Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport DDPS
armasuisse
Science and Technology

Mission Critical
TECHNOLOGY OR METHODOLOGY?

An introduction to Mission Critical Thinking

armasuisse Science and Technologies
Feuerwerkerstrasse 39
CH-3602 Thun

Contact :
Dr. Quentin Ladetto | quentin.ladetto@ar.admin.ch
Mr. Olivier Desjeux | olivier.desjeux@advancedvalueglobal.com

April 2024

deftech.ch | armasuisse.ch

Dear Reader,

This document was written for all of those, who, for any good or bad reason could not participate to the 29th Deftech-Day on April 16th 2024 entitled: Mission Critical – Technology or Methodology? For those who had the pleasure to witness the day, I'm confident that these pages, authored by Mr. Olivier Desjeux, together with whom we organized the event, will bring back good memories of the learning experience!

In former days, *Mission Critical* was a terminology assigned to a product. The design, the production and maintenance of the product was done in such a way as to ensure the product could provide its full capability within the boundaries of its scope.

Nowadays, this statement is still valid. However, the battlefield has become a complex architecture of interoperable Mission Critical systems running Artificial Intelligence, sourced from different vendors. The **difficulty to maintain** Mission Critical systems becomes very challenging.

While Mission Critical systems seem to remain a mandatory technological requirement, the recent conflicts have demonstrated how the usage of **non Mission Critical** items can strongly disrupt the course of operations.

Independently of the application, we hope that this document will enable you to anticipate the future of Mission Critical systems and provide the most suitable and reliable solution for the mission.

We wish you a stimulating read.

Dr. Quentin Ladetto
Head of Technology Foresight

If you are reading from a printed a version and you would like to directly access the html sources, the PDF version of this document is available at this address – https://deftech.ch/mission-critical

Mission Critical, Technology or Methodology

An introduction to Mission Critical Thinking

Keywords: Mission Critical Solutions, software, real-time, assessment, telecom, aerospace, data, space, command, control, communications, computers, intelligence, surveillance, reconnaissance, cyber-defence, combat-systems, observation, orientation, decision, action, electronic, safety, life, impact, product, system, procurement, defence, failure, disruption, activity, IT, edge-computing, operation, technology, methodology, rules, standards.

Purpose

The purpose of this booklet is to trigger reflective thoughts on the Futurs of Mission-Critical thinking within the defence context.

This terminology has been, and is still commonly used as a principal characteristic of a highly sophisticated product or service. Is Mission-Critical necessarily related to high-tech sophistication or is it time to adopt a lean methodology and look out for alternatives?

The era of increasingly fast generation of diversified threats is here, including:

- The rising threat of natural disasters caused by the global warming expands the possibility to face unexpected dramatic situations.
- Ten of the world's deadliest attacks happened after September 11th, 2001 [1]. Disruptive and frighteningly efficient operating modes were used to maximize the impact of the disaster occurred.
- Today's fraught global dynamics, the geopolitics risk is now climbing to an unprecedented level since the end of the cold war. Weaknesses in national security, resulting from a very long quiet peaceful context, are being exposed now that war is next door.
- Other threats including social network and cyber intrusion attacks have the power to break the civil society's psychological cohesion.

The drivers of those categories, i.e. the dynamics of threats evolutions, are on the way. They are shaped, purposely or not, to chop-off some portions of the common resilience, and do certainly not share commonly agreed concepts of warfare.

During the Viet-Nam war, Henry Kissinger observed that "*the guerilla wins if he does not lose. The conventional army loses if it does not win.*"

Anticipating, preparing a mission responding to potential disasters requires, more than ever, quick agility and adaptability, sometimes in contradiction with strict traditional procurement requirements.

Applying the right balance of technology in combination with a carefully thought methodology is required to keep control of the situation. Preparing for the next challenge with the right balance of mission-critical thinking is crucial in every aspect of defence contingencies as well as within the civil society.

Within the context of the Deftech-Days of armasuisse, this publication results from numerous discussions held with mission-critical stakeholders. It looks towards the future and what innovation is developing to drive control efficiently.

While dead angles of the technology race leave unforeseen vulnerabilities wide open, thinking in a creative way about what it takes to operate Mission-Critical operations is more than essential for the preservation of our futurs.

Olivier Desjeux, April 2024

Contents

Background and Definition

The common ground between telecommunication networks, medical monitoring unit, search and rescue, personal locator beacon, gas leakage detection system or aircraft's navigation unit is a Mission-Critical procurement, design and execution. The way to engineer the criticality is obviously fairly different for all of the above examples, driven by unrelated physical concerns. However, they all require at least an extraordinary amount of integrity and reliability to operate within reasonable safety margins, to avoid failure with fatal consequences. Vendors usually put their specific definition in the context of utilization of the product or system advertised, ranging from individual products, all the way to vast complex interoperable systems.

Mission-Critical doesn't follow any formal lexical definition. Despite a lack of unified standardized specification, Mission-Critical has, and is still playing a significant role in the procurement of equipment from the defence sector. Most of the time, Mission-Critical, as a general guide, is part of a set of requirements composed of a very long list of standards, all required for formal compliance.

In relation to US DoD Information Technology System, an example of Mission-Critical requirement looks like: "*Mission-Critical information technology systems are necessary to continue warfighter operations and direct mission support of warfighter operations …*" [2].

A Mission-Critical product or system is one whose failure or disruption would cause an entire operation or activity to fail. It is a type of product or system that is part of a chain, mandatory to pursuing the success of operations [3]. It suggests a context of major adverse impact and real possibilities of individual or collective loss of life, serious injuries, or at a global scale, military, economic, political or social consequences to the nation. If the system fails or is interrupted, operations are dramatically impacted.

Consequently, Mission-Critical products or systems available on the market have undergone rigorous engineering processes, with extensive meticulous test and qualification, resulting in significant costs and time before commercial availability. They are "*Fit-For-Function*" ready to perfectly serve the purpose of their mission, within the context in which they have been specified.

In the current landscape, technology is at center stage in Mission-Critical environments. Cutting-edge technology-solutions have emerged as the backbone of interoperable systems, enabling rapid complex data analysis, unparalleled situational awareness and real-time decision-making.

This results from year longs of development and improvement, living together with challenging specification compliance for the procurement of such systems.

While technology is undeniably essential, methodologies are equally crucial for Mission-Critical success. Robust methodologies guide its implementation and operations, ensuring the products or systems perform reliably under extreme conditions. Methodologies rely on carefully crafted operational forward and depth maintenance and support, combined with logistics and adequate redundancy to ensure the required availability for the purpose of the mission.

If mission-criticality was certainly guiding the decisions since as long as humanity exists, its formalization finds its roots within the telecommunication sector. If the design of telecommunication networks was initially for civilian applications, its operation quickly became considered as mission-critical. This characteristic started guiding the topology and networking concepts, just before the turn of the twentieth century.

Since then, the defence sector started adopting mission-critical concepts. The earliest formalization is identified under US military authority. The Command and Control, acronym C2, focuses the efforts of entities (individuals and organizations), including information, toward the achievement of specific tasks, objectives, or goals.

Three major management areas have been defined: Information, Management and Decision.

Those three management areas carry the following four functions: Observation, Orientation, Decision and Action. (OODA loop cycle)

For Mission-Critical operations, the functions are embodied within six major characteristics, as represented in the chart below. [4] (Figure 1)

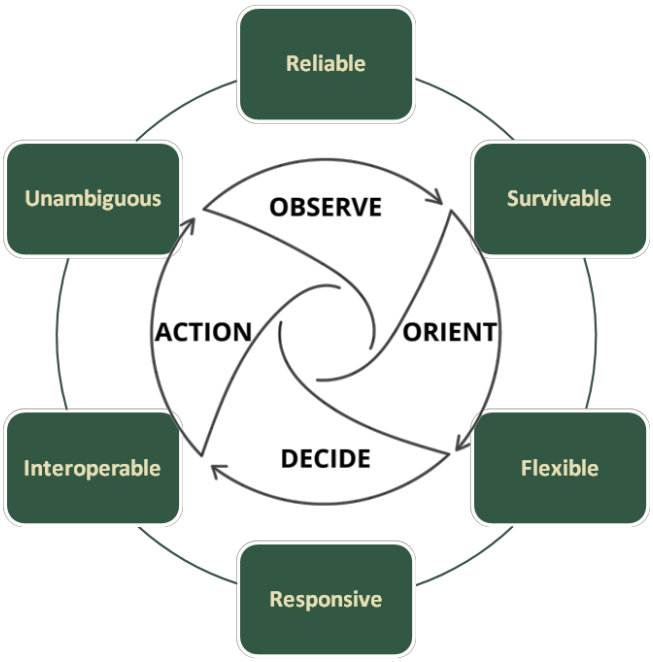

Figure 1 – The four functions of mission-critical command and control process guided by six essential characteristics

Since it was introduced in 1976 by the Colonel John R. Boyd*, the OODA loop has become a well-established blueprint for evolving decisions. **Technology**, **Human-Machine Interface**, and **Human Performance** contribute to the speed required to move through an OODA cycle, creating the differences between failure and success of the mission. If the "Responsive" characteristic is essential to win, none of the five other ones may be omitted during the Mission-Critical process cycle.

**Colonel John R. Boyd was an US Air Force pilot, flying the F86 Sabre during the Korea war. He wanted to know why F-86 fighter pilots often defeated MiG-15 fighter pilots in dogfights, even though the MiG-15 was an aerodynamically more maneuverable aircraft than the F-86. He observed that, what made a significant difference in the outcome was how quickly pilots could go through the OODA loop and move ahead. He concluded that the hydraulic flight control of the F-86 made the difference against the basic mechanical controls of the MIG-15.*

Before and Now

When considering the future, a good practice is to understand the origin, from where the concept comes from. The graph below is a very succinct representation of the evolution of Mission-Critical systems since World-War II. (Figure 2)

During World-War II, the technology was still in its infancy as compared to today. However, Mission-Critical operations were conducted. If none of them was considered as decisive, the outcome would have been different without them.

The example below shows a reconnaissance aircraft, a Spitfire from the Royal Air Force *(source: military-history.org)* fitted with a camera. Photo reconnaissance played a crucial role in both WW1 and WW2. In this case, the setting consisted of 3 cameras, 2 pointing vertically and one oblique on the port side.

The intelligence mission flown by the aviator was indeed critical. It was one of the ways to understand the opponent's troop positions and movements, for the purpose to forge sharp tactics.

The technology consisted of a chain of 3 elements, the aircraft, the cameras and the pilot. At that time, the telecommunication consisted of voice messages. The radio-communication was certainly part of the mission, but probably not on the critical path.

The methodology exposed during the briefing was pretty simple, something like: take-off during a day of clear sky, fly high to avoid the anti-aircraft artillery, but not too high to grab good enough pictures, activate the cameras, overfly the targets repeatedly and then make it safely and swiftly back home.

If any of the 3 elements of the chain would fail, the mission would be lost. A chain is as strong as its weakest element, so a lot of pressure was placed on each of them. There was presumably some redundancy with multiple aircrafts on the same mission, but I leave this point (interesting though) to the historians.

The Spitfire was introduced in the RAF just before WW2. It was designed as a short-range, high-performance interceptor aircraft. With a lower attrition rate and a higher victory-to-loss ratio than Hurricanes, it has been selected as the preferred selection for this type of mission.

A close look at the camera reveals its intention to be exposed to harsh missions, engineered and built purposely on top of past experience of previous missions. Both, the aircraft and the cameras were independently designed and produced in such a way as to avoid failure during severely exposed missions.

The third element of the chain was the pilot. An extremely solid track record, including acts of bravery must have been part of the selection. For the rest, he probably received a map of the area as main part of his briefing, concluded by a sincere and warm *Good Luck* salutation.

Several methods were used for data intelligence to construct a mental representation of the opposed forces. The air-reconnaissance was one of them. At that time, the difficulty was to interpret the information, with a different meaning of *real-time* than nowadays concept. With the rather long inertia of troop's movements, the validity of one single observation allowed combination from other sources to shape the picture of the opponent's strategy.

Figure 2 - From WW2 up to modern warfare systems

Since then, the electronic, telecommunication and overall digitization have been under careful scrutiny for Mission-Critical operations. The picture in the middle of the chart below, exhibits a typical piece of Mission-Critical

equipment, probably onboard computing, radar or telemetry unit. This unit could be one of the constructing elements of a complete Flight Information System, which in turn serves the interest of a complex Command, Control, Communications, Computers (C4ISR) system, becoming C5 while including also Cyber-Defence [4].

Increasingly complex, multilevel and cross-sector situations, requires a need for a more interdisciplinary and multi-dimensional approach to defence innovation [5]. On top of the characteristics exposed in the Background and Definition section of this booklet, current systems distinguish themselves by the abundant inbound real-time dataflow.

Controlling information streams and avoiding information overload will be essential in contemporary and future land warfare. On the battlefield, it will be necessary to ensure an effective balance between soldiers' protection and mobility, with connectivity and communications remaining two crucial aspects of the next generation Mission-Critical systems.

About collaborative Data-Links

Under NATO operations, interoperable tactical data link are defined from link 1 to link 22 to ensure "continuous data exchange in (nearly) real time about space, ground, air, surface and subsurface platforms including allied, neutral and foe units data." [6] [12]

Collaborative systems are also in development within several European terrestrial armed forces, such as (non-exhaustive):

- Switzerland, started the NEO (Network Enabled Operations) since 2006
- Germany, the DLBO has been launched. (Digitalisierung Landbasierter Operationen)
- Sweden, the LSS Mark started its deployment in 2021 (Ledningsstödsystem Mark)
- France works on the integration of the SCORPION program (Synergie du Contact Renforcée par la Polyvalence et l'Infovalorisation)

For the purpose of interoperability of those different systems the LATACC program (LAnd TActical Collaborative Combat) was launched by the European

Commission in 2022 with its European Defence Fun [18]. Solid innovation capacities in the era of sensors, robotic, cloud and artificial intelligence are expected to be brought by the participants, complementing the MIDS/JTIDS data links [12] already existing, common to NATO countries.

The Aegis ballistic missile defense (BMD) program [14] is a good example of a complete C5ISR integration. It provides regional defense onboard US-Navy Aegis cruisers and destroyers against potential hostile ballistic missile attacks. (Figure 3)

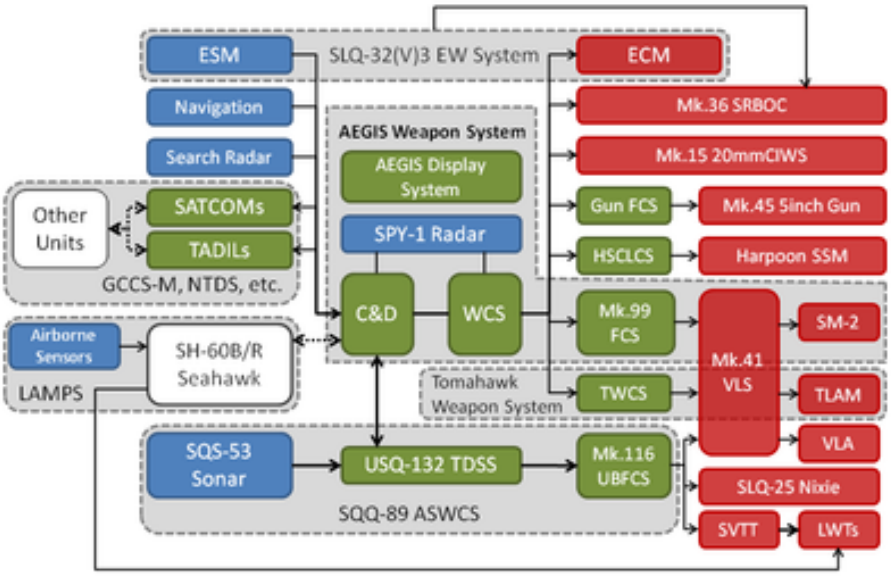

Figure 3 - Diagram of the Aegis Combat System (Baseline 2-6)

The complexity of the illustration is a good example of the progress done since gathering a sum of elementary data collection one by one. Nowadays, given the advanced motorization, the lifetime for the validity of a single piece of data is highly reduced. While many concurrent sources contribute to improved assessment, the time to gather data and set cross-correlations still impacts the **Orient** phase of the OODA cycle loop.

The Essence of Mission-Critical Systems

The future era of Mission-Critical systems requires a delicate balance between cutting-edge products and well-defined methodologies. Products empower technological applications with advanced capabilities, while methodologies provide the **AAA**, **Anticipation**, **Agility** and **Adaptability** required to operate those products along the operations. This seems to contradict with traditional Mission-Critical procurement requirements. But in today's nomenclature, Mission-Critical products or systems is transitioning from expensive, rigid and long lead times towards contracts that include software-defined solutions, designed to be modular, flexible, adaptable and configurable.

The trend of Mission-Critical systems tendency is breaking the silos: from war-fighting towards a virtual networking interconnection, serving the interest of a globally integrated commandment. The integration at a global level of the OODA is on the way, towards even the integration of civilian reporting into the network.

Battlefields are now waged with data-ification, software and AI, while more military decisions are handed off to algorithms [9] [10]. Civilian defence-tech startups, as well as established companies, stand to wield outsize power as independent actors [13]. Civilian startup involvement doesn't contradict with Mission-Critical requirements. It however adds-up to the complexity of context shaping for each individual mission within the contingency of an interconnected framework, not to mention the ethical and legal issues of responsibilities.

"Ukraine is a living laboratory in which some of these AI-enabled systems can reach maturity through live experiments and constant, quick reiteration," says Jorritt Kaminga, the director of global policy at RAIN, a research firm that specializes in defense AI. Yet much of the new power will reside in the hands of private companies, not governments accountable to their people. "This is the first time ever, in a war, that most of the critical technologies are not coming from federally funded research labs but commercial technologies off the shelf," says Steve Blank, a tech veteran and co-founder of the Gordian Knot Center for National Security Innovation at Stanford University. "And there's a marketplace for this stuff. So the genie's out of the bottle."

Foresight considerations

While practicing foresight, we like to plot different scenarios on a 2x2 matrix to help visualize the forces in actions. The illustration below makes no exception to the rule. (Figure 4)

One of the axes, the vertical is the technology complexity, while the horizontal one is the redundancy.

High-Complexity, High-Technology, Single unit operation: In this quadrant, a typical example is brought by the spacecraft Euclid, a typical example of a single unit mission-critical system. Its research and development program lasted for many years, under the authority of ESA. Its mission is to investigate the expansion history of the Universe and the growth of cosmic structures over the last 10 billion years of cosmic history. It is a space telescope with instruments that can detect visible and near-infrared radiation [15]. With a Nominal mission lifetime of six years (ending 2028), and the possibility of a five year extension, the criticality of the mission relies on the careful engineering and assembly of all its components for the success of the mission.

High-Complexity, High-Technology, Redundant system operation: This quadrant is a perfect representation of a complex battlefield. Many individual Mission-Critical systems are gathered by multiple vendors to shape this command and control infrastructure, running artificial intelligence over a comprehensive dataset brought by multi-platforms, running sensor-fusion. If every single piece of this complex system is individually designed for Mission-Critical operation, it is also backed by real-time data redundancy brought by complementary units to address the requirement of Time Sensitive Targetting.

Under technical considerations, the bottom quadrants are usually not considered as Mission-Critical items. However, they do carry the potential to wreak havoc among conventionally structured forces. Until recently they were considered as unconventional, or part of the asymmetric warfare. But the reality is that they are taking an increasingly important space within the equation.

Figure 4 - Plot of mission-critical systems

A low complexity, highly redundant example is brought by the massive introduction of low-cost quadcopters. The title of the picture doesn't require any additional comment.

Massively built drones borrowed from the civilian market do not require survivability. With a price tag below the cost of an unguided 155mm artillery shell, they exhibit capabilities which were unknown to the battlefield until recently. Precision targeting together with massive launch capability have proven to offer strategic advantages with very brief lifetime for its mission.

The American think tank Mitchell Institute has carried out several simulations highlighting the added value that an extended range of combat drones brings to modern collaborative combat, in particular to confront a symmetrical adversary with powerful access denial systems, as is the case of China [16].

Finally, the picture of **low-tech, single usage** is brought by this kite assembled by post-teenagers. Made of low-cost components, the kite carries a torch, on fire, lagging behind the kite in connection to a 5m string. Even if the failure rate

of such equipment is presumably important, the ones who make it to the target carry significant damaging capabilities.

This argument is published in a book called “Unrestricted Warfare” [21] written in 1999 by two colonels of the People Liberation Army of China. The authors argue that the primary weakness of the United States in military matters is that they thought about military dominance solely in terms of technology. They further argue that to the US, military doctrine evolves because new technology allows new capabilities. As such, the United States does not consider the wider picture of military strategy, which includes legal, economic, information, technological and biological factors, making the case that the country is vulnerable to attack along asymmetric lines. Progress has been done since 1999 but the warning is still here.

“For the first time in the history of warfare, for a few hundred euros, combatants can have access to precision weapons at a low price. They abound, they prowl, they are murderous.

Last fall, in less than a week, they destroyed up to 75 Russian tanks and 101 artillery pieces. Ukrainians in 2024 are expected to produce between one and two million of them... Never before had the battlefield been saturated with smart munitions achieved so fast at such low cost.

With AI, the development of swarms is getting closer. It will make it even more difficult to understand the battlefield and how to guard against such a threat.

This technology is developing at the frantic pace of the mass market of a consumer society greedy for technological gadgets of all kinds, adding new capabilities with each new release. And it's spreading all over the world... In Myanmar, for example, small workshops are using 3D printing to produce parts and assemble drones.”

The Economist, February 2024

The disruptive forces

As we stand at the intersection of traditional approaches and the disruptive forces of both low-tech and advanced technologies, the difficulty of maintaining Mission-Critical systems becomes pronounced. Recent conflicts

have underscored the critical role played by non Mission-Critical elements, shedding light on the potential disruptions caused when even seemingly unimportant components get into action. In this era, where every element is interconnected and dependent on seamless operation, the importance of Mission-Critical Solutions is more pronounced than ever, while at the same time its utility gets more controversial than ever.

Qualifying for Mission-Critical specification product or system compliance is a long journey. But the composition of the battlefield is increasingly versatile, turning quickly and opportunistically non-conventional products or technologies into potentially destructive weapons. *"Collapse adversary's system into confusion and disorder causing him to over and under react to activity that appears simultaneously threatening, ambiguous, chaotic, or misleading."* Statement from retired colonel John R. Boyd, 1982.

So, under the authority of its ministry of digital transformation, Ukraine has chosen the agile and adaptable path. They've built in a record time a battlefield tactical information management system, called Delta. It's a native cloud development data sharing and info-valuation platform that can be used from any digital platform. Many sensor sources are qualified to provide data under a secured protocol, including any citizen, able to share valuable tactical information.

Also, Ukraine has brought a different approach to ELectronic INTelligence (ELINT), claiming that the lifetime of a video shot on the battlefield has an operational duration of 10 minutes before obsolescence. Within such short amount of time, the video can't make it through the information channel, get processed and then back to the relevant units. So instead of investing into a complex, long and expensive program, they just use Discord, the mobile app, for the video transmission of information, which provides the ability for up to 25 participants to join simultaneously in a video chat. It's a sort of decentralized OODA loop cycle.

If they have the power to bring value to a global defence organization, items considered as non Mission-Critical can strongly disrupt the course of operations. "Malicious actors are laying the groundwork for victory on tomorrow's battlefield by using the same innovation and critical infrastructure

democracies are using to save lives. Terrorists, however, are using new technologies to extinguish lives." [2]

Those technologies are often massively abundant, coming from everyday's civil life, having the power to saturate the conventional sophisticated defence systems. Excerpts:

"The attack on October 7 is unprecedented from Hamas both in scale and sophistication, displaying characteristics of a special-forces operation that employed small units with bespoke training, equipment, and tactics to achieve outsized strategic results [7]. On that day, over 1,000 Hamas fighters entered southern Israel through nearly 30 breach points in the country's border wall with Gaza. The 40-mile-long barrier, which cost over $1 billion and was upgraded in 2021, was designed to prevent infiltration with a variety of surveillance and defense technologies. These include cameras, radars, and other technological sensors, as well as barbed wire and an underground concrete barrier to prevent tunneling. In addition to the 20-foot-tall fence, observation towers with remote machine gun turrets were positioned, in some areas, every 500 feet along the border.

Figure 5 - Footage from Drone Attacks on Israeli Border Fence on October 7, 2023
Source: Video shared on Telegram by al-Qassam Brigades

To overcome these defences, Hamas employed a combination of innovative tactics. Using commercial quadcopter drones, they dropped explosives onto the observation towers, disrupting Israel's sensors, communications, and

weapons systems (Figure 5). It's a creative use of drones, which are also being used in new ways by Russian and Ukrainian forces.

Simultaneously, some of the fighters flew on motor-powered paragliders across the border fence into Israeli territory. Although slow and loud, the gliders had to cover only a short distance. A video of the attack shows that some motor-paragliders crossed the border under the cover of rocket barrages. (Figure 6)

Figure 6 - Footage of a Hamas Fighter Using a Paraglider during the October 7 Attack
Source: Video shared on Telegram by al-Qassam Brigades

On that tragic day, one of the most modern communication and control system in the world has been defeated by a low-cost low-tech adversarial maneuver.

Just like for the Sept. 11 attack on the twin towers, a bet was placed on the success of the consternation effect. The surprise of using massive low-cost rockets to overwhelm the protection lines, as well as the audacious usage of commonly available civilian equipment like bulldozers or this motorized paraglider (Figure 7), broke down the defence organization [7].

Each of the individual actions could fail. But the massive amount of de-correlated operating modes was such that it produced the required effect.

Hamas's attack represents an evolution in the group's capabilities and tactics. In the 1990s and 2000s, they frequently conducted suicide bombing attacks against civilian targets, including universities, buses, and restaurants in Israel.

Since taking control over the Gaza Strip, fewer suicide attacks were conducted, stymied in part by Israeli border security measures, instead expanding its rocket and drone capabilities.” [8]

Figure 7 - Armed paragliders
Source: The Telegraph

Technology or Methodology - Charting the Course Ahead

In earlier times Mission-Critical denoted a meticulous approach to designing, producing, and maintaining products to ensure optimal functionality within predefined parameters. It used to play a central role in the procurement of equipment.

This principle remains steadfast today; however, the battleground has morphed into a sophisticated network of interoperable Mission-Critical systems, now infused with Artificial Intelligence, sourced from diverse vendors. The maintenance of these systems, crucial for success in defence and aerospace, poses unprecedented challenges with the threat's evolution.

Figure 8 - Mission-Critical?
Source: The Economist, Sep. 21st 2023

Artificial intelligence will be deployed in all French air traffic control centers by the end of 2024. Its use, currently limited to non-critical operations, is a breakthrough in an industry where safety is a priority. Objective: To help controllers limit the risk of human error. [11]

Concurrently, officials recognize that some artificial intelligence capabilities developed in a lab might not be up to snuff when they're sent into a warzone. [6]

The crux of the matter lies in determining the future era of Mission Critical systems - will it be defined by advancements in technology or innovative methodologies, a combination of both, and is low-tech [17] required to be included into the structure?

As we grapple with this question, the keywords such as AI-Optimized, Edge-AI, Methodological Approaches and AI-Driven Innovations for Critical Tasks become pivotal. The integration of AI in Critical Systems Implementation and the pursuit of Agile Methodologies for Critical Operations are shaping the futurs. From one single piece of highly sophisticated, intrinsically safe and secure system, all the way to a swarm of low cost but highly redundant robots, the shape of Mission-Critical systems is undergoing a significant transformation. Remaining competitive on the battlefield calls to the usage of a similar vocabulary as remaining competitive on the commercial landscape.

If the usage of artificial intelligence counts numerous and undisputed positive track records, several concerns are raised by agencies with respect to its limitations. Just like with other tools, its implementation, the methods and quality of its training may lead to unforeseen adverse situations.

“Because models are trained a priori on data (and simulations) in an anticipatory fashion, AI-based systems encounter situations in the real world that are incompatible with training feature distributions and parameterization of employed algorithms. The result is degradation to model performance that can negatively impact mission effectiveness and safety. Therefore, the US Air Force requires new battle management processes to monitor the performance of AI-based systems and update incumbent models in response to changing battlespace conditions,…” statement from the DoD Broad Agency Announcement in the section for Technical Area 1, which deals with command and control of artificial intelligence systems to achieve mission-tailored AI [20].

“*A new kind of battle manager within the forward tent, deemed the AI Interface Officer, monitors the performance of computer vision models hosted on UAVs and looks for cases of ‘AI drift’ — unexpected behavior caused when the domain of the learned function is no longer compatible with input data. In this case, an object detection model is no longer performing, with live sensor data due to significant changes from a weather event. The AI Safety officer must evaluate the risk to mission success posed by continued employment of the model. If the risk is deemed too high, the AI Safety Officer will coordinate with remote operators via cloud-based services to determine the root cause of the drift and propose new AI adaptation strategies (e.g., replace model, fine tune, transfer learn, etc.) and deployment options (e.g., ‘use uplink to replace*

model on UAV at 1500 hours') that accommodate the environment while also adhering to imposed mission timelines,"

Jon Harper, Defensescoop, March 2024 [6]

The future of Mission Critical systems resides at the crossroads of Technology and Methodology.

Striking the right balance and leveraging the capabilities of AI is already instrumental in navigating the complexities of modern defence and aerospace operations. Introducing alternative methodologies becomes vital to take strategic decisions in increasingly fast evolving and dynamic pattern environment.

More than ever, Mission-Critical requires the AAA: Adaptation, Anticipation, Agility. Very significant budgets are already allocated by several armed forces to come up with the appropriation of AI-autonomous low-cost equipment [19]. The transition is on the way. A mix structure of available components opens the technical question of interoperability. Ultimately, the requirement shall transition from the usual platform-centric approach towards a decentralized capability-centric approach.

But the Pandora box is opened, with questions related to responsibility, ethics and legal issues. Mission-Critical Technology and Methodology are ready to transition, with potential ability to conduct the next generation of war operations. Is the doctrine organization ready?

Illustrations

References

1. Source Statista. DOI
2. Countering Terrorism on Tomorrow's Battlefield: Critical Infrastructure Security and Resiliency (NATO COE-DAT Handbook 2). Lucas M. Cox, Denise Feldner, Trevor P. Helmy, Frank J. Kuzminski, Sarah J. Lohmann, Marcus Mohlin, Aleksander Olech, Wuraola Oyewusi, Gabriel T. Raicu, Silke Ruhl, Sabrina Schulz, Máté Tóth, and Megan A. Ward. DOI
3. Investopedia. Mission Critical: Overview, Examples, FAQ. DOI
4. Trenton Systems Blog Command and Control . DOI
5. The Next Generation Soldier: A System of Systems Approach? *Alessandro Marrone, Karolina Muti* DOCUMENTI IAI 21 | 15 - NOVEMBER 2021 – ISSN 2280-6164. DOI
6. Air Force provides more details about plans for 'battle management' of AI, *Jon Harper,* Defensescoop, March 2024. DOI
7. Hamas 's October 7 attack: Visualizing the Data. Commentary by Daniel Byman, Riley McCabe, Alexander Palmer, Catrina Doxsee, Mackenzie Holtz, and Delaney Duff. CSIS Center For Strategic & International Studies, Published December 19, 2023. DOI
8. Homemade rockets and modified AK-47s: An annotated look at Hamas' deadly arsenal. *Isabelle Chapman, Audrey Ash, Daniel A. Medina and Allison Gordon, CNN. Visuals by Tal Yellin, Ian Berry and Vanessa Leroy.* CNN Investigates. DOI
9. Advances of Artificial Intelligence in Aeronautics. *Byron Sanchez*, Athenea. DOI
10. A Deep Reinforcement Learning Approach for Improving Age of Information in Mission-Critical IoT. *H. Farag, M. Gidlund and Č. Stefanović*, 2021 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT), Dubai, United Arab Emirates, 2021, pp. 14-18, DOI
11. Le contrôle aérien français adopte l'intelligence artificielle. Olivier James, L'Usine Nouvelle, Mars 2024. DOI
12. Tactical Data Link – From Link 1 to Link 22. Anca STOICA, Diana MILITARU, Dan MOLDOVEANU, Alina POPA, "Mircea cel Batran" Naval Academy Scientific Bulletin, Volume XIX – 2016 – Issue 2. DOI
13. How Tech Giants Turned Ukraine into an AI War Lab. Vera Bergengruen, Time Magazine, DOI
14. Navy Aegis Ballistic Missile Defense (BMD) Program: Background and Issues for Congress (RL33745)". Congressional Research Service. 2024-02-06. DOI
15. Euclid Spacecraft Fact-Sheet. DOI
16. Five Imperatives for Developing Collaborative Combat Aircraft for Teaming Operations. The Mitchell Institute Policy , 2022-10-06 . DOI
17. Le Soldat Low-Tech. Le Coup d'Après. Armasuisse Deftech.ch Sept 2022. DOI
18. LATACC - LAnd TActical Collaborative Combat – Eurpean Defence Projects. DOI
19. Unmanned Campaign Framework, Department of the Navy. March 16th. 2021. DOI
20. ARTIFICIAL INTELLIGENCE AND NEXT GENERATION DISTRIBUTED COMMAND AND CONTROL, DEPT OF DEFENSE, DEPT OF AIR FORCE, Notice ID FA875023S7006. DOI
21. Unrestricted Warfare. Wang Xiangsui, Qiao Liang. People's Liberation Army Literature and Arts Publishing House, February 1999. ISBN 9787540318871

Standards

It's important to note that the specific standards and guidelines applicable to mission-critical systems vary depending on the industry, domain, and the nature of the system in question. Organizations developing or operating mission-critical systems typically tailor their quality, safety, and security practices to meet the specific requirements of their projects.

Standardization organizations haven't dedicated any specific standard to mission-critical systems. However, a variety of standards and guidelines relevant to mission-critical systems in different domains is available.

The list below is a non-exhaustive selection, of common standards or guidance references.

Notice that standards and regulations are poised to evolving over time, so it's essential to stay current with the latest developments.

ISO/IEC 27001 - Information Security Management: ISO/IEC 27001 is a standard for information security management systems (ISMS). It is crucial for mission-critical systems, especially in the context of cybersecurity, to implement robust information security practices. ISO/IEC 27001 provides a framework for managing information security risks.

ISO 26262 - Road Vehicles - Functional Safety: ISO 26262 is a standard for functional safety in the automotive industry. While specific to automotive systems, it has principles and practices that can be relevant to the development of mission-critical systems in other domains.

ISO 12207 - Systems and Software Engineering - Software Life Cycle Processes: ISO 12207 provides guidance on software life cycle processes, including requirements, design, testing, and maintenance. Mission-critical software systems often adhere to ISO 12207 practices.

ISO 20000 - Information Technology - Service Management: ISO 20000 is a standard for IT service management, which can be applicable to the management of mission-critical IT systems and services.

ISO 21500 - Guidance on Project Management: ISO 21500 provides guidance on project management principles and processes. Effective project management is essential for the successful development and maintenance of mission-critical systems.

IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems - The safety integrity level (SIL) provides a target to attain for each safety function.

TADIL J: INTRODUCTION TO TACTICAL DIGITAL INFORMATION LINK J AND QUICK REFERENCE GUIDE (NATO Link 16, June 2000)

JACG NAVAIR Public Release 11-514 - Aviation Source Approval and Management Handbook (16 March 2011)

JEDEC-JC13 Committee responsible for standardizing quality and reliability methodologies for solid state products used in military, space, and other environments requiring special-use condition capabilities beyond standard commercial practices.

AS9100 Quality Systems - Aerospace - Model for Quality Assurance in Design, Development, Production, Installation and Servicing

MIL-STD-810H: Department of Defense. Test method standard: Environmental engineering considerations and laboratory tests (31-JAN-2019)

MIL-STD-883L: Department of Defense. Uniform methods, controls, and procedures for testing microelectronic devices suitable for use within military and aerospace electronic systems (16-SEPT-2019)

MIL-PRF-38535: NASA. Standard Microcircuits, Hermetic and Non-hermetic (14 June 2021)

...

About the author

olivier.desjeux@advancedvalueglobal.com

Olivier Desjeux is an electronic engineer/MBA, who spent his career in the development of wireless transmission units.
Several of his products helped to save lives of pilots, with the Breitling Emergency wristwatch. He developed internationally recognized Search and Rescue experience, which led him to consult within several armed forces, including the US Navy.
Other products developed and produced by his previous company, Ingecom, saved lives by microlocalisation of 4000 miners trapped into the South African deepest mines of the world, 4000m underground.
His consulting firm is active in strategic advisory, in particular for industrial companies of the aerospace and military segment.
Being himself a pilot, helicopter flight instructor, he carries the voice of both the engineer and the operational user. From Vision to Execution.

deftech.ch