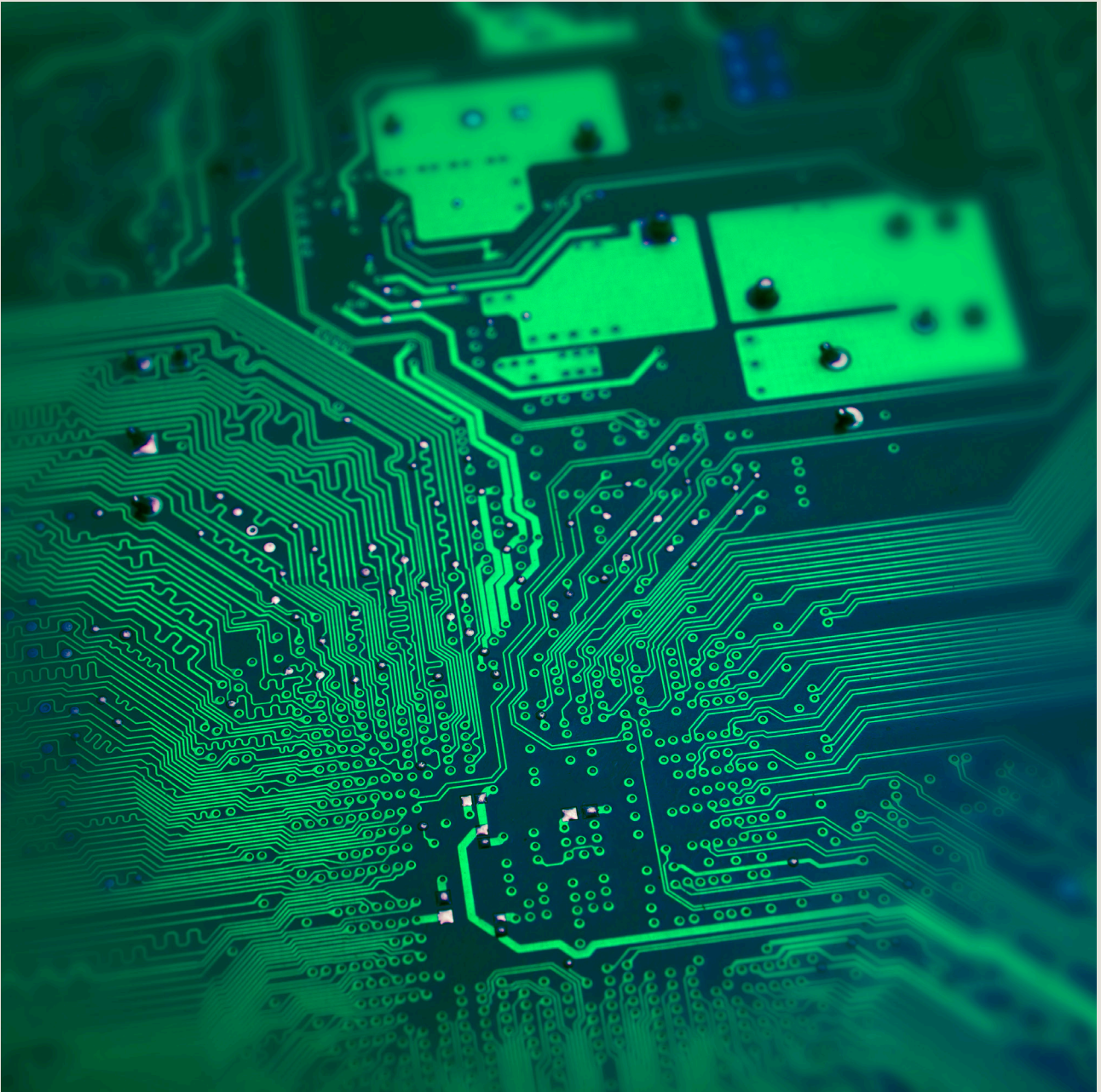


**KEYS**  
*Public A*  
*Public B*  
**Secret C**



**KEYS**  
*Public A*  
**Secret B**  
*Public C*





CHAPTER V

# Glossary

# Acronyms

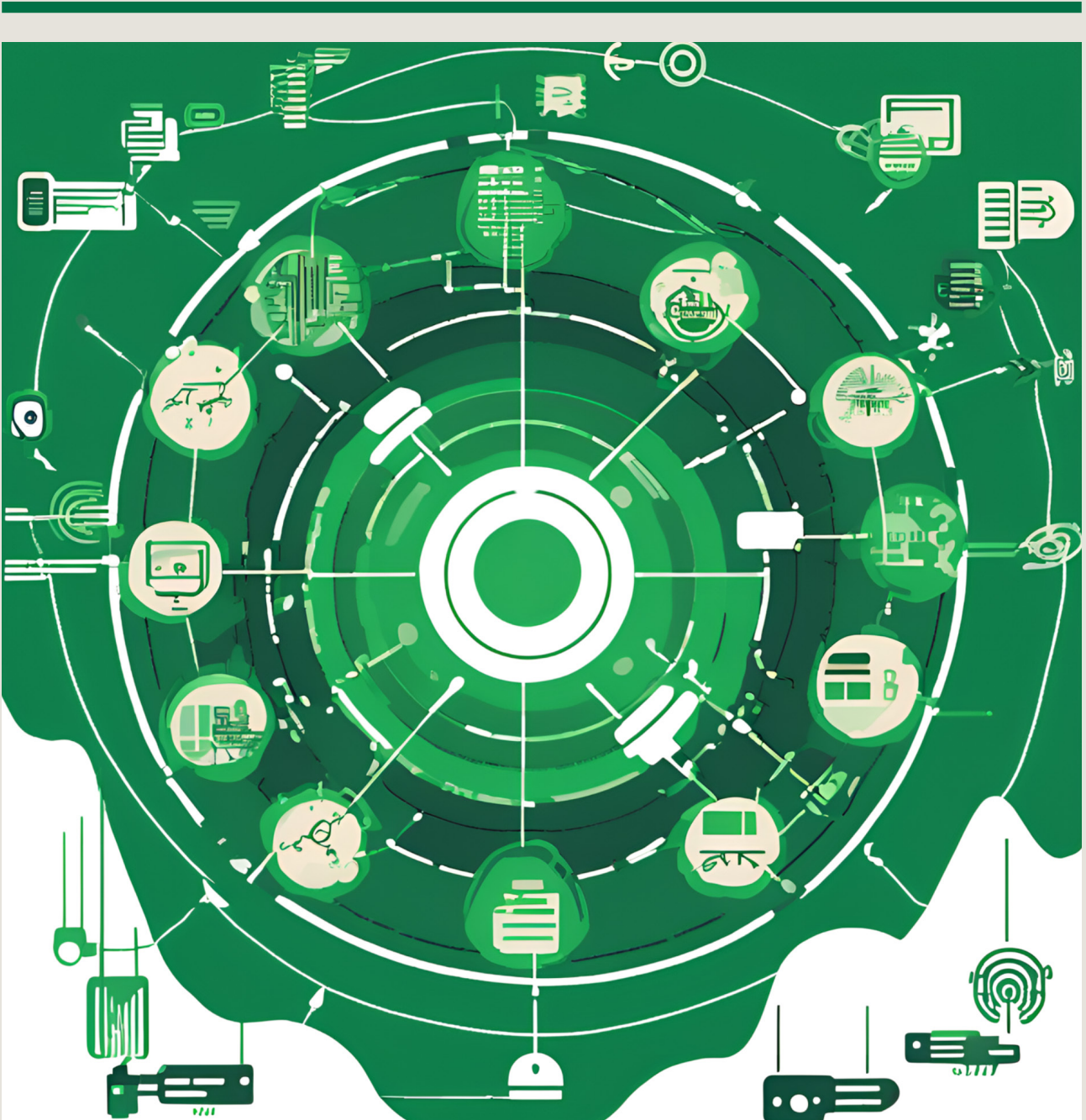
---

<b>AES</b>	Advanced Encryption Standard	<b>IOMT</b>	Internet of Military Things
<b>AI</b>	Artificial Intelligence	<b>IOT</b>	Internet of Things
<b>AKA</b>	Authentication and Key Agreement	<b>iSIM</b>	integrated Subscriber Identification Module
<b>ASIC</b>	Application Specific Integrated Circuit	<b>ISO</b>	International Organisation for Standardization
<b>BCI</b>	Brain Computer Interface	<b>LAN</b>	Local Area Network
<b>C4ISR</b>	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance	<b>LoRa</b>	Abbreviation for Long Range Physical layer Protocol
<b>CDMA</b>	Code Division Multiple Access	<b>LoRaWAN</b>	LoRa Wide Access Network protocol LoS Line of Sight
<b>CMOS</b>	Complementary Metal Oxide Semiconductor	<b>LP-WAN</b>	Low Power Wide Area Network
<b>CNN</b>	Convolutional Neural Networks	<b>LTE</b>	Long Term Evolution
<b>CPU</b>	Central Processing unit	<b>MAC</b>	Medium Access Control Address
<b>DNA</b>	Deoxyribonucleic acid DoS Denial of Service	<b>MCU</b>	Microcontroller
<b>EDGE</b>	Enhanced Data Rates	<b>MEMS</b>	Micro-electromechanical systems
<b>eFPGA</b>	Embedded FPGA	<b>MHz</b>	Mega Hertz
<b>ELT</b>	Emergency Locator Transmitter	<b>ML</b>	Machine Learning
<b>eSIM</b>	embedded Subscriber Identification Module	<b>NB-IOT</b>	Narrow-Band Internet of Things
<b>ETSI</b>	European Telecommunication Standards Institute	<b>NIST</b>	National Institute for Standards and Technology
<b>FPGA</b>	Field Programmable Gate Array	<b>NRE</b>	Non Recurrent Engineering (cost)
<b>GAN</b>	Generative Adversarial Networks	<b>NTN</b>	Non Terrestrial Network
<b>GHz</b>	Giga Hertz GPRS General Packet Radio Service	<b>ODL</b>	On Device Learning
<b>GNSS</b>	Global Navigation Satellite System	<b>OODA</b>	Observe, Orient Decide Action
<b>GPU</b>	Graphic Processor Units	<b>OSINT</b>	Open-Source Intelligence
<b>GSM</b>	Global System for Mobile Communication	<b>PAN</b>	Personal Area Network
<b>HiFi</b>	High Fidelity	<b>PCB</b>	Printed Circuit Board
<b>IC</b>	Integrated Circuit	<b>PLB</b>	Personal Locator Beacon
<b>IEC</b>	International Electrotechnical Commission	<b>PTT</b>	Post Telephon Telegraph
<b>IFF</b>	Identification Friend or Foe	<b>QCF</b>	Quantum Coin Flipping
<b>IMSI</b>	International Mobile Subscriber Identity	<b>QKD</b>	Quantum Key Distribution
		<b>Qubit</b>	Quantum Bit
		<b>RAM</b>	Random Access Memory



<b>RFID</b>	Radio-Frequency Identification
<b>RFID</b>	Radio Frequency
<b>RIS</b>	Reconfigurable Intelligent Surface
<b>RNN</b>	Recurrent Neural Networks
<b>RSA</b>	Rivest Shamir Adelman
<b>SIL</b>	Safety Integrity Level
<b>SIM</b>	Subscriber Identification Module
<b>SINR</b>	Signal to Interference plus Noise ratio
<b>SOC</b>	System on Chip
<b>SNR</b>	Signal to Noise ratio
<b>TDMA</b>	Time Division Multiple Access
<b>THz</b>	Tera Hertz
<b>TPU</b>	Tensor Processing Unit
<b>UAV</b>	Unmanned Aircraft Vehicle
<b>UID</b>	Unique Identifier
<b>US</b>	Unite-States of America
<b>WAN</b>	Wide Area Network
<b>WWW</b>	World Wide Web





CHAPTER VI  
**Sources**

# More information from the sources

---

**armasuisse W+T:** <https://deftech.ch/>

Drohnen Und Roboter in den Streikräften: Die Waffen des 21. Jahrhunderts?  
ISBN: 978-3-906211-88-6

Soldat Augmenté  
ISBN: 978-3-9525653-0-8

Soldat Low-Tech  
ISBN: 978-3-9525653-3-3

Engins & Systèmes Autonomes  
ISBN: 978-3-9525653-4-6

Electronics Foresight  
ISBN: 978-3-9525653-9-1

Quantum Technologies  
Trends and Implications for Cyberdefence – Cyber-Defence Campus, Semi-annual report 2024/1

Mission Critical, Technology or Methodology

**Revue Militaire Suisse:** <https://www.e-periodica.ch/cntmng?pid=rms-001:2000:145::1050>  
Combat SAR Electronic search beyond the radio horizon

**Département Fédéral de la Défense, de la protection de la population et des sports DDPS –  
Armée Suisse**

Armée Suisse Conception Générale Cyber - <https://www.newsd.admin.ch/>

## Other publications

---

Internet of Things in Air and Missile Defence A System Solution Concept  
<https://ieeexplore.ieee.org/document/8870070>

Intervention of Internet of Things in Supply Chain and Logistics Management  
<https://ieeexplore.ieee.org/document/10428672>

Towards an Internet of Things based architectural framework for defence

<https://ieeexplore.ieee.org/abstract/document/7475314>

On The Quantitative Definition of Risk

<https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1539-6924.1981.tb01350.x>

ISO 31000 – Risk Management

<https://www.iso.org/iso-31000-risk-management.html/>

High-speed and large-scale intrinsically stretchable integrated circuits.

<https://www.nature.com/articles/s41586-024-07096-7?fromPaywallRec=true#citeas>

Lithography-free reconfigurable integrated photonic processor

<https://www.nature.com/articles/s41566-023-01205-0>

Quantum circuits with many photons on a programmable nanophotonic chip

<https://www.nature.com/articles/s41586-021-03202-1>

Faster More secure Photonic Chips boosts AI

<https://spectrum.ieee.org/photonic-ai-chip>

The future of deep learning is photonic

<https://spectrum.ieee.org/the-future-of-deep-learning-is-photonic>

At the Speed of Light: Unveiling the Chip That's Reimagining AI Processing

<https://scitechdaily.com/at-the-speed-of-light-unveiling-the-chip-thats-reimagining-ai-processing/>

The future transistors

<https://www.nature.com/articles/s41586-023-06145-x>

Process integration and future outlook of 2D transistors

<https://www.nature.com/articles/s41467-023-41779-5>

Summarizing CPU and GPU Design Trends with Product Data

<https://ar5iv.labs.arxiv.org/html/1911.11313>

Photonics Bus UCle

<https://www.uciexpress.org/>

AI Acceleration Tensor Processing Unit

<https://medium.com/@aamiraftabcloud/ai-chips-and-hardware-acceleration-asics-tpus-gpus-a881993bf92f>

In Sensor and On-device Tiny Learning for Next Generation of Smart Sensors

[https://www.youtube.com/watch?v=EVE06-OHH5U&ab\\_channel=tinyML](https://www.youtube.com/watch?v=EVE06-OHH5U&ab_channel=tinyML)

Graphene

<https://www.nature.com/articles/s41586-023-06811-0>

Marvell optical technology

<https://www.marvell.com/company/newsroom/marvell-launches-products-technology-and-partnerships-at-ofc-2024.html>

Foxconn and MediaTek seize photonics opportunities

<https://www.trendforce.com/news/2024/03/27/news-foxconn-teams-up-with-mediatek-to-seize-silicon-photonics-opportunities-strengthening-ai-server-integration-strategy/>

Intelligence Community OSINT

<https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2024/3785-the-ic-osint-strategy-2024-2026>

Empowering Reconfigurable Intelligent Surfaces with Artificial Intelligence to Secure Air-To-Ground Internet-of-Things

<https://ieeexplore.ieee.org/document/10463696>

Review about the Applications of Nanoparticles in Batteries

[https://www.researchgate.net/publication/372825002\\_Review\\_about\\_the\\_Applications\\_of\\_Nanoparticles\\_in\\_Batteries](https://www.researchgate.net/publication/372825002_Review_about_the_Applications_of_Nanoparticles_in_Batteries)

On-Chip batteries

<https://onlinelibrary.wiley.com/doi/10.1002/aenm.202103641>

Neural Bio-Sensing, EPFL NeuralTree

<https://ieeexplore.ieee.org/document/9905664>

<https://ieeexplore.ieee.org/document/9731776>

Walking naturally after spinal cord injury using a brain-spine interface

<https://www.nature.com/articles/s41586-023-06094-5>

Elon Musk announces Neuralink advance toward syncing our brains with AI

<https://spectrum.ieee.org/elon-musk-neuralink-advance-brains-ai>

<https://neuralink.com/blog/prime-study-progress-update/>

**Photo/Image/Infography credits:** ETSI, U.S. Army, Internet of Battlefield Things (IoBT), Ingecom, Nokia, Pixabay, Techovedas, Nature, Synology, Skyeton, TDK, Nano-Micro, University Basel, Neuralink, IOT Analytics, photo.ai, Freepik, Unsplash, Olivier Desjeux





Information has always been at the center of warfare. Sharing real-time information between sectors is a critical aspect involved in managing the battlefield.

Many innovative tools, protocols and algorithms overwhelm the present of the IOT\*. Shaping the future with all of them is like resolving a Rubik's multicahedron\*\* with n particles on each side. By chance, several patterns already exist between the sides, improving the chances to trace a path that'll lead somewhere.

IOT is a complex mix of interdisciplinary domains like mobile computing, software architectures, embedded firmware, wireless communication technologies, security, networking, sensing technologies, energy efficiency, information management, data analytics and artificial intelligence.

As the society adapts to an increasingly complex security environment, it is imperative to understand how to harness the power of technological improvements and what to operate within new geopolitical contexts. Investments in C4ISR systems and infrastructure to analyze and disseminate data is how advanced military organizations will make the difference.

Fasten your seat belts, we're engaging in a fascinating road-trip. From vision to execution, from chip to solution, get ready. The world of augmented possibilities gets available to shape our Futures.

