3 Initial Steps to Address Unsecure Cyber-Physical Systems

Published 4 November 2021 - ID G00743283 - 17 min read

By Analyst(s): Katell Thielemann

Initiatives: Cybersecurity and IT Risk

> Business-led Internet of Things or converged OT-IT projects have largely underestimated or ignored security and safety risks. Security and risk management leaders must go beyond data security by embracing cyber-physical system security efforts, or they will soon be overwhelmed by new threats.

Additional Perspectives

- Summary Translation: 3 Initial Steps to Address Unsecure Cyber-Physical Systems (12 February 2022)

Overview

Key Findings

- Cyberattacks that have halted physical processes at companies such as Colonial Pipeline and JBS have clearly shown that many connected assets are cyber-physical systems (CPS). CPS represent an opportunity to tackle security and safety across information technology (IT), operational technology (OT) and Internet of Things (IoT) initiatives.
- Deployment of CPS is tightly coupled with business initiatives driven by industry needs, as many CPS deployments occur outside IT departments.
- The growing realization that all connected assets are CPS directly challenges the traditional roles, responsibilities, and authorities of security and risk management (SRM) leaders beyond IT and data-centric security. Digital business transformation will accentuate this challenge.
- CPS pose unique technical challenges for IT-centric security leaders.

Recommendations

To succeed with, and learn from, the growing convergence of cyber and physical domains, and the expansion of CPS, SRM leaders responsible for technology, information and resilience risk should:

- Prioritize discovery of all CPS in their environment. They should identify specific CPS security controls already in place, determine what existing IT security controls can address CPS vulnerabilities, and document gaps in preparation for an action plan.
- Anchor security strategy, governance and tactics to the business value that CPS directly support, and to vertical industry needs. This industry-centric approach will be the most helpful way to deliver tangible and beneficial results, particularly in critical infrastructure sectors.
- Focus on one tangible governance and one pragmatic technical challenge at a time initially, and then iterate. Security changes in operational and mission-critical environments mandate caution, and both technological and cultural changes need to be thoughtful.

Introduction

With the number of connected assets on the increase, tomorrow's world will be one in which these assets are everywhere and anywhere. It will be a world in which a hyperconnected intelligent mesh of CPS connects everything and everyone to everything and everyone.

CPS are engineered to orchestrate sensing, computation, control, networking and analytics in order to interact with the physical world (including humans).

They underpin all smart and connected efforts for which security considerations span the cyber and physical planes. These efforts relate to developments and technologies such as, or associated with, connected OT (e.g., ICS, SCADA, weapon systems), the IoT, the industrial IoT (IIoT), Industrie 4.0, smart buildings, smart cities, smart ships, smart medical devices, installations of the future, the Internet of Battlefield Things and drones.

When secure, CPS enable safe, real-time, reliable, resilient and adaptable performance. When not secure, they can lead to halted operations — or worse, to safety or environmental issues.

Interest in connecting OT to enterprise networks, as well as in deploying new connected assets (thereby creating CPS), continues across most organizations, led by business or mission-related needs. Unfortunately, too often being “first to market” remains more important than being “secure to market,” and business convenience also usually wins out over security. As a result, these asset-related digital transformation efforts bring forth increased risks, as threats and vulnerabilities grow, and SRM leaders continue to struggle to get to grips with them.

Time and again, Gartner is asked what three actions to start with, so we provide the beginnings of a roadmap below.

Analysis

To prevent the Internet of Things becoming the Internet of Dangerous Things, and stop OT-IT convergence turning into OT-IT meltdown, SRM teams must focus on the cyber-physical security considerations of these connected assets that can be articulated and tackled pragmatically.

Too often, they zero in on IT and data-centric concerns instead, which addresses only half the issues. Adopting a pragmatic cyber-physical security risk mindset, and focusing on understanding the threats and vulnerabilities of CPS, is imperative.

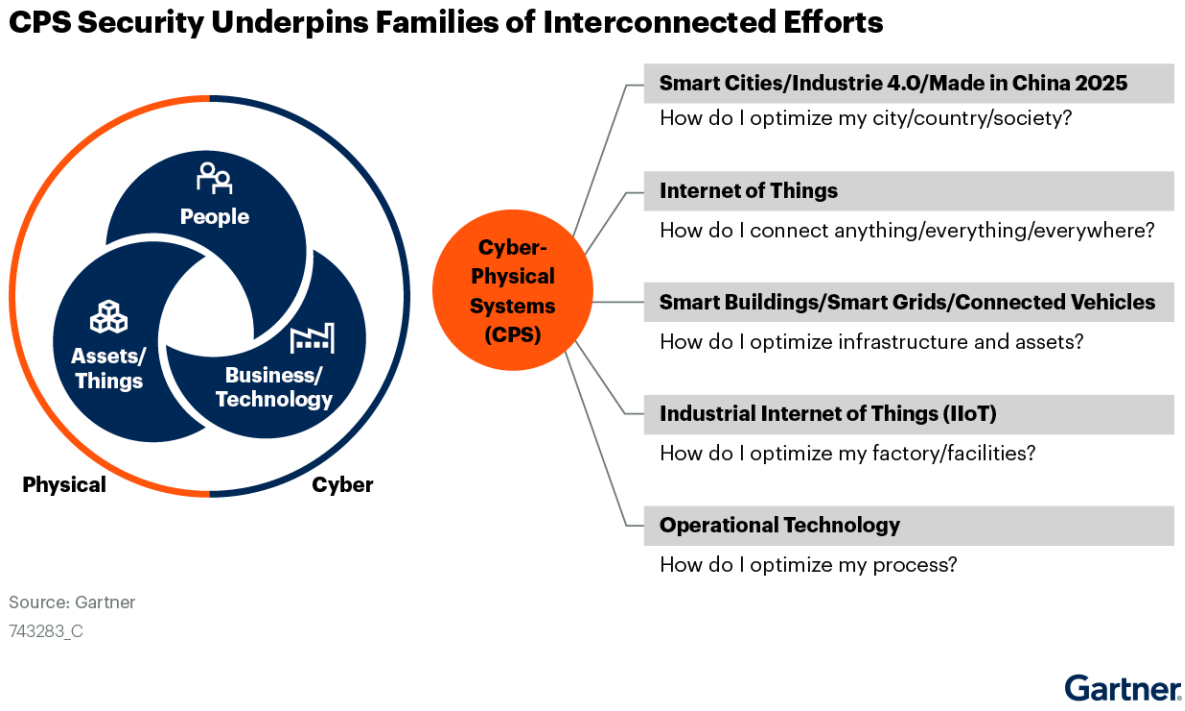
Recent Events Have Raised Awareness of the Cyber-Physical Nature of Connected Systems

CPS underpin families of interconnected efforts (see Figure 1) that seek to optimize outcomes, from individual processes to entire ecosystems, by merging cyber/digital approaches with the physical world.

Unlike enterprise IT systems that focus on data in the digital world, CPS “do” things. They sense things. They create or change things in the real world.

As a result, CPS increase attack surfaces in both the digital and physical worlds through their reach and complexity. But what can be learned from their connectedness to the physical world can also shed light on better defenses for all systems.

Figure 1. CPS Security Underpins Families of Interconnected Efforts



Source: Gartner
743283_C

Gartner

The interdependency of the cyber and physical worlds has been felt for years, as a result of incidents caused by, for example, Stuxnet, NotPetya and Mirai attacks.

But, in 2021, they came to life for many like never before, due to large-scale ransomware campaigns against:

- **Hospitals:** Springhill Medical Center is being sued for what could be the first death directly attributable to ransomware, when clinical devices became inoperational. [1]
- **Pipeline operators:** Colonial Pipeline stopped all its fuel processing for days when it fell victim to a ransomware attack. [2]
- **Water utilities:** An attacker managed to physically move gauges in Oldsmar, Florida, U.S. [3]
- **Food plant operators:** Multiple plants of the largest meat packer in the U.S. ground to a halt due to an attack. [4]
- **Ports and transportation systems:** In South Africa, an attack halted operations in the middle of a crucial food export season. [5]

Ransomware is no longer an IT-only security issue. Halting the physical operations of asset-centric organizations increases the likelihood of ransom payments, because every idle hour is a hit to the bottom line and could threaten safety. Every organization should assume that its CPS environment will be increasingly targeted.

CPS Are Tightly Coupled With Business Initiatives Driven by Vertical Industry Needs

CPS tend to operate in mission-critical environments that prioritize safety, availability, security, reliability, resilience and adaptability. They exist across a wide range of environments, with very strong vertical industry characteristics (see Note 1).

From a vendor-marketing standpoint, the use cases in Note 1 are often grouped into generic “OT security” or “IoT security” categories. From a security and risk practitioner standpoint, however, SRM leaders need to treat smart buildings, remotely piloted aircraft or connected medical devices, for example, completely differently. They need security approaches for the specific assets in their specific environments.

This is critical because risks, vulnerabilities, threats, controls, industry protocols and governance approaches vary widely for different scenarios. In addition, the evolution of many CPS has been driven by business needs and led by business units. Whether organizations are looking to get more visibility into production systems, remove costs, increase maintenance intervals, manage just-in-time inventories, or automate routine or unsafe tasks, the drivers of the explosive growth of CPS are business-driven, not security-driven.

Anchoring security approaches to business strategy, business models, and outcomes in the vertical industries served will help reduce challenges and deliver results. It will also help shift internal security discussions from security “geek-speak” to business impact discussions.

Traditional IT Roles and Governance Are Uniquely Challenged by CPS Security

As the CPS environment continues to evolve, the roles of chief information officer (CIO), chief information security officer (CISO) and chief risk officer (CRO) will come under increased scrutiny from boards of directors and shareholders.

Key role-oriented questions will include:

- Is the CISO's focus on "information" too limiting when it comes to CPS? Gartner has long recommended that safety, reliability and privacy be added to the security triad of confidentiality, integrity and availability. The physical plane of CPS will make safety, reliability and privacy even more important in the future. CPS security is also about asset-centric and ecosystem-centric security, not just network- or data-centric efforts.
- Are CIO organizations, which CISOs often report to, equipped to focus on business operational processes in factories or mission-critical uptime?
- Can CROs adequately focus on CPS at the microlevel while also focusing on macrocompetitive, societal or supply chain risks in an increasingly volatile world?
- Who really has authority over risk, safety and security when industrial control systems (ICS) and supervisory control and data acquisition (SCADA) are owned by engineering, when physical security is the responsibility of facilities managers, when compliance reports to a legal counsel, and when the board is increasingly under scrutiny to own enterprise-level risk management? Should there be an overall chief security officer (CSO) who reports to a chief operating officer (COO) or directly to the board?

Whatever the organizational structure, SRM leaders in charge of CPS (whatever their role is called) must also deal with governance issues, such as:

- Cultural challenges to ensuring that CPS security is seen as a value-add to the business, instead of an alarmist, obstructionist and expensive cost center.
- An evolving patchwork of frameworks, regulations and legislation, which is growing rapidly, particularly in critical infrastructure-related sectors.
- The difficulty of translating strategy into action in a complex business environment, including planning, communications, stakeholder management, change management, governance, skills and talent management, among other things.
- A fast-moving technology and vendor landscape.

Technical Complexities Unique to CPS

CPS present unique technical challenges, due to the inherent complexity of their architecture and the safety or mission-critical dimension of the environments they operate in.

Examples of these challenges include:

- Choreographing highly complex systems and interactions for outcomes in the physical world.
- Accounting for scale, when the physical and cyber planes stretch from remote field environments to enterprises.
- Managing interdependencies, and dealing with entanglements so complex that one might come up against the “changing anything changes everything” (CACE) principle. [6]
- Handling interoperability issues in environments with many protocols, processes, proprietary systems and emerging open standards.
- Incorporating human-centered design to ensure optimal and safe operations.
- Optimizing bandwidth, while minimizing latency, to allow for the uninterrupted flow of communications.
- Managing computation/storage limitations driven by mobility and energy consumption factors, and evaluating a growing role for cloud-to-edge computing.
- Dealing with the increasing share of resources spent on software costs and complexity, which demands increased efforts relating to algorithms, machine learning and model-based analysis.

Because CPS security needs to focus on safety, reliability, resilience, adaptability and privacy (and in some sectors, such as defense, survivability), SRM leaders must also focus on:

- Security of controls, actuators or sensors.
- Network segmentation, isolation or masking complexity.
- Size and limited computational power to run security on deployed devices.
- Identity management and authentication in resource-constrained devices.
- Security by design for new emerging systems versus securing and integrating what was installed decades ago.
- Secure communications and telemetry data.

- Regulations and compliance in highly regulated industries.
- Supply chain security, such as anti-tampering capabilities, and efforts to manage a proliferation of components with hard-wired back doors that cannot be blocked or easily updated.
- Continuous evolution of new attack vectors, such as drone-mounted signal jammers, GPS jamming and spoofing, and object spoofing for autonomous vehicles.

Recommendations

Step 1: Discover All CPS

For many organizations, the technology-driven convergence of the cyber and physical worlds is a new phenomenon that has not yet entered their business psyche. As a result, they fail to realize the extent of the convergence, integration and interdependency of CPS already present in their organizations, let alone the next wave.

This is why it is imperative, as a first step, to discover all the connected assets in your environment, including all CPS "owned" by the business. The old adage holds true: You cannot manage what you cannot measure. Time and again, Gartner client inquiries show the value of deploying the asset discovery and inventory solutions that are on the market for non-IT systems (see Market Guide for Operational Technology Security). Critical information can then be captured and mapped, such as manufacturers, models, OSs, Internet Protocol (IP) addresses, Media Access Control (MAC) addresses, protocols, patch-level information, firmware versions, and asset locations (physical and logical).

Armed with this level of information, you can:

- Evaluate the current state of CPS security, if any.
- Look at what existing IT security practices can be extended to CPS.
- Perform a gap analysis to learn what hybrid IT-CPS security approaches might be needed (for instance, vulnerability and patch management).
- Document CPS-specific risks and new security approaches that are needed as a result.

Step 2: Anchor CPS Risk Strategies to Business Value and Vertical Industry Needs

Every strategy for CPS risk management and security should be anchored to two pillars: business value and vertical industry needs. CPS are assets, not just data-producing systems. As such, their value to an organization's operations or mission-critical outcomes cannot be dissociated from their security and risk posture.

The business value pillar helps:

- Quantify the impact of attacks that disable CPS. For instance, attacks that have crippled Maersk, Norsk Hydro and JBS have been quantified as costing the victims millions of dollars per day.
- Model and quantify risk, based on CPS type and location, in order to prioritize security efforts.
- Engage with the board of directors and the C-suite in language they understand, not arcane security techno-speak. Too often, the risk and security function remains a compliance exercise, or worse, an alarmist, obstructionist and expensive cost center. When it comes to CPS security, using business terms turns the discussion to value protection.

The vertical industry pillar helps:

- Understand the regulatory landscape, which is often sector-based — as, for example, with the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) and new directives to pipeline operators in the U.S.
- Align with frameworks or standards that are also usually sector-based. They include various industry profiles developed for the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF), such as those for:
  - Manufacturing [7]
  - Maritime bulk liquid transfers [8]
  - Health sector [9]
  - Emergency services [10]
- Engage with sector-based Information Sharing and Analysis Centers (ISACs) for intelligence and best-practice sharing. [11]

- Select CPS security vendors that have demonstrated vertical industry knowledge, due to unique protocols and rules of engagement. For instance, some companies are forming partnerships to serve specific industries, such as Nozomi Networks and Cervello for rail, [12] and Dragos and Xylem for the water utilities sector. [13]

Step 3: Select CPS Risk Challenges Carefully and Then Iterate

Security changes in operational and mission-critical environments mandate caution, and both technological and cultural changes need to be thoughtful. Instead of immediately starting large-scale changes (and likely running into a wall), SRM leaders should first select one tangible governance challenge and one pragmatic technical challenge to focus on at a time, and then iterate.

Governance challenges can include:

- Working with business and technology stakeholders to develop a vision and strategy for CPS security.
- Updating vulnerability management policies to account for the unique patching challenges of CPS.
- Developing a hybrid IT-CPS approach to threat intelligence.
- Creating a remote access policy for CPS OEMs.
- Ensuring the SRM team includes CPS security skills.
- Developing executive and regulatory compliance metrics and reports.
- Working with procurement teams to enhance supply chain risk management.
- Workforce training on CPS security.

Technical challenges can include:

- Revisiting the posture of all firewalls in operational environments to ensure they are properly configured.
- Deploying anomaly detection and alerting solutions for operational environments that can feed into IT security tools.
- Updating privileged access management efforts.

- Inventorying and closing all unnecessary open ports.
- Developing and testing incident management playbooks.
- Discovering which CPS can support multifactor authentication and isolating those that cannot.
- Reviewing physical and logical access for all high-value CPS.

Evidence

The analysis in this research is based on primary and secondary research reflecting Gartner's many daily interactions with end users and technology providers.

[1] Kevin Poulsen, Robert McMillan and Melanie Evans, A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death, The Wall Street Journal, 30 September 2021.

[2] David Jones, Colonial Pipeline Disconnects OT Systems to Silo Ransomware IT Threat, Cybersecurity Dive, 12 May 2021.

[3] Kevin Senator, Oldsmar, Florida Breach Sheds Light on Need for Industrial Cybersecurity, CPO Magazine, 17 March 2021.

[4] Sara Morrison, Ransomware Attack Hits Another Massive, Crucial Industry: Meat, Vox, 10 June 2021.

[5] Zandi Shabalala and Tanisha Heiberg, Cyber Attack Disrupts Major South African Port Operations, Reuters, 22 July 2021.

[6] D. Sculley and others, Hidden Technical Debt in Machine Learning Systems, Advances in Neural Information Processing Systems 28 (NIPS 2015).

[7] Keith A. Stouffer and others, Cybersecurity Framework Manufacturing Profile, NIST, 20 May 2019.

[8] Maritime Bulk Liquids Transfer Cybersecurity Framework Profile, U.S. Coast Guard

[9] Healthcare Sector Cybersecurity Framework Implementation Guide, May 2016.

[10] Emergency Services Sector: Cybersecurity Framework Implementation Guidance, U.S. Department of Homeland Security, May 2020.

[11] National Council of ISACs

[12] Nozomi Networks and Cervello Partner for Rail Cybersecurity Solutions, Railway Technology, 23 September 2021.

[13] Xylem, Dragos Partner to Bring Cybersecurity Leadership to Water Utilities, Business Wire, 4 October 2021.

[14] World Population Projected to Reach 9.7 Billion by 2050, United Nations, 29 July 2015.

[15] Dana Gunders, Wasted: How America Is Losing Up to 40 Percent of Its Food from Farm to Fork to Landfill, Natural Resources Defense Council, August 2012.

[16] Linda Doman, EIA Projects 28% Increase in World Energy Use by 2040, U.S. Energy Information Administration, 14 September 2017.

[17] Quick Look: 277 Active Shooter Incidents in the United States From 2000 to 2018, U.S. Government.

[18] Snapshot: A Summary of CBP Facts and Figures, U.S. Customs and Border Protection, March 2021.

[19] Asad J. Khattak and others, A Taxonomy of Driving Errors and Violations: Evidence from the Naturalistic Driving Study, Accident Analysis & Prevention 151, March 2021.

[20] Daniel Flatley, Pentagon Might Obtain Self-Driving Vehicles First, Transport Topics, 30 April 2018.

Note 1: Examples of Cyber-Physical System Use Cases by Industry

Table 1: Examples of Cyber-Physical System Use Cases by Industry

(Enlarged table in Appendix)

Industry	*Use-Case Examples*
Agriculture	Precision agriculture: ■ With the global population expected to reach 9.7 billion by 2050, [14] a shrinking farming population and up to 40% of U.S. food lost between production and consumption, [15] CPS: ■ Increase food safety and efficiency throughout the value chain ■ Improve environmental footprint ■ Create opportunities for a higher-skilled workforce
Energy	Smart grids: ■ With today's aging, unreliable, vulnerable electric grids and a projected 28% increase in world energy use by 2040, [16] CPS-enabled smart grids improve the reliability, security, economics, safety, and efficiency of electricity delivery and consumption.
Healthcare	Connected medical devices/personalized medicine: ■ Whether acting as monitoring or delivery devices, CPS improve the effectiveness of patient care by providing personalized treatment through sensing and patient monitoring, while ensuring physical safety and individual privacy.
Infrastructure	Physical security information management systems: ■ With public safety threats rising, which includes a dramatic increase in active shooter incidents in the U.S. in the past 17 years, [17] CPS accelerate the convergence of perimeter security, access controls and intrusion detection technologies. Smart buildings, smart bases, smart campuses and smart cities: ■ Whether they mesh security, fire protection, environmental conditions and energy consumption tracking or enable Wi-Fi hot spots on streetlights, CPS solutions are transforming the way people live daily.
Law enforcement	U.S. customs and border protection: ■ Officers check imported goods worth $6.5 billion on an average day; [18] illegal substances and contraband can represent both economic and national security concerns. CPS help find these "needles in a haystack."
Manufacturing operations	Smart manufacturing systems, the industrial IoT or Industrie 4.0 initiatives: ■ CPS solutions help connect procurement, production, logistics, services and product delivery processes in real time to respond to rising labor and energy costs, environmental pollution or fast-changing market conditions.
Military/Aerospace	Smart weapon systems: ■ Whether it is remotely piloted aircraft/unmanned aerial vehicles (UAVs), increasingly powerful space assets, or 8 million lines of code for the F-35 fighter jet, CPS enable all modern weapon systems. Emerging aerospace systems: ■ Developments in UAV technologies in particular are occurring in the civilian and defense sectors at breakneck speed and producing an explosion of case studies on topics ranging from medical deliveries to counter-UAV technologies.
Automotive	Connected and autonomous vehicles: ■ Human error accounts for 93% of the approximately 6 million annual automotive crashes, [19] and 52% of casualties in combat zones are attributed to military personnel delivering food, fuel and other logistics. [20] CPS improve efficiency and safety in global transportation networks.

Source: Gartner (November 2021)

Document Revision History

Focus More on the Realities of Cyber-Physical Systems Security Than on the Concepts of IoT - 19 May 2020

Focus More on the Realities of Cyber-Physical Systems Security Than on the Concepts of IoT - 11 October 2018

Recommended by the Author

Some documents may not be available as part of your current Gartner subscription.

Facing New Threats — Cyber-Physical Systems

How to Develop a Security Vision and Strategy for Cyber-Physical Systems

Maverick* Research: You Will Be Hacked, So Embrace the Breach

Market Guide for Operational Technology Security

Table 1: Examples of Cyber-Physical System Use Cases by Industry

Industry ↓	*Use-Case Examples* ↓
Agriculture	Precision agriculture: ■ With the global population expected to reach 9.7 billion by 2050, [14] a shrinking farming population and up to 40% of U.S. food lost between production and consumption, [15] CPS: ■ Increase food safety and efficiency throughout the value chain ■ Improve environmental footprint ■ Create opportunities for a higher-skilled workforce
Energy	Smart grids: ■ With today's aging, unreliable, vulnerable electric grids and a projected 28% increase in world energy use by 2040, [16] CPS-enabled smart grids improve the reliability, security, economics, safety, and efficiency of electricity delivery and consumption.

Industry ↓	*Use-Case Examples* ↓
Healthcare	Connected medical devices/personalized medicine: ■ Whether acting as monitoring or delivery devices, CPS improve the effectiveness of patient care by providing personalized treatment through sensing and patient monitoring, while ensuring physical safety and individual privacy.
Infrastructure	Physical security information management systems: ■ With public safety threats rising, which includes a dramatic increase in active shooter incidents in the U.S. in the past 17 years, [17] CPS accelerate the convergence of perimeter security, access controls and intrusion detection technologies. Smart buildings, smart bases, smart campuses and smart cities: ■ Whether they mesh security, fire protection, environmental conditions and energy consumption tracking or enable Wi-Fi hot spots on streetlights, CPS solutions are transforming the way people live daily.
Law enforcement	U.S. customs and border protection: ■ Officers check imported goods worth $6.5 billion on an average day; [18] illegal substances and contraband can represent both economic and national security concerns. CPS help find these “needles in a haystack.”

Industry ↓	*Use-Case Examples* ↓
Manufacturing operations	Smart manufacturing systems, the industrial IoT or Industrie 4.0 initiatives: ■ CPS solutions help connect procurement, production, logistics, services and product delivery processes in real time to respond to rising labor and energy costs, environmental pollution or fast-changing market conditions.
Military/Aerospace	Smart weapon systems: ■ Whether it is remotely piloted aircraft/unmanned aerial vehicles (UAVs), increasingly powerful space assets, or 8 million lines of code for the F-35 fighter jet, CPS enable all modern weapon systems. Emerging aerospace systems: ■ Developments in UAV technologies in particular are occurring in the civilian and defense sectors at breakneck speed and producing an explosion of case studies on topics ranging from medical deliveries to counter-UAV technologies.
Automotive	Connected and autonomous vehicles: ■ Human error accounts for 93% of the approximately 6 million annual automotive crashes, [19] and 52% of casualties in combat zones are attributed to military personnel delivering food, fuel and other logistics. [20] CPS improve efficiency and safety in global transportation networks.

Industry ↓	*Use-Case Examples* ↓

Source: Gartner (November 2021)