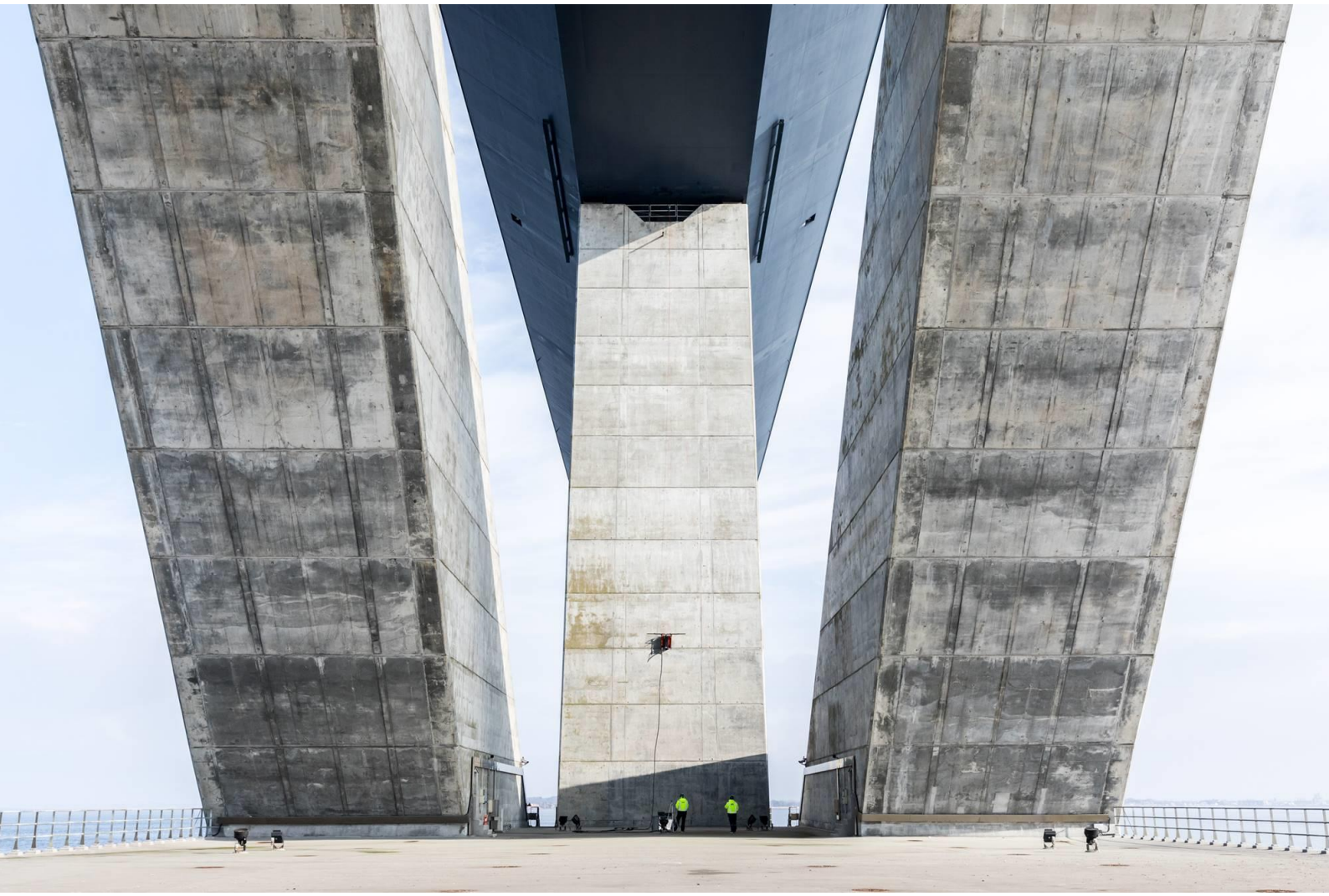
Successfully adopting IoT in harsh environments



***Anders Jacob Madsen**, IoT, Technology & Architecture Specialist,*
IoT, Data & Services Innovation, FORCE Technology (ajm@force.dk)

***Michele Colli**, Industrial IoT Specialist,*
IoT, Data & Services Innovation, FORCE Technology (mic@force.dk)

Table of Contents

1. IoT and the need to deal with harsh environments 3

2. What is a harsh environment? 3

3. Classifying harsh environments: the use of standards 5

4. Mission profiling and the need for considering virtual aspects when dealing with IoT products 5

5. The importance of testing in realistic environments 8

6. Cases 9

7. Winning in harsh environments: key takeaways 11

References 11

1. IoT and the need to deal with harsh environments

With the spread of the Internet of Things (IoT), “smart” connected products are being adopted in increasingly diverse environments and for increasingly diverse applications. These often imply particularly challenging places, where IoT can facilitate the monitoring of critical parameters and relieve humans from both expensive and dangerous jobs. Nevertheless, the application of IoT in “harsh” environments is not without challenges, as harsh environmental conditions either prevent a device from functioning properly or degrade it too fast, significantly reducing its operating lifetime.

Because of that, when designing an IoT device intended for a harsh environment, special design and testing guidelines need to be followed in order to make sure that the technology installation functions properly for the required operating lifetime.

This whitepaper addresses the need for information concerning the adoption of IoT in harsh environments, both unfolding the related characteristics and challenges and suggesting a set of guidelines, tools and approaches to address them.

2. What is a harsh environment?

All electronic products degrade over time despite the environment. IoT products – which are strongly based on electronics - make no difference. Each environment entails a set of stress factors that cause – sooner or later – the degradation of electronics over time. Harsh environments are characterized by a particularly challenging set of stress factors, which cause a significant increase in degradation speed, generating a precocious failure of the product.

Some of these stress factors, when particularly severe, can either limit or completely prevent the product from functioning. For instance, if water or electromagnetic compatibility (EMC) are not handled correctly, the eventual ruggedization of the product may immediately either destroy or prevent the correct functioning of the product.

The most common stress factors that are generally characterizing harsh environments are the following:

- EMC
- Radio frequency
- Vibration
- Shock
- Mechanical stress such as flection, torsion, traction and compression
- Temperature
- Humidity
- Water
- Dust
- Pressure
- Corrosive chemicals such as salt, acid and gas
- Power supply

Commonly known industries characterized by harsh environments are transportation, marine, space, construction, mining, heavy industry and farming. These sectors require particular attention and testing when it comes to designing and developing an IoT product.

Most of the known stress factors characterizing harsh environments are indeed considered when designing and testing electronic components. To contain development expenses, such components are usually designed in order to be able to cope with a wide spectrum of applications, complying with industrial standards ensuring that the aforementioned stress factors are taken into account up to a certain degree.

Nevertheless, IoT products have proven to be subject to further stress factors in addition to the aforementioned ones. These can be classified as “virtual stress factors”, and concern the data processing activities characterizing the environments where such products have to operate it. Examples of virtual stress factors are

- Computing capacity
- Data-rate
- Latency
- Range
- Stability
- Interoperability

These should be taken into account as well in order to ensure the expected performance and durability of IoT products that need to be deployed in harsh environments.

3. Classifying harsh environments: the use of standards

To be able to quantify the levels of harshness of an environment is fundamental in order to identify which are the right industrial standards to refer to when designing (or choosing) an IoT product that has to operate in a harsh environment. A way to quantify the harshness of an environment (and the capability of an IoT product to deal with it) is to take advantage of standards that classify the stress factors that characterize an environment. One of the most known it is the so-called "*ingress protection rating*", or IP rating.

The IP rating is built on the IEC standard 60529. The IP rating is a scale indicating the resistance of a product to water and to dust, and is denoted by IPXX. The first X is to be replaced by a digit – between zero and six – which represents the level of dust resistance of a given product. The second X is to be replaced by a digit – between zero and nine – which represents the level of water resistance of a given product. While a value of zero represents no protection, a value of nine represents the highest possible protection. For instance, the capability of an IoT product to operate in environments characterized by high-pressure and high-temperature jet sprays, wash-downs, and steam-cleanings.

As for incrementally grading the resistance of a product to water and dust, the IP rating can also be used as a well-established scale across different industries to evaluate the harshness of an environment.

As the IP rating, there are several standards that can be used to classify the stress factors that characterize an environment and, consequently, evaluate its harshness. For instance, IEC 62368-1, Annex Y, is used to classify vibration and shock for outdoor equipment while IEC 60601-1-11 is used to classify particularly relevant stress factors for medical devices.

4. Mission profiling and the need for considering virtual aspects when dealing with IoT products

Stress factors are, however, often more complex that water and dust alone. It is therefore important – for each product – to identify all the relevant stress factors that should be considered when designing (or choosing) it.

Mission profiling is a process that provides the user with an overview of all the stress factors that affect a product throughout its lifetime. This is used by engineers to support them in the development of a robust and reliable product which is able to survive the physical conditions that characterize the product's operating environment.

There are multiple ways of approaching mission profiling. The ZVEI Handbook for Robustness Validation - a handbook realized for the automotive industry - describes a set of guidelines for designing robust electronic modules for vehicles through mission profiling (Figure 1).

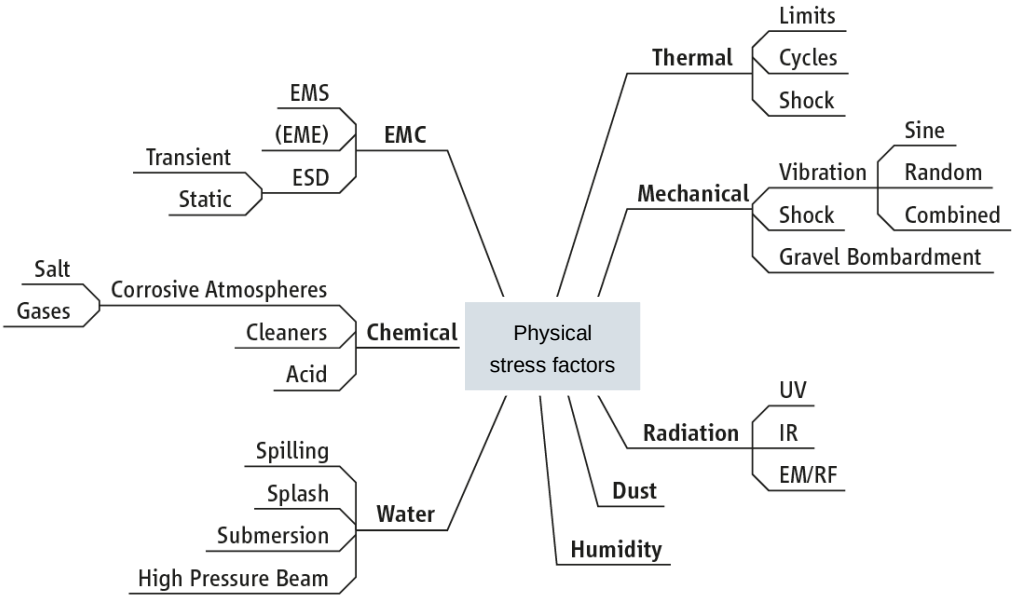


Figure 1 - ZVEI tree describing the physical stress factors affecting a vehicle (Elektrotechnik-und, 2013)

Such guidelines can be used for facilitating the design of robust IoT products, minding that IoT products, due to their nature, entail not only a physical but also a virtual dimension, concerning the generation, transmission, analysis and use of product data that are intended to support the execution of physical or decision-making processes. This generates additional "virtual stress factors" that need to be considered. These can be related, for instance, to software, firmware, data transmission, data storage and computing capacity, and can affect the performance of an IoT system. For example, the availability of meta data is important to diagnose the status of an IoT device, but it also lowers the effective data throughput for the payload, as it increases the size of the package that is sent. This stresses the data transmission function and limits the performance of the IoT system.

According to that, the overall environmental and functional stress factors affecting an IoT product can be clustered in four main groups:

- Virtual environmental stress factors
- Virtual functional stress factors
- Physical environmental stress factors
- Physical functional stress factors

Virtual environmental stress factors concern the capabilities of the software platforms an IoT product is connected to and (and which are used to process its data) and their limitations from, for instance, an analytic or storage perspective.

Virtual functional stress factors concern the interactions between an IoT product and the software platforms, for instance the frequency at which the platform accesses data from the IoT product or the need for constant data streaming from the IoT product to a software platform.

Physical environmental stress factors concern the physical characteristics of the environment where the IoT product has to operate in (see the list in section 2).

Physical functional stress factors concern the physical interactions between the IoT product and the system where the product is being deployed, whether these regard human-to-machine interactions or machine-to-machine interactions. For instance, how many times a button is pushed or how many times an actuator is activated.

Starting from the concept from ZVEI (Figure 1), FORCE Technology has developed an environmental stress factors tree regarding IoT products. This contains the above mentioned four stress factors' clusters and unfolds the related stress factors (see Madsen, 2020).

The different stress factors for IoT products can be further categorized under each one of the four clusters (Figure 2).

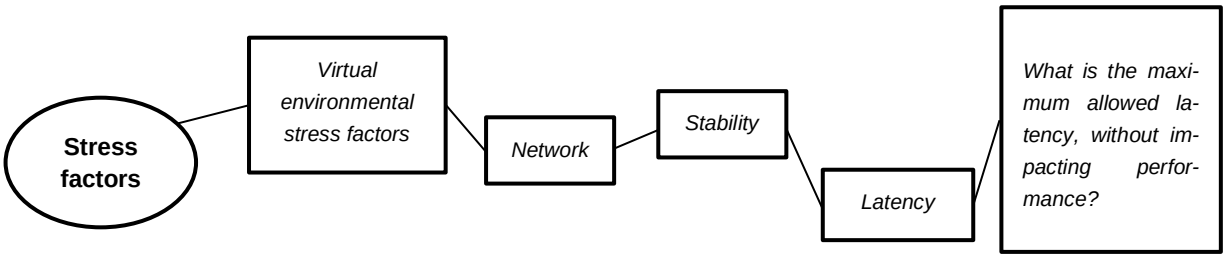


Figure 2 - Example of categorization in the environmental stress factors tree from FORCE Technology

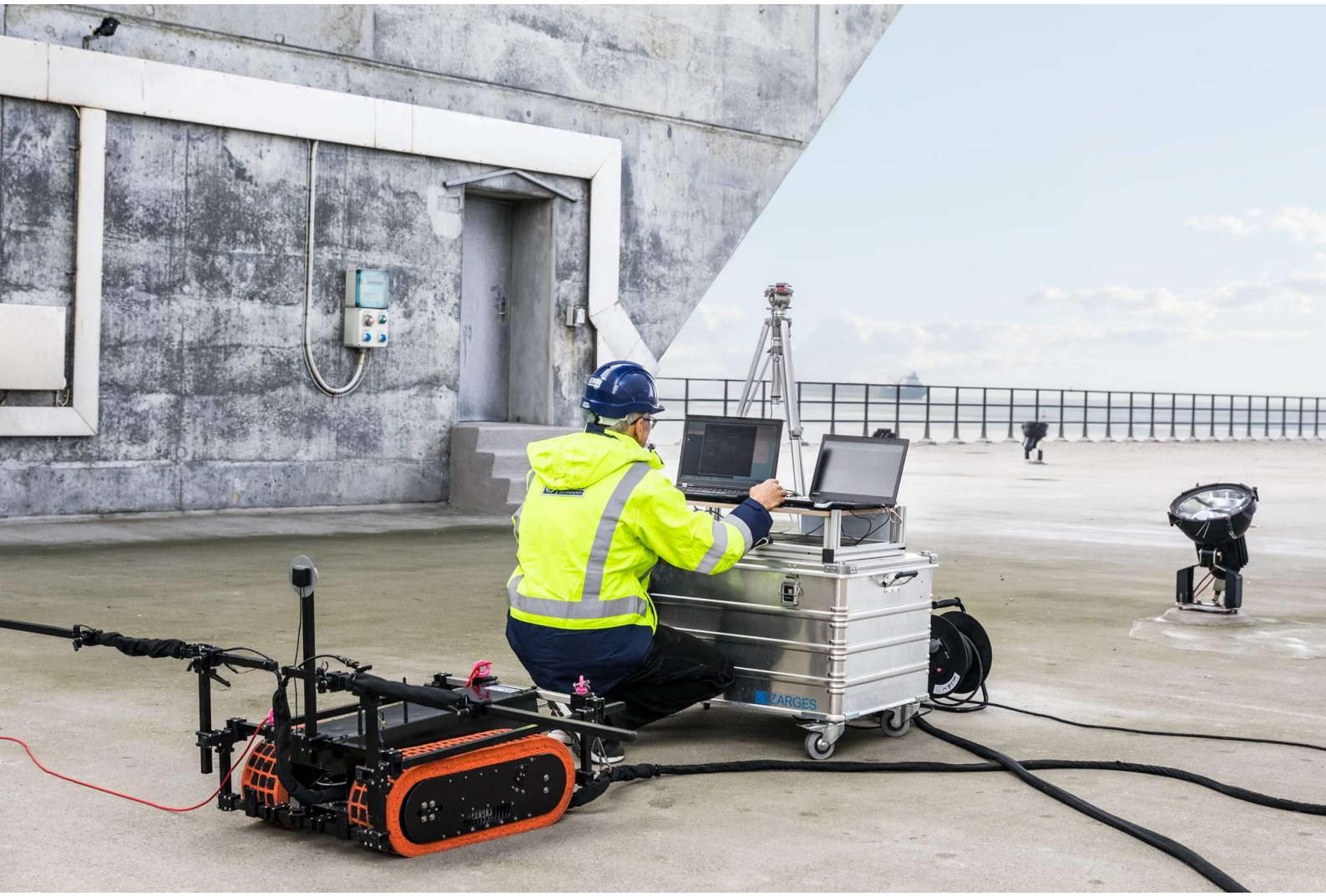
Each cluster has a lot of sub-categories – down to five levels – to ensure the clear identification of each stress factor (Madsen, 2020). These are:

- Level 1: Cluster
- Level 2: Categories
- Level 3: Parameters
- Level 4: Sub-parameter (detail)
- Level 5: Questions

5. The importance of testing in realistic environments

When all the relevant environmental stress factors have been identified, the IoT product has to be tested in order to verify its compliance with the defined standards. An often-overlooked part of testing is testing in a realistic environment – fundamental to ensure the actual compliance of an IoT product in operating conditions, especially when it comes to harsh environments.

The testing in a realistic environment highlights those faults that are a product of combinatorial stress. For instance, while stress related to heat and to salt themselves could be below a warning level, it is their combination that catalyze corrosion. Similarly, there are several other combinatorial pitfalls that need to be taken into consideration: it is therefore paramount to set up a realistic environment testbed for identifying them.



6. Cases

Wireless communication from light poles

The case involves a municipality in Denmark which, after installing a “smart” lightning system, immediately started experiencing systematic issues in its behavior. The “smart” system consists of 3000 light poles equipped with a low-power wide-area network (LoRa) and should be able to locally control its lighting intensity according to the external natural light conditions, optimizing lighting effectiveness while minimizing energy consumption.

Before being installed, the poles have been tested in regard to:

- *Temperature* - Inside a light pole, temperatures can reach 50 degrees Celsius during a summer day. The “smart” components located inside the pole must withstand such temperatures and function correctly in those environmental circumstances
- *Power supply* - The “smart” components have been designed to be powered by the same power supply of the light pole - 230 VAC. It had been made sure that, in compliance with CE specifications, the power supply was not noisy or had any alarming transients
- *Communication* – Due to the need for communicating a very small amount of data, the poles communicate through LoRa, which is using the 868 MHz ISM band, a non-licensed radio frequency that can be used by everybody complying with a set of rules regarding “on air” time and transmission power. Testing activities concerned the number of nodes to be simultaneously connected (i.e. 3000) on the 8 gateways

Although single poles have been tested in these regards, they have not been tested combinatorically as a whole system, making sure to resemble – during the testing activities – a realistic setup. Indeed, when installed and scaled in the 3000 light poles, the problems arose: poles could not turn on simultaneously when they should have.

Connecting to a LoRa network requires a system to generate a “join request” and a “join accept” message. In the Danish municipality’s smart lightning system, this process had to be scaled to 3000 poles which, at the same time, had to generate these messages and communicate them through 8 gateways only. On one hand, this caused messages to interfere with each other. On the other hand, since LoRa gateways are only half-duplex, several poles’ messages have been completely lost, as gateways were not able to receive a message from one pole while transmitting a message from another one.

This case shows how preliminary testing simulating a realistic environment is often fundamental to avoid large costs related to the retrofitting of the whole system after its installation.

Temperature of pipes on a vehicle

The case involves the development of a system to be installed on a vehicle in order to measure pressure changes in its pipes.

The ability to measure pressure changes in a pipe may entail the installation of a temperature probe inside the pipe. While this provides the needed pressure data by measuring the temperature gradient inside the pipe, the installation of the probe is performed by breaching the pipe: this introduces a weakness point in the pipe, making it more prone to leaking. Another way to detect such changes in pressure is by measuring temperature changes on the surface of the pipe. While pressure variation data are not as accurate as the ones provided by a probe, the installation of this system is not invasive: it does not require to breach the pipe and, consequently, it does not compromise the structure of the pipe and its capabilities to avoid leakages.

To be able to choose the best measurement system to detect pressure changes in a pipe in a specific case, it is paramount to identify – at first - both the needed data accuracy as well as the needed resistance to leakages. Once these have been clarified, testing in a realistic setup is required to validate the behavior of these two different systems when providing data concerning pressure changes in the vehicle pipes.

The testing has been performed on a real vehicle equipped by such systems in regard to:

- *System installation to provide the right data accuracy* – On one hand, the temperature probe measures the temperature of the flow it is directly exposed to. On the other hand, external temperature sensors – which measures the temperature of the flow indirectly - should be applied on the pipe surface despite its curvature. It is fundamental to find the right sensors which can adapt to such curvature, clamping properly on the pipe. In addition to that, the air turbulence outside the pipe – and interacting with its surface – needs to be taken into account as it could interfere with the indirect temperature measurement, e.g. cooling down the pipe where the sensor is positioned and giving a false readouts. Insulation might be needed
- *Network coverage* – Data needs not only to be generated, but also to be transmitted. Network coverage is hence important, especially because the system will be moving. This limits the choice of network technology and therefore also the power consumption related to data transmission

The test showed that, for the external sensors, considering the temperature changes at the vehicle testing speed and in order to provide the required data accuracy, data points had to be collected at least five times per minute. This highlighted how battery-powered sensors were not feasible due to the high data transmission frequency, which was considered too energy consuming. This led to the choice of adapting the system in order for it to be able to run on the main power supply on the vehicle. However, this generated too much noise, compromising the quality of the data generated by the probes.

The insights obtained through the testing activities led to significant system changes. It is worth highlighting that these insights would not have been detected if the tests would have not been performed taking advantage of a realistic setup.

7. Winning in harsh environments: key takeaways

To be able to develop technology solutions – in our case, more specifically, IoT solutions – which can successfully deal with harsh environments often requires an extensive amount of testing. While this prolongs time to market, it can significantly reduce the risk of ”unexpected errors correction” costs.

To do so, there are few key points to be taken into account when testing IoT solutions that need to be deployed in harsh environments:

- Perform a “mission profiling” to identify all the physical critical stress factors characterizing an environment (e.g. EMC, radio frequency, vibration, shock, mechanical stress - flection, torsion, traction and compression, temperature, humidity, water, dust, pressure, corrosive chemicals – e.g. salt, acid and gas, current)
- Take advantage of existing standards to classify the harshness of an environment, such as the IP rating and other standards concerning shocks and vibrations for outdoor equipment (IEC 62368-1) and medical devices (IEC 60601-1-11)
- Take into account virtual environmental and functional stress factors in addition to the physical ones
- Test every identified critical stress factor both individually and in combination with the other stress factors
- Test every identified critical stress factor in a realistic setup
- Comply with industry standards, which are based on former testing experience in a field. This would facilitate the design of IoT solutions that can resist to application environments – even when harsh – and may increase the market access of a product, as they could be a requirement from some potential customers - especially when dealing with harsh environments

References

Elektrotechnik-und, Z. Z. (2013). Handbook for Robustness Validation of Automotive Electrical/Electronic Modules.

Madsen, A. J. (2020). IoT Trust Assurance Guideline. Nordic Iot Centre. https://nordiciot.dk/iot-trust-assurance-guideline/