Rugged devices in the Enterprise

WHITE PAPER

hexnode

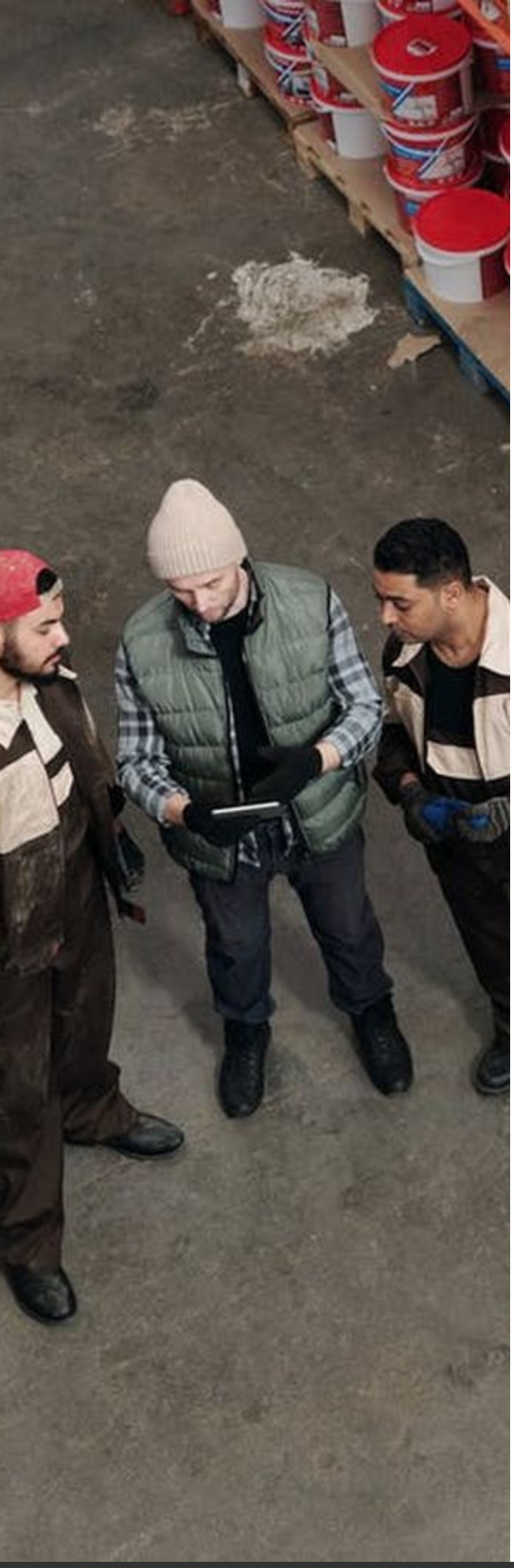
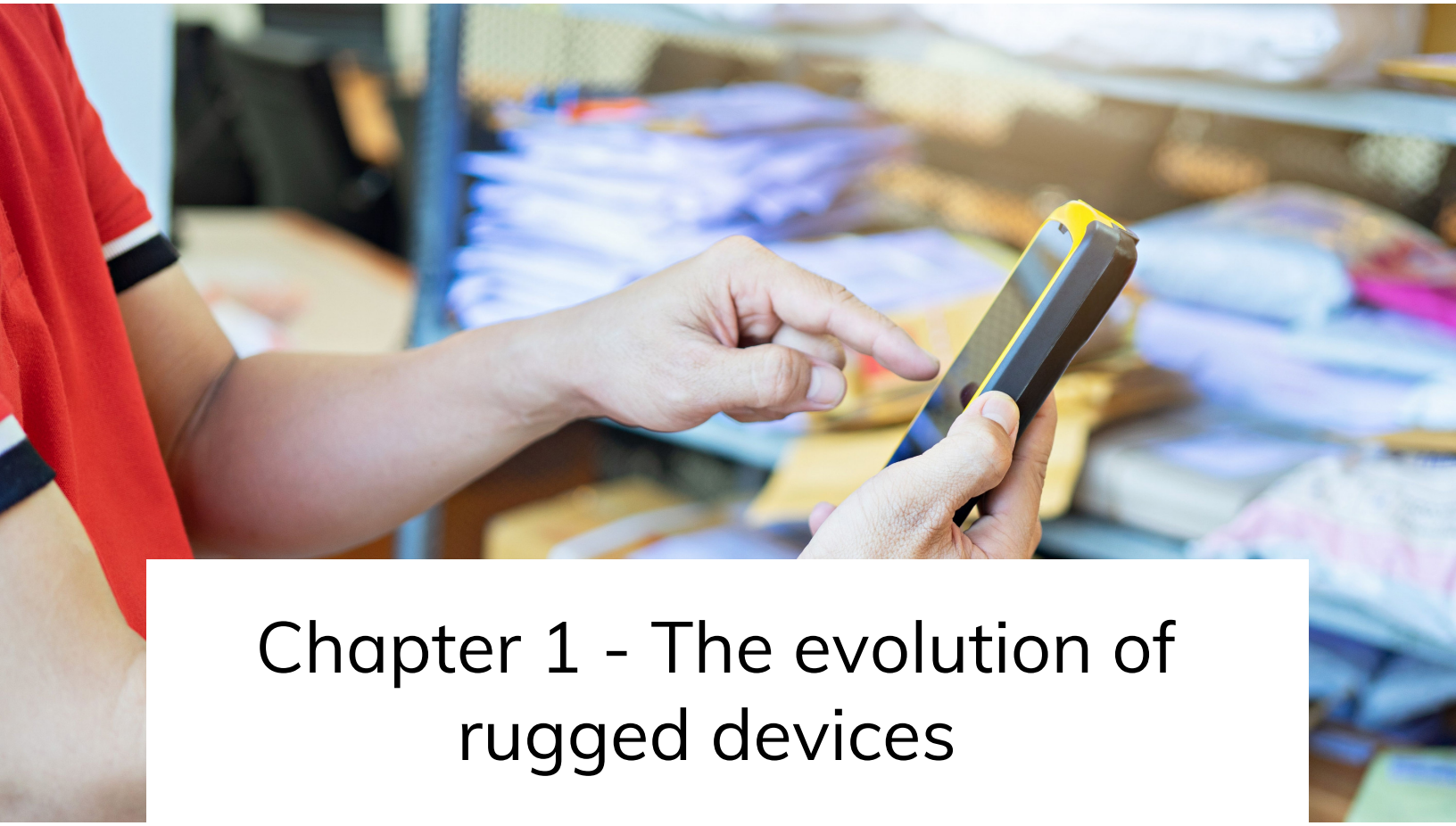


Table of Contents

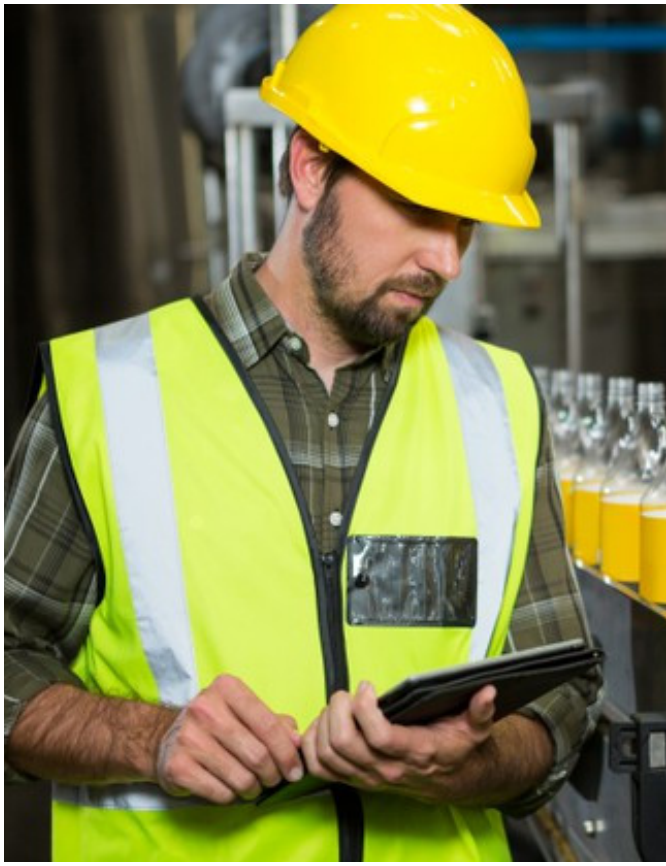


Chapter 1 - The evolution of rugged devices

The DVW Husky issued in 1981 was the very first handheld computer that was designed to be used in harsh weather conditions. The device could be dropped from a great height onto hard surfaces without suffering any damage, and it was waterproof. The Husky was first manufactured for Severn Trent, a water company based in the UK and was later used by the Ministry of Defense for its Rapier Missile project. Pretty soon, devices with barcode scanners began appearing in warehouses for easier inventory management.

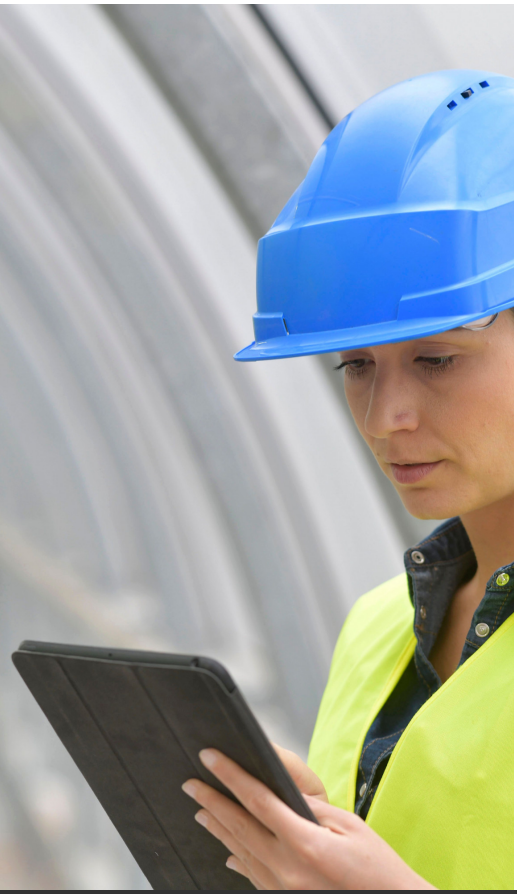
It wasn't until the early 1990's that portable computers with scanners capable of recording proof of delivery were manufactured. FedEx used Honeywell's (known then as Hand Held Products) Micro-Wand portable data collection device to start the system of proof of delivery for tracking their packages.

Problem with these early devices



Early devices, due to the limitation of components present at the time, were only capable enough for basic tasks such as data entry. The screens were small and unreadable under direct sunlight, and they often stopped working if they were exposed to excessive rain, extreme heat, or dropped onto a hard surface. This was a time before flash memory, so all the data had to be stored on the device until the user could return to his workplace and download everything they needed to the host system. The battery capacity was inadequate and often died out midday leaving its users exposed to the risk of losing important data when the battery ran out. For several years, most of the device models remained unchanged.

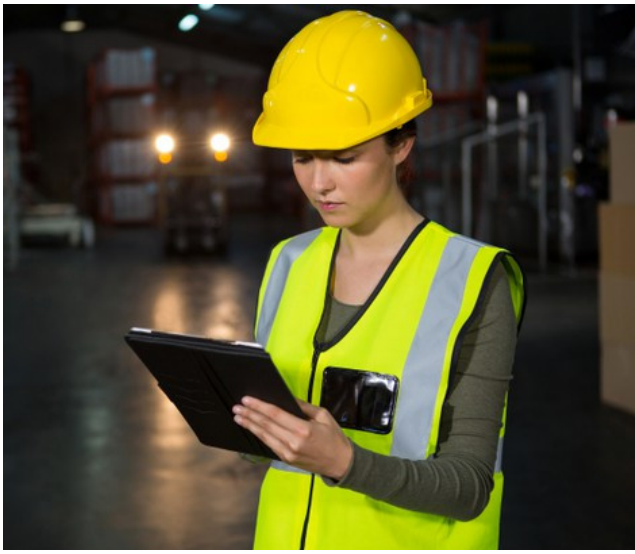
This was a problem, especially for people working in a time sensitive and mission critical line of work such as the military and healthcare.



Toughening up the rugged devices

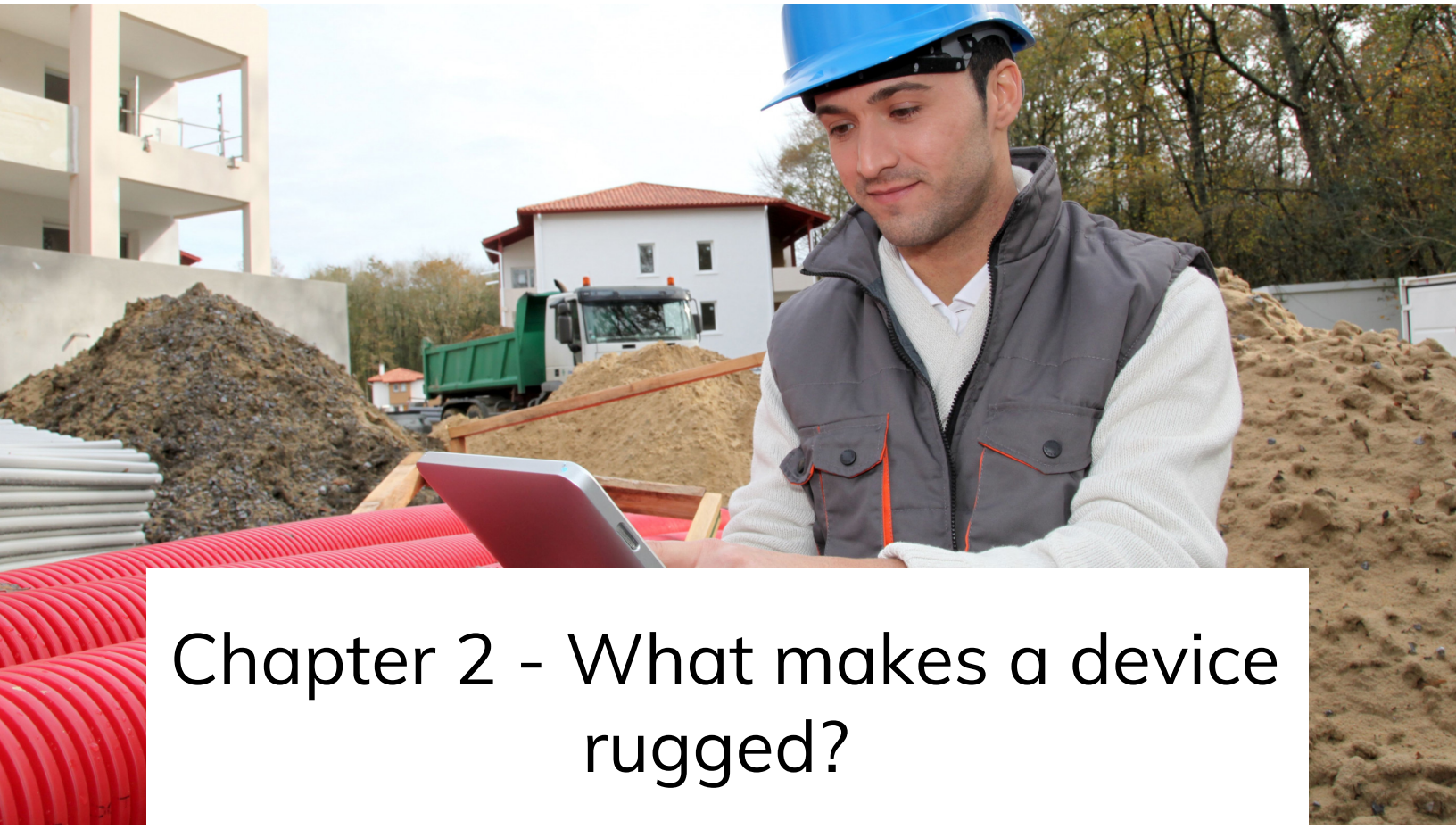
Keeping these aforementioned limitations in mind, many key players in the manufacturing industry stepped in to develop rugged devices that could:

- Withstand the harshest of the weather and environmental conditions.
- Transmit necessary data over the air.
- Extend the battery life for over 30 hours and more.
- Have an ergonomic design.
- Have bigger and better visibility screens.
- Have various integrations such as GPS, RFID, barcode readers, voice recorders, and cameras.
- Have integrated industrial-grade miniature scan engines.
- Have capacitive multi-touch capabilities.



As the demand for improving the ruggedness of the device kept on increasing, new dustproof, waterproof, shockproof, and shatterproof devices were added that could efficiently operate in temperatures anywhere from –20℃ to +49℃. Rather than giving importance to their fancy looks and consumer specific features, it was their ruggedness and convenience to be operated in harsh ambients that were always emphasized. Instead of making the devices totally rock solid, they are becoming increasingly lightweight and easy to carry around.

With the rise of SaaS in the past couple of years, many businesses have now begun using device management solutions to manage rugged devices and deploy essential applications to their users.



Chapter 2 - What makes a device rugged?

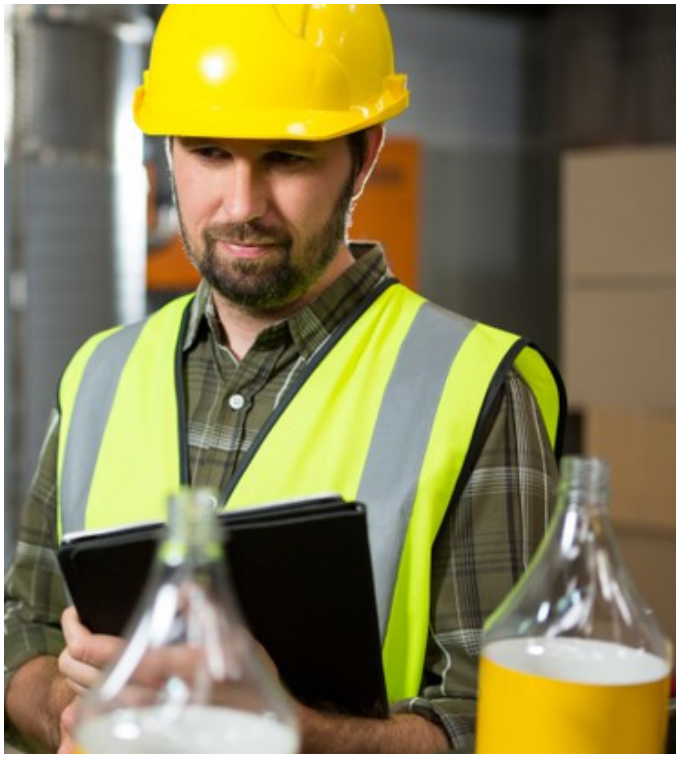
Rugged devices are meant to be used anywhere. Due to their constant exposure to a number of outdoor conditions, they are also designed to be immune to shocks and drops. Before the devices are considered rugged, they are subjected to multiple tests such as the MIL–STD tests and the Ingress Protection (IP) scale.

MIL–STD-810:

This is a US military standard that tests whether commercial devices can efficiently operate under various environmental conditions during their lifetimes, such as low pressure, exposure to high and low temperatures, temperature shock, random vibration, rain, humidity, fungus, salt fog, sand and dust exposure, explosive atmosphere, leakage, acceleration, and gunfire vibration. The initial intent of introducing this series of tests was to simulate an environment with the same level of stress the device will have to hold up to during their operation period. However, over the years, these initial sets of tests were revised multiple times.

Some of the test methods in MIL-STD-810 include:

- Test Method 500.6 Low Pressure – Altitude
- Test Method 501.6 High Temperature
- Test Method 502.6 Low Temperature
- Test Method 503.6 Temperature Shock
- Test Method 506.6 Rain
- Test Method 507.6 Humidity
- Test Method 508.7 Fungus
- Test Method 509.6 Salt Fog
- Test Method 510.6 Sand and Dust
- Test Method 511.6 Explosive Atmosphere
- Test Method 512.6 Immersion
- Test Method 513.7 Acceleration
- Test Method 514.7 Vibration
- Test Method 514.7 Vibration
- Test Method 519.7 Gunfire Shock



Ingress Progression (IP) Scale:

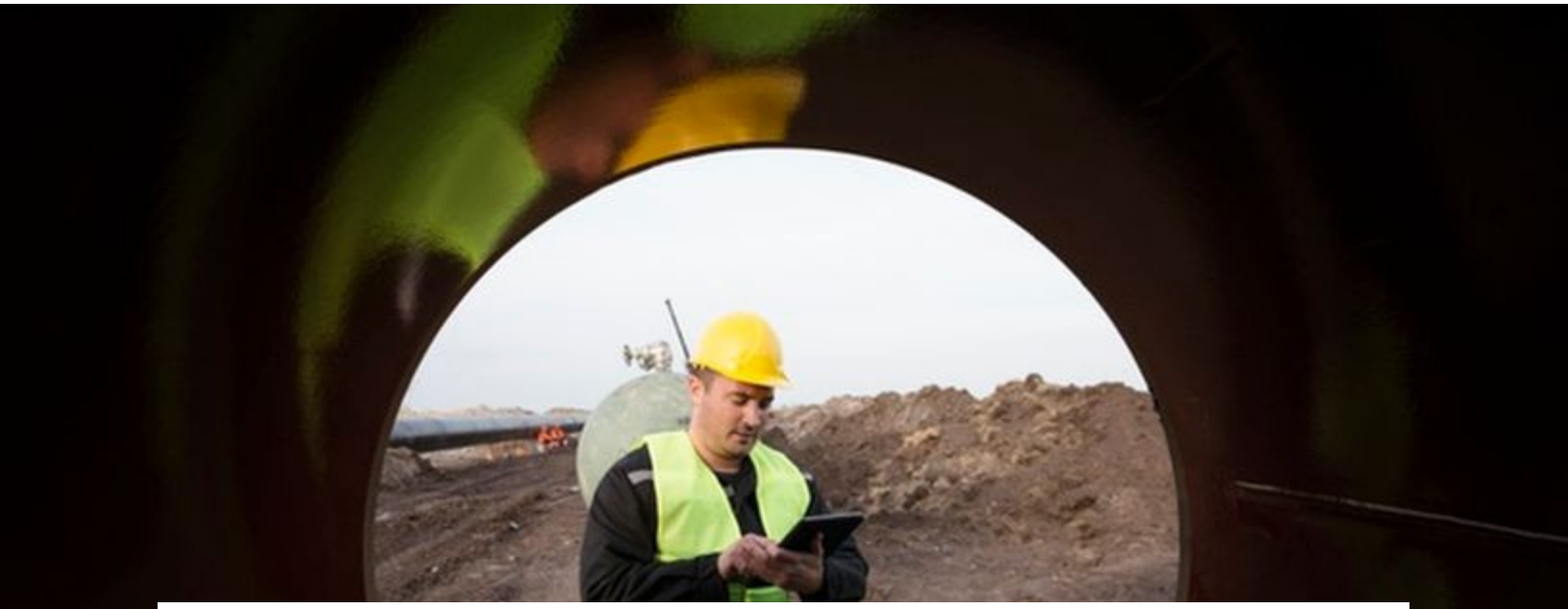
IP ratings define the sealing effectiveness of the devices against intrusion from any solid particles such as dust, dirt, and liquids like moisture from any sprays, drips, or submersion. There is a board called the International Electrotechnical Commission that actually defines and publishes standards for ingress protection. All the ratings will be in the form of a two-digit number of which the first digit shows the protection level against solid particles, with the second digit showing the protection level against liquids. For example, a device rated IP24 will have a protection level of 2 for solids and 4 for liquids. Thus, the device will be adequately protected from objects greater than 12 millimeters, and it can withstand water spray from any direction. A device with a scale of IP08, on the other hand, will have no protection from solids but can stay protected from long term immersion up to a specified pressure. That is, in short, the device will be having high resistance to that particular kind of ingress if the number showing that ingress is high.

IP Rating Chart

First digit	Degree of protection against solid objects
0	No protection
1	Protected against solid objects over 50 mm
2	Protected against solid objects over 12 mm
3	Protected against solid objects over 2.5 mm
4	Protected against solid objects over 1 mm
5	Protected against dust
6	Totally protected against dust

Second digit	Degree of protection against water
0	No protection
1	Protected against vertically falling drops of water or condensation
2	Protected against direct sprays of water up to 15 degree from vertical
3	Protected against sprays of water up to 60 degree from vertical
4	Protected against water splashed from any direction
5	Protected against low pressure jets of water from any direction
6	Protected against strong jets of water from any direction
7	Protected against complete continuous submersion in water
8	Protected against complete continuous submersion in water

The knowledge of IP ratings for rugged devices is very helpful in deciding whether the rugged devices are worth their cost. If the device is certified to be tolerant and durable, the businesses will be willing to spend on them even if they are a little costly. There are many other tests like torture test, bowling or tumbling test, and so on to check the ruggedness of devices. All the specifications mentioned above are handy benchmarks to decide on rugged devices, but a truly rugged device should be usable in any working condition the business need to use them. Even if a device passes industrial durability standards, it is not sure that they are truly equipped to handle the real-life working scenarios. Many factors like device material that won't wear and tear over time, highly viewable displays, rugged connectors and swappable batteries, and many other things have their part in toughening the rugged device.



Chapter 3 – Growth of Rugged Devices

One of the key factors that widened the gap between rugged and consumer devices is their purchase price. Due to their unique design and protective features, rugged devices often cost more than their consumer counterparts, but the return on investment quickly pays-off. And, even when we consider the total cost of ownership, ruggedized devices have proven to be the real winner as they are reliable and durable. To add, the advent of many new technologies has further made rugged gadgets much affordable for most industrial verticals, and this paved the way for the rapid adoption of rugged devices for industrial use cases. And now, ruggedized handheld devices are used almost everywhere, by warehouse workers, healthcare professionals, delivery personnel, emergency responders, and most frontline workers.

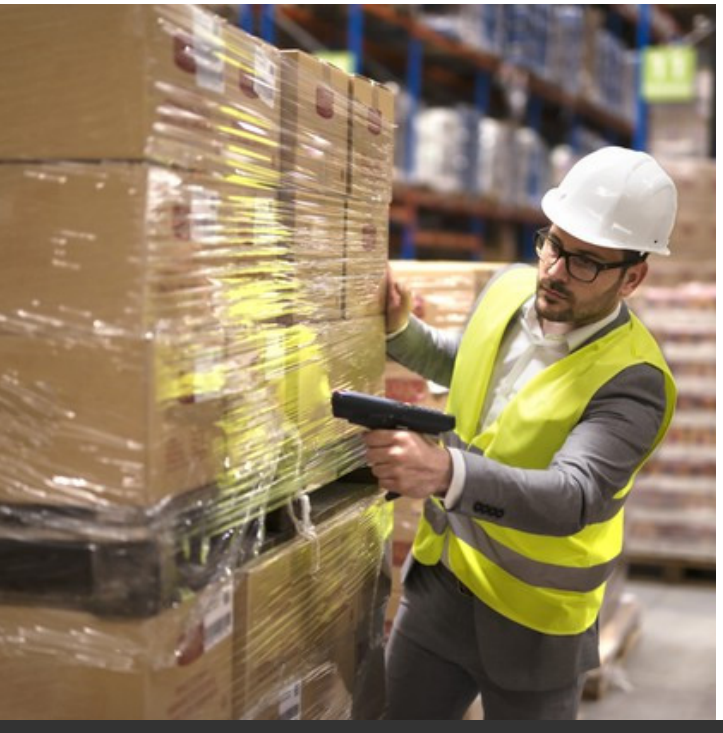
Initially, most of the rugged devices were running on a version of the Windows Embedded operating system, but later, there was a shift to other popular platforms like Android OS. However, with the ever-evolving technological landscape and newly arriving operating systems, customer demand and market pressure are high, and vendors are always forced to find new innovative varieties of rugged devices.

The different kinds of Rugged Devices

This was a problem, especially for people working in a time sensitive and mission critical line of work such as the military and healthcare.

Classification based on hardware

- Rugged Mobile computers - Mobile computers are used in many businesses to increase the productivity of their workforce. Unlike consumer mobile computers, a rugged mobile computer is designed to operate efficiently in extreme temperatures, resist vibration and shock. They come with enhanced battery life, more durability, more security and enhanced outdoor display.
- Rugged tablets - Consumer tablets work best for personal use and simple enterprise operations such as checking the work mail and using various enterprise deployed applications. Rugged tablets, on the other hand, are primarily used in adverse working conditions, and those environments need a durable design and reliable features from a tablet PC. They are mostly used by field workers and service technicians. Some of the conditions that rugged tablets are designed to withstand include – Extreme high and low temperature, vibrations, shock, dust, harsh sunlight, high humidity, and any drops to hard surfaces.



- Reader/scanner - Ruggedized bar code readers and scanners are perfect for warehouse employees and other field workers who are often required to work outside. Their hardened exterior and capability to withstand a number of environmental conditions make it easier for warehouse employees to track the inventory, properly manage the assets, and package delivery.

Classification based on the level of ruggedness

- Semi-rugged - Semi-rugged devices typically come with minimal rugged features and are regarded as commercial off-the-shelf devices. There is a high probability that only some parts of such devices have undergone actual stress testing and are hence less reliable for harsh environments. If these devices are subjected to extreme environmental conditions, they could experience a significant drop in performance or even stop being functional.
- Fully-rugged - Fully-rugged devices with their more enhanced capabilities are used in more risk-prone environmental conditions. They are usually used by the military and by other professionals who spend much of their working outdoors. According to the level of tolerance they have been certified for, fully rugged devices can be exposed to any intensity of temperature, pressure, humidity, rain, direct sunlight for any amount of time. They can be dropped or stressed without diminishing their performance level. Due to their prolonged durability, they are preferred by many professionals for mission critical applications that require continuous operation.
- Ultra-rugged - Ultra-rugged devices are pretty much the same as fully-rugged devices. The only difference that lies between the two is that ultra-rugged devices are more durable and come with more enhanced capabilities to stand additional stresses. They can even survive being submerged under water because it's fanless, sealed, and conformal coated. They are more expensive than fully-rugged devices.

Classification based on consumer characteristics on rugged smartphones

- Consumer rugged smartphones: They are consumer-oriented devices with characteristics of a conventional smartphone. Such smartphones typically have an IP rating of 68 and MIL_STD-810G standard. They are relatively cheap. Major vendors issuing this type of rugged smartphones include Kyocera, Samsung, RugGear, Crosscall, etc.
- Ultra-rugged smartphones: They are industrial oriented devices with few consumer characteristics and specifically designed to survive extreme rugged testing. These devices are considered relatively expensive and are typically used only in hazardous environments. Major vendors issuing such rugged smartphones include Motorola Solutions, Sonim, Bartec Pixavi, etc.

The different operating systems on rugged devices

Windows and Android are the two popular platforms most rugged device comes with. Both have their own benefits regarding the rugged place that makes the “Windows or Android OS?” a tough choice. Still, these two are the leading operating systems for rugged devices along with some other minor contributors, and there are some important aspects of mobile operating systems that may make them suitable for rugged applications.

Windows

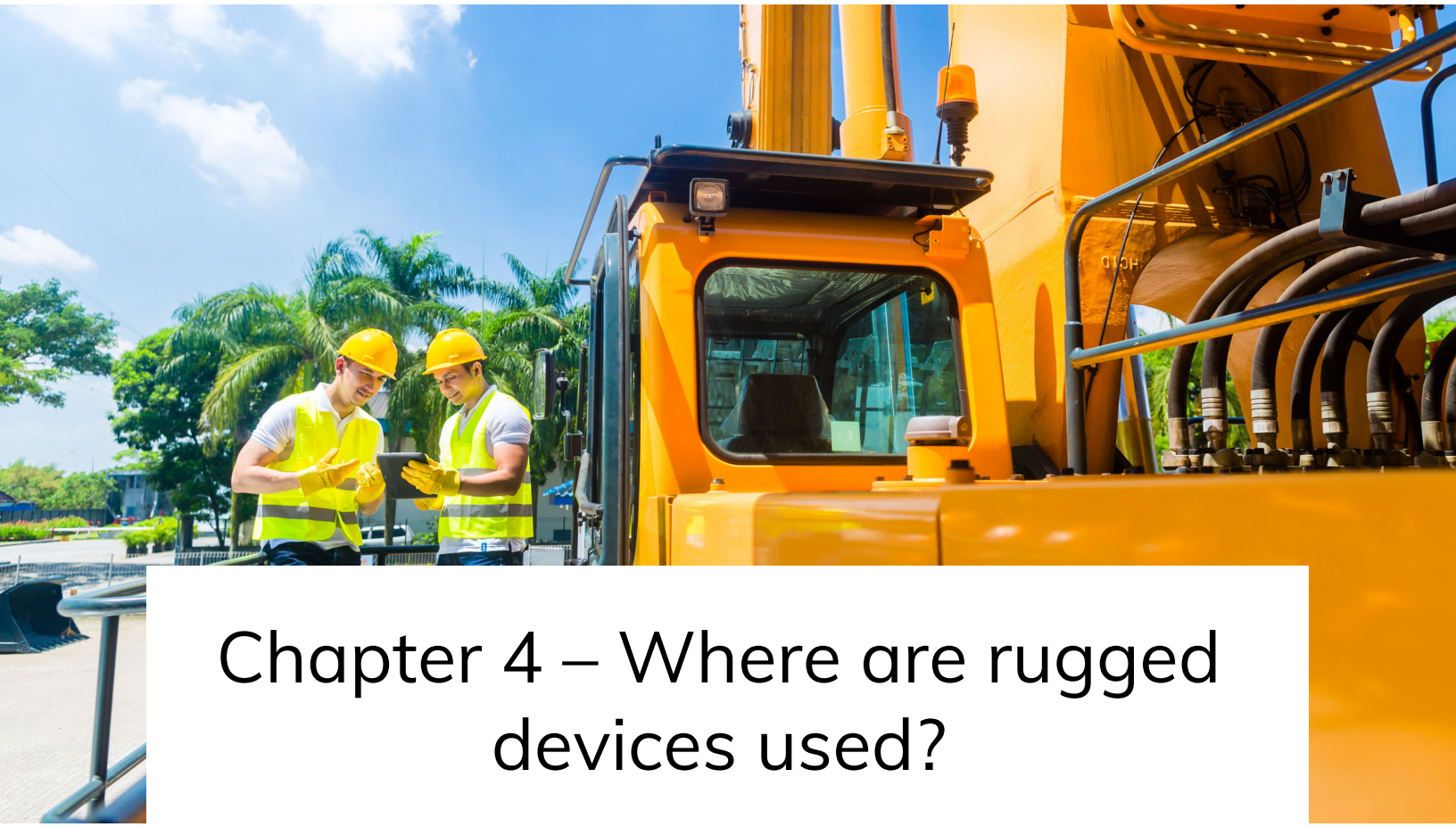
Being a veteran of operating systems, Windows devices have been there for rugged applications a couple of decades prior to other platforms and hence considered as the legacy operating system for rugged devices. When it comes to device features, Windows devices tend to have higher memory as well as computing power and are good to handle lots of data. This is indeed a benefit, but on the other hand, a large memory is connected with extra power usage, which in effect drains the battery more quickly. So, in terms of battery durability, they are not an excellent option to make. Another essential thing to consider is the ability of Windows devices to connect with peripherals.

Android OS

Android-powered devices have gained ground quickly in the rugged market. The most important upside of this operating system is certainly its familiarity, so users will be most comfortable using them for work purposes. One drawback that comes coupled to this familiarity is that if the companies don’t lock these devices with an MDM solution, the employees are more likely to get into device settings and alter things they shouldn’t be doing effortlessly than any other OS platforms. Android devices have lower computing power and onboard storage as compared to a Windows device. But they have better battery life and hence are more durable. As the platform is open source, a greater level of customizations can be done on Android devices.

iOS

Apart from Windows and Android OS, iOS is a prominent operating system that tends to be used for rugged applications. Though there are no popular rugged devices, iOS devices are used with protective covers or cases for some applications, but they are never a good fit for intense use cases in harsh environments.



Chapter 4 – Where are rugged devices used?

There is a sizable niche of businesses looking for devices that are tougher, optimized for outdoor use, and fit for their work purposes. With a set of successful vendors in the space, the rugged device market has a significant growth trajectory driven by a number of interlinked factors like their durability, drop proofing, proper water and dust proofing, extended battery performance, effective power management, and thick tempered glass protection.

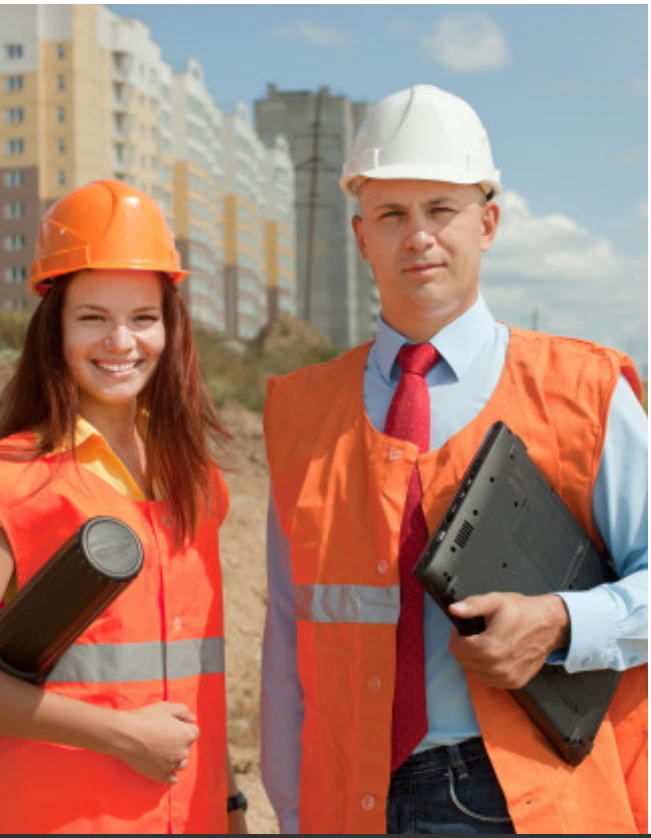
Leading rugged device manufacturers provide relevant features that improve their robustness and suitability to hold out against many critical enterprise scenarios.

Benefits of using Rugged Devices

- They are durable and can withstand a number of harsh environmental conditions. They are made to last.
- In addition to having a user-friendly design, with the advancement of screen technologies, rugged devices can provide clarity in any outdoor conditions.

- They are increasingly becoming lightweight and are shatterproof.
- They have a prolonged battery life, have a better ROI, and contribute significantly to improving employee productivity compared to consumer devices.
- With the help of an MDM/UEM solution, rugged devices can be quickly enrolled.
- They enable frontline communication even in the most extreme of environments and hard-to-reach locations.
- They can extend for up to many years without having a mandatory software update.
- They are highly tolerant of faults and hence reliable.
- They have integrated many functionalities and built-in support for many peripheral features purpose-built for enterprise operations. This makes them suitable for multiple industrial use cases.
- They have minimal failure rates causing no costly downtimes and therefore ensure increased worker productivity.
- They are becoming more or less consumerized by incorporating new and appropriate technologies that will entice new customers.
- They support input with wet fingers and gloved finger touch input.
- The customer focus of the rugged market is narrower, which allows vendors to invest in delivering new and improved features relevant to their target users.

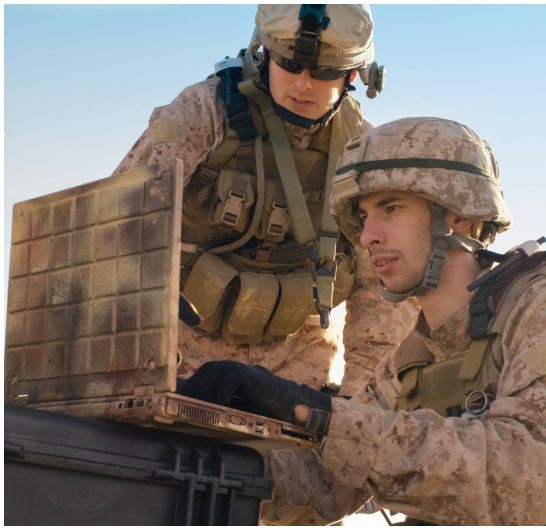
Use case of rugged devices across multiple industries



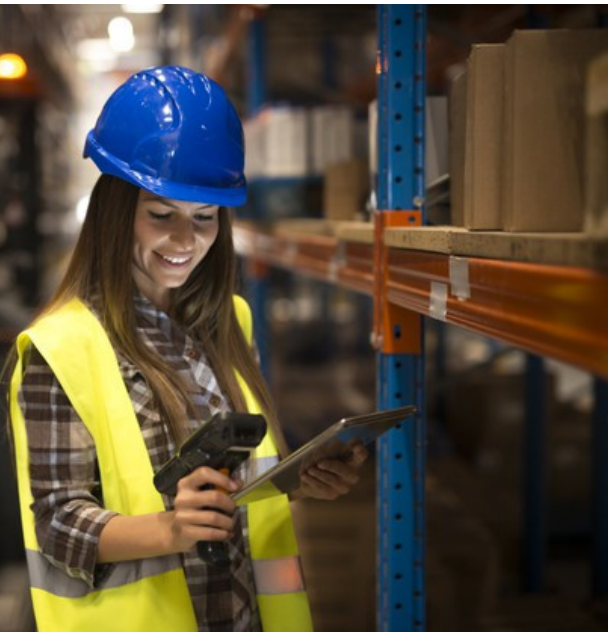
Construction

The construction industry, like many other industries, needs work devices that are durable, secure, and rugged. Construction workers are one of the field workers who have to work in some of the harshest working conditions. They need devices that can withstand dirt, dust, drops, shock, and extreme weather like cold, humidity, and temperature. Water-proofing is essential to prevent the ingress of water or other liquid into the devices. Most rugged devices have features that not only survive water exposure but also work without failure in wet conditions, keeping the workers always connected and productive.

Military



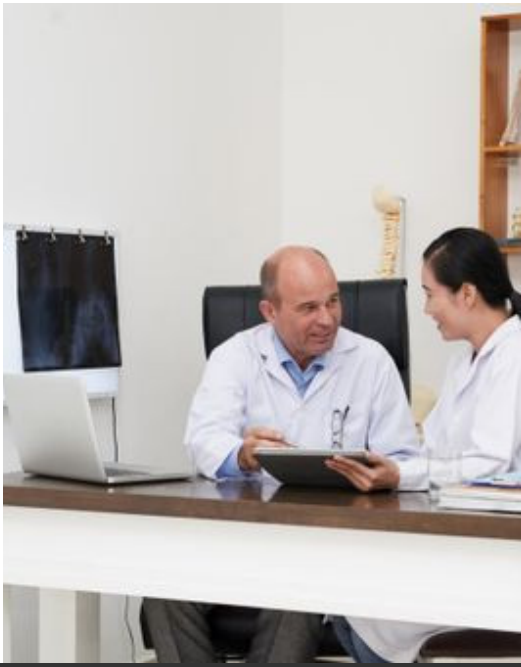
Military officials must remain productive irrespective of the weather and environmental conditions they have to work at. They need purpose-built mission critical devices to handle extreme conditions and heavy usage. For all use cases, including mission planning, communication, supply chain, and logistics operations, alert and awareness, fight-line maintenance, command, and control, downtime, malfunctioning, or failure of any technology can cost a life. And hence, military-grade rugged devices that can survive harsh and hostile conditions are a must for their operations.



Logistics

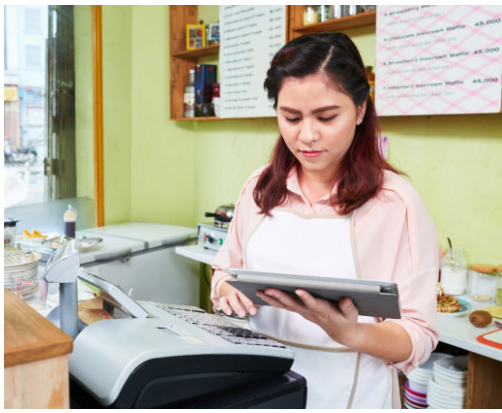
For logistics and supply chain management services, rugged mobile devices have their own roles in the distribution of consumer packaged and industrial packaged goods. Most rugged devices have in-built RFID and barcode scanning capabilities required during the shipping and delivery of goods. They also provide PDA driven inventory management capabilities to manage stocks, record physical inventories, track inventory in transit and during loading and unloading to know their exact location. Most of these applications require ruggedized devices that could be carried around with minimal wear and tear.

Healthcare



Healthcare employees need devices that can adapt and evolve with them in any conditions to save a life. Especially in the healthcare sector, where everything is fast-paced, and anything like shocks, drops, vibrations, dust, and temperature variations are inevitable, the use of devices that can withstand physically is important. Rugged devices support health specific applications for different functions helpful for health companies. Mobile imaging feature helps give quicker access to medical images like x-rays and ultrasounds that are important in the diagnosis process.

Retail



High speed connectivity, along with barcode and RFID scanning capabilities and credit card readers are all vital for the retail industry to reach up to customer expectations. In fields like stores, restaurants, vending management, rugged devices have their application as mobile POS, inventory tracking, promotion tracking, store operations, account management, staff management, and line busting solutions.

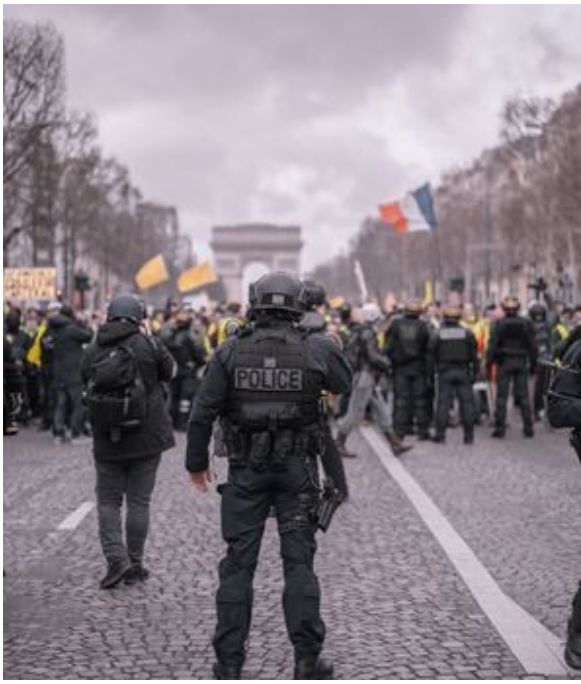
Mining

Mining is an industrial sector where nothing entering the environment will come out of the scene without scratches or dents, and the industry is going rough and tough as always. The industry requires exceptionally sturdy technology for tasks like GIS mapping, workforce automation, geotagging, proof of service, equipment maintenance, communication, machine guidance, dispatch, data collection, work order management, asset management, shipping and receiving, resource optimization, and reporting. All the workers have to encounter challenging environments involving hard surfaces, variable weather conditions, airborne dust and dirt, and vibrating spaces. Rugged devices, with their toughened nature, provide tailored and fit-for-purpose features for mining operations.

Manufacturing

Rugged devices are incredibly handy in every stage of manufacturing. This industry can leverage exceptional benefits from rugged devices as most of the functions have a great deal of extremities like vibrations and temperature variations to be faced. The devices have to maintain their working conditions and be efficient all the time. There are specific applications and extensions that work fine on rugged devices for quality control, inventory management, and other important functionalities. To add, the impressive battery life of rugged devices makes them ideal for working entirely along the multiple shift hours, minimizing employee downtime.

Public safety

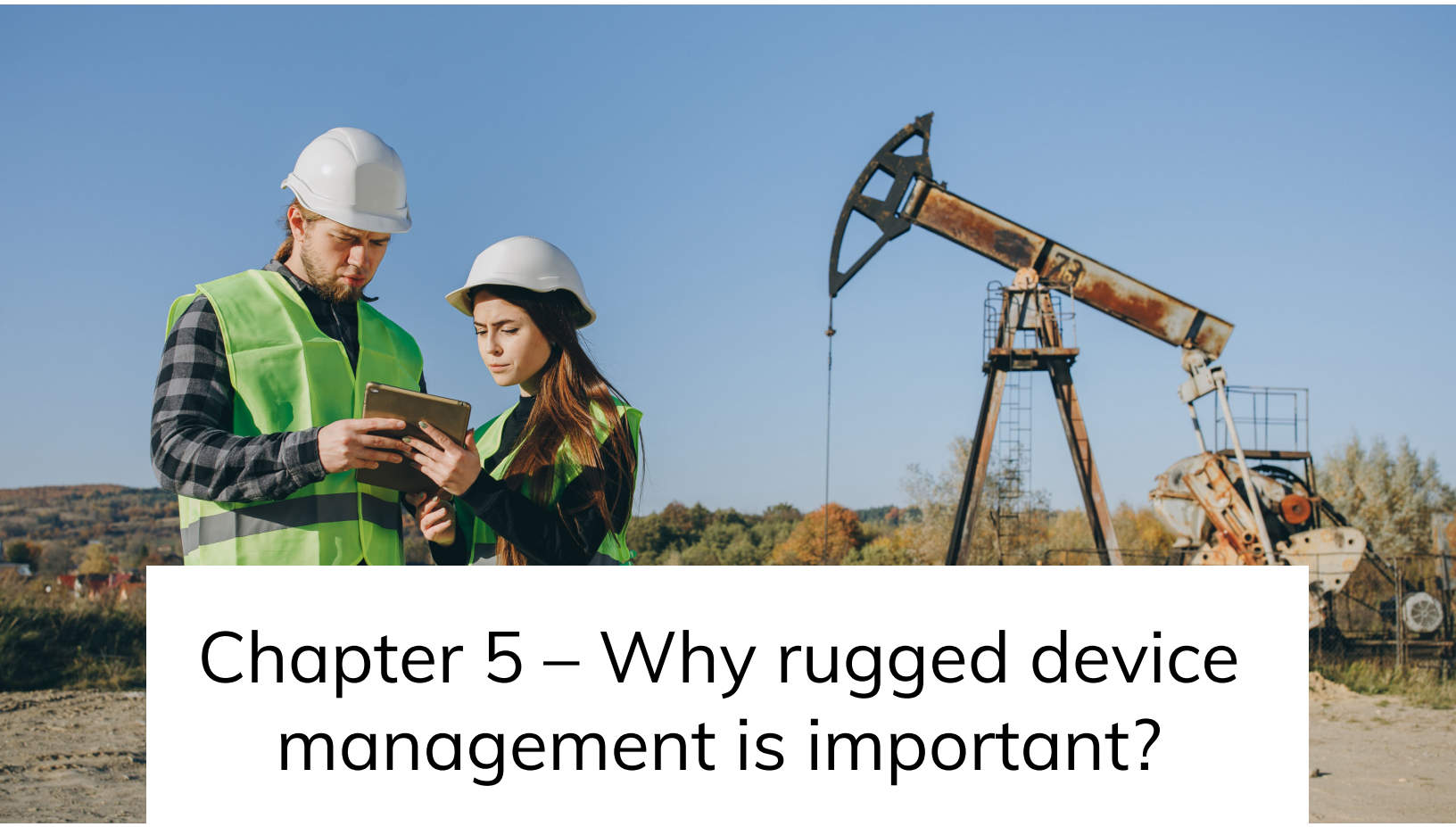


For public safety officials like the police or first responders, real-time communication is quite important, but the device failure rate is high for these use cases. Devices, in this case, are to be interchangeably work in indoor and outdoor environments. In all these environments, drops, wear and tear, everything is inevitable factors, and to add, there is an increased likelihood for everything to encounter extreme situations. Device failures during public safety services mean that an official has no access to important electronically stored data to complete critical tasks and hence is not tolerable. They need powerful, reliable, flexible, robust, and toughened devices in almost all cases.

Popular rugged device vendors

Many vendors come with field-oriented and substantial devices built to be durable and can be used in the place of regular consumer phones as well. They feature excellent wireless connectivity and promising processing power for optimum productivity. Most of the leading manufacturer of high performing data collection hardware like rugged mobile devices and barcode scanners offer advanced asset management solutions for most industrial verticals. Leading rugged device vendors among many others include:

- Zebra Technologies
- Datalogic
- Getac
- Honeywell International
- Panasonic
- Kyocera
- Sonim
- Bullitt
- Urovo
- Bluebird
- Spectralink
- Amrel
- Dell
- Lenovo
- Samsung



Chapter 5 – Why rugged device management is important?

Rugged devices are designed to provide a great user experience in spite of the rougher treatments, hard knocks, long drops, temperature variations, dust and all other adversities. It's a true case that in order to ensure that they can survive the extremities of what they can be put through, during the test, they will be put through rigorous conditions. But still, there are many ways they can leave businesses inconvenienced and out of pocket while on the premises or on the road.

Challenges faced by organizations going for rugged devices

- From micro and small organizations to large scale organizations, employee owned rugged consumer devices are entering as BYOD or personally liable devices. Most organizations allow BYOD wherein employees purchase their own choice of the rugged handset with the assumption that they work well at work. But the most vexing issue with the personal decision of what device to invest in is the security concerns following it. As the users are having device ownership, they are free to use those devices in their own ways even at work, and this can pose serious security threats to potential data and inadvertently attack corporate resources.
- Keeping pace with the rapid evolution of devices and a whole host of new

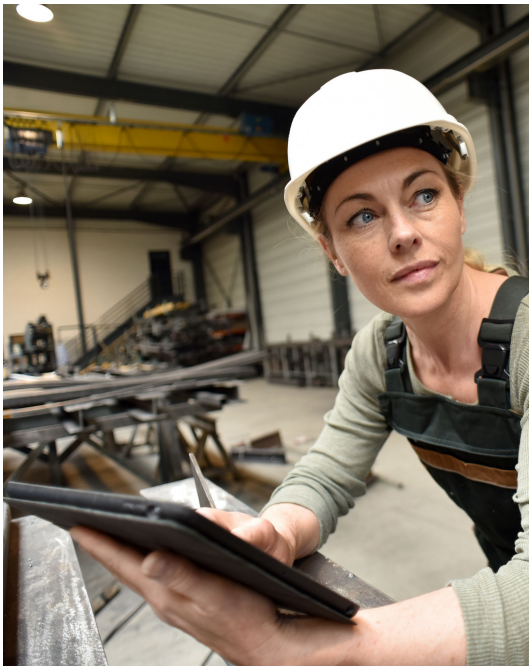
products and providers in the rugged sector and ensuring rigorous identity and access management is not a unique challenge to organizations handling rugged devices. Still, this can be met only by a solution with a complete set of management capabilities.

- The ever-changing combination of configurations, features, carriers, and devices having different form factors add to the management complexities and lead to a frustrating IT team.
- App management is another critical issue. Rugged devices need particular applications for work specific purposes like RFID scanning, and distributing these apps across multiple device types is a challenging task. The IT has to find resources to tailor apps to specific business processes and make sure that all the apps do necessarily function well on all devices.
- Configuring and securing wireless networks to tolerate critical business workloads and managing bandwidth consumption is something beyond the capacity constraints of legacy business systems.
- Without proper management, it is challenging to keep up with the compliance standards, stay fine tuned, and up to date with critical security updates, fixes and patches recommended by manufacturers.

A holistic approach to rugged device management

Adopting a unified endpoint management solution is the main way of mitigating most of the risks associated with rugged device management. UEM solutions are purpose-built to monitor endpoints, provide role-based access functionality, manage software distributions, blacklist unwanted services, enforce security policies and provide mobile threat defense capabilities in a consistent manner, and find more ways to keep the workers productive. Most popular vendors like Google have their own offerings for managing ruggedized devices, and an efficient UEM solution should walk hand in hand with such offerings to maximize data protection, standardize endpoint management, and enhance worker productivity.

Hexnode UEM can secure and manage rugged devices across industrial verticals. Hexnode helps you create a management strategy from the ground up or provides a solid foundation to optimize your existing working environment. Along with basic security features like password enforcement, remote wipe, lock, view, and control, Hexnode provides options to restrict device features, lockdown devices to kiosk mode,



manage OS updates, set encryption policies, distribute apps, enroll devices in bulk, configure Wi-Fi, email accounts, VPNs, and install certificates. It works well with most of the leading rugged device vendors and extends specialized management features for rugged devices in association with Android Enterprise and OEMConfig support offered by manufacturers like Zebra, Honeywell, Datalogic, Seuic, Bluebird, Cipherlab, Point mobile, Unitech, Spectralink, Samsung, and Kyocera. The basic essence of Hexnode UEM is that it is capable of turning any kind of device, sometimes a new device, off the shell into a work-ready gadget without the need to alter it, fully image it, or connect it to the enterprise network manually. All that required is a simple configuration process.

Android Enterprise and OEMConfig

Android Enterprise has included several features over time that are tailor made to add Android-based rugged devices to enterprises for handling critical tasks. To accommodate dual work and personal usage without affecting work data, Android Enterprise has a set of controls specific to BYOD devices. All these controls can be pushed to rugged devices with the help of UEM to make those devices ideal for people working outside the office, in extreme locations, or in busy environments.
Android Enterprise lays only a basic set of management APIs, and OEMs are free to build on top of that to develop enterprise management strategies of their own if desired. UEMs normally take the APIs offered by device manufacturers and build them into their platforms in order to manage devices. But this is a complex process, and OEMConfig is a quick attempt to get all the management features that device vendors offer without the need to actually integrate them into the UEM platform. Especially in the case of rugged devices having all the latest controls and security features is at most important, and the OEMConfig is targeted explicitly towards rugged devices. OEMConfig fixes all the flaws with zero-day support to all the new features and functionalities, and this is how it works:

- OEMs develop their own OEMConfig application and publish them on Google Play.
- Organizations approved and add the OEMConfig app onto their devices via their UEM solution.
- OEMs develop relevant APIs over and above Android Enterprise.
- Once a new feature comes, organizations immediately get support for the feature via the OEMConfig app using managed app configurations.

- The new feature gets automatically supported on all the devices on which the OEMConfig app has already been added.

Given below are the OEMs for which Hexnode have support for OEMConfig:

Vendor	Application Name
Samsung	Knox Service Plugin
Zebra	Zebra OEMConfig powered by MX
Honeywell	Honeywell OEM config
Lenovo	Lenovo OEMConfig
Datalogic	Datalogic OEMConfig
Kyocera	Device Config Plugin
Unitech	Unitech OEMConfig
CipherLab	CipherLab OEMConfig
Seuic	Seuic OEMConfig
Spectralink	Spectralink Device Settings

Android Enterprise Recommended for rugged devices

Android Enterprise Recommended is Google's validation program to find and confidently deploy quality devices to be used for enterprise cases. Devices submitted for certification goes through thorough examinations in terms of hardware specifications, support for bulk or zero touch deployment, consistent application experience, availability of unlocked devices, IP64 certification for rugged devices and delivery of Android security updates within 90 days of release for a minimum of 5 years in the case of rugged devices.

Android Enterprise Recommended defines a separate device category for rugged devices to be worked in harsh environments with a standard set of specifications including hardware, software, deployment options, update specifications along with drop testing and ingress protection. All the standardized features defined by Android Enterprise Recommended let IT manage rugged devices seamlessly.

Mitsogo Inc., Unites States (HQ), 111 Pine St #1225,
San Fransisco, CA 94111
Tel: Intl +1-415-636-7555, Fax: Intl +1-415-646-4151