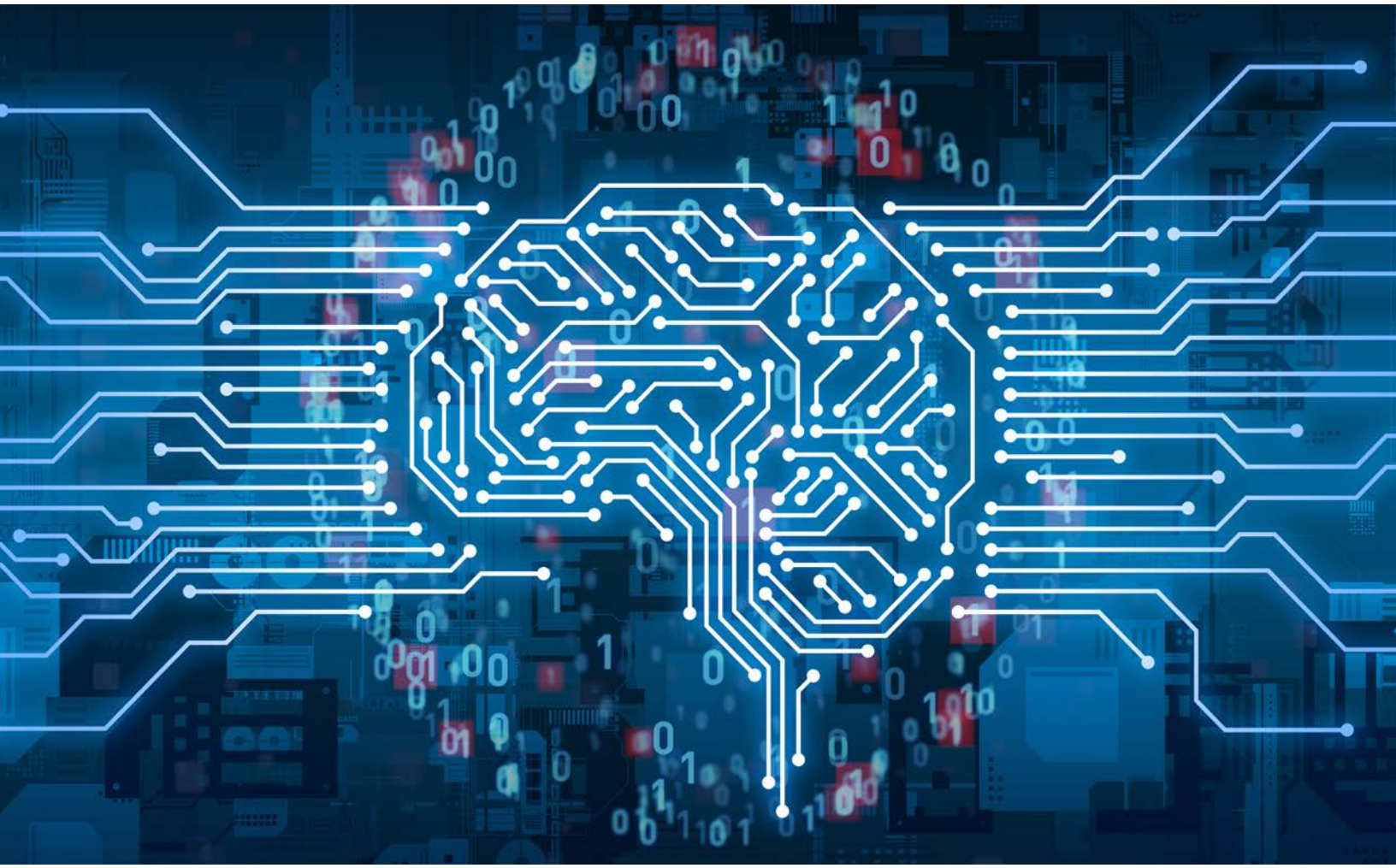
tyco

Whitepaper

Artificial Intelligence

Understanding its place in physical security



Johnson Controls

The AI market is growing

The Artificial Intelligence (AI) narrative has shifted from one that romanticizes a 'science-fiction' uprising to one where AI fuels real technologies and capabilities that enrich and improve human lives every day. In fact, IDC forecasts that spending on AI technologies will grow to US $97.9 billion in 2023—more than two and a half times the spending level of 2019.[1]

The truth is, AI has been at play for decades, deployed across a wide spectrum of use cases to solve business problems—from managing and automating IT infrastructure, and gleaning new insights about customers, to identifying and responding to cyber threats, and much more.

In physical security, more and more companies have been advancing their data-related capabilities and integrating AI into their business processes. In the coming years, AI will likely become even more pervasive. Just as mobile strategies have become just part of doing business, AI will soon become standard—maybe even faster than we expect. Results from a McKinsey Global Survey suggest that organizations are using AI as a tool for generating value and are planning to invest even more in AI in response to the COVID-19 pandemic to empower safer 'return to work' strategies.[2]

The great news is that tactical implementations of AI can likely be achieved through your business' existing security ecosystem.

Machine learning. Machine learning is a type of artificial intelligence where a technology is able to learn, by being programmed with defining criteria, and to alter its algorithms as it learns more about the data it is processing. As applied in the physical security industry, machine learning is often used to distinguish normal behaviors from suspicious behaviors.

Deep learning. Considered a subset of machine learning, deep learning technology, based on artificial neural networks, learns through exposure to massive amounts of data. The more data that the program receives, the more intelligent the deep learning algorithm will be. Cutting-edge security systems apply deep learning to differentiate everything from people, animals, vehicles, and static objects to weather conditions and the time of day.

Natural language processing. NLP is the ability to extract or generate meaning and intent from text in a readable, stylistically natural, and grammatically correct form.

Computer vision. Computer vision is the ability to extract meaning and intent from visual elements, whether characters (in the case of document digitization) or the categorization of content in images and videos, such as faces, objects, scenes, and activities.

Source: Deloitte

AI in the context of physical security

At its annual "Securing New Ground" conference, the Security Industry Association (SIA) identified artificial intelligence as #1 in its top 10 megatrends that will define physical security in 2021. It's easy to understand why.

Data is the fuel that feeds AI, and security systems gather LOTS of information. Video cameras and access control sensors record huge amounts of data that can be used to advance machine learning and make systems and devices smarter. This resulting torrent of data is too massive for human analysts to make full use of. Artificial intelligence helps solve this problem.

Video analytics turn insights into action

Video analytics start with the collection of surveillance video from as many vantage points as possible. In many cases, that information is analyzed by human analysts with the help of technology that can "see" in ways that humans can't. This kind of technology is often highly sophisticated, but that doesn't necessarily mean it is employing artificial intelligence.

True artificial intelligence goes beyond mere data collection and analysis and **detects patterns** not only from the data it collects and the analysis it conducts, but also from other various historical data so it can make inferences about the present, predictions about the future, and connections between seemingly unrelated events.

Deep-learning AI analyzes footage and detects anomalies in real-time, supplementing and enhancing a security workforce who can only absorb and process data so quickly. In the time that it takes for a human to identify and label an image, an AI algorithm can classify one million images.[3]

Top 10 physical security megatrends:

1. Artificial intelligence
2. Cybersecurity of physical security
3. Predictive data analytics
4. Connectivity and the IoT of everything
5. Cloud computing
6. Touchless and frictionless solutions
7. Facial recognition
8. Responsive environments and intelligent spaces
9. Emphasis on data privacy
10. Move to service models

Source: Security Industry Association

tyco | AI

Combining AI and video analytics

By simply allocating a license to a camera, a victor/VideoEdge video management system will immediately begin collecting behavioral metadata, reporting key performance indicators, and triggering real-time alarms.

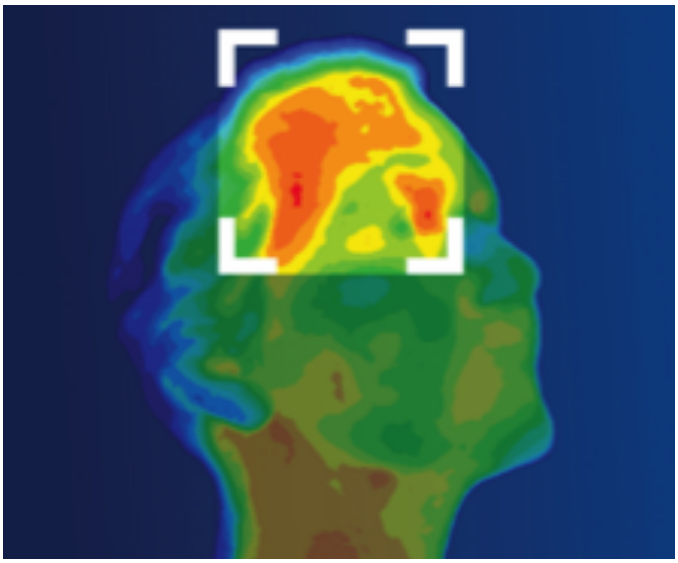
Johnson Controls

Timely uses of AI-powered security solutions

Because of what we've learned during the pandemic, wearing face coverings may become standard operating procedure as the first line of defense to support a healthy workplace. In busy environments, it can be difficult to monitor who does or does not have a face covering – at least without a little help from AI:

- Video management systems employ AI for powerful face mask detection to help mitigate breaches in protocols
- Intelligent searches powered by AI enables rapid location of individuals by searching by appearance across many cameras
- AI algorithms let you create virtual borders that count people entering and exiting a defined area to enforce occupancy limits and social distancing
- Thermal cameras that scan for elevated skin temperatures as people access a building to ensure no one entering has a fever – the most common symptom of illness

exacqVision video management system offers a face mask detection feature that is easy to implement with cameras you may already have in place.



Illustra Pro Thermal EST cameras can measure skin temperatures with a ±0.2°C / 0.4°F accuracy tolerance at an effective distance of 1 to 2 meters (3.3 to 6.6 feet).

Applying AI to access control solutions is also trending, especially in the current healthcare crisis where there is widespread concern about virus exposure and spread. In a growing market that is transforming from a hardware-centric approach to intelligence focused, there is increasing demand to remove 'friction' from the user experience.

AI empowers fast and reliable facial recognition that allows you to seamlessly grant or deny access to restricted areas without cards or mobile credentials to support better hygiene and freedom of movement. AI-empowered facial recognition can simultaneously recognize and make decisions about multiple faces in the camera's field of view while utilizing anti-spoofing technology to authenticate identity – discerning high-resolution images designed to 'trick' the system.

The cloud is essential for implementation and management of AI solutions

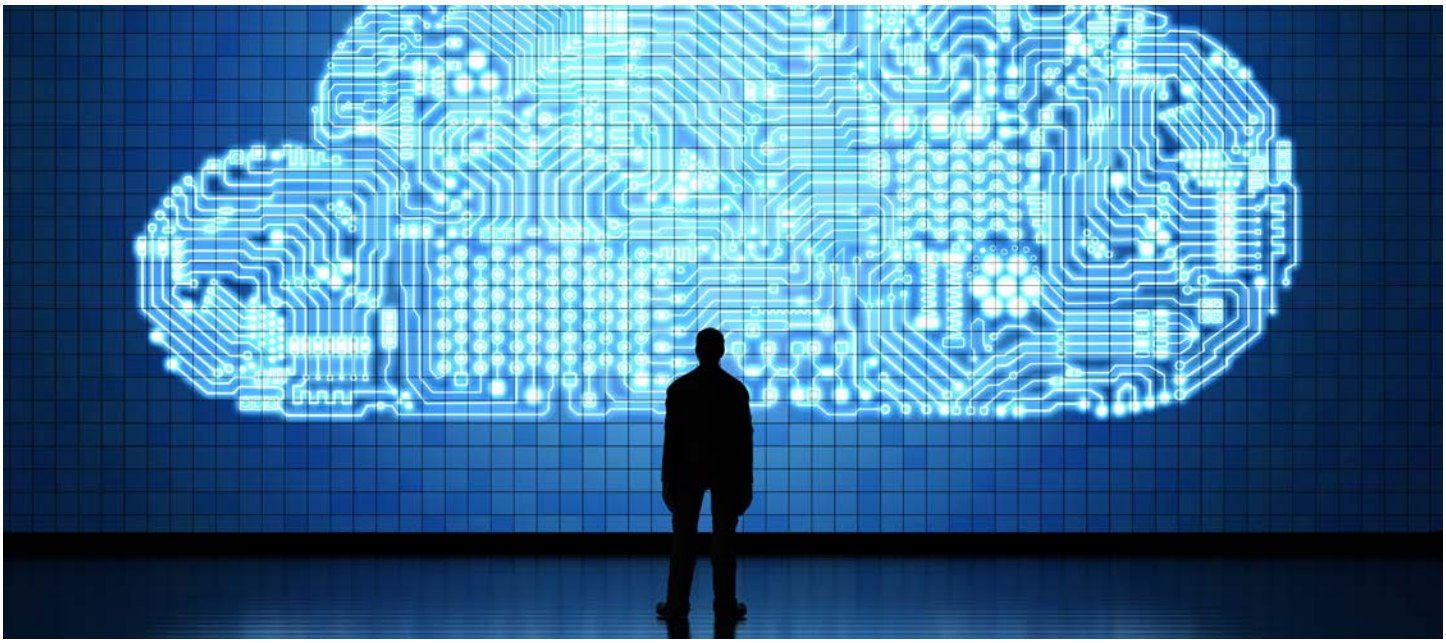
One of the major challenges with developing deep learning-based applications is access to real-word data and the ability to train the applications to work in any environment. Cloud-based solutions provide a significant advantage as they allow for continuous updates and easy collection of vast amounts of data, while also centralizing the management of an entire security system in one interface.

Facial recognition employing AI

Whether combined with Illustra Insight, or used with existing IP cameras, Tyco AI provides fast and reliable facial recognition.

- 99.7% accuracy with low-to-no False Acceptance Rates
- Hardened against cyber threats
- Uniquely designed to protect personally identifiable information (PII)

Cloudvue from Johnson Controls simplifies surveillance, streamlines access control, and provides powerful intelligence that improves security operations and helps with organizational efficiency.



Johnson Controls

Common misconceptions of AI

Even with enthusiasm for AI growing, there remain reservations. While cybersecurity tops the list of potential adopters' most worrisome AI risk, these other common misconceptions can slow or stop implementation of AI technologies in security.

Misconception #1: No humans will be needed and AI will take away jobs

AI-based systems remain dependent on humans. While AI is good at processing data, it is bad at thinking in abstract, applying common sense, or transferring knowledge from one area to another.

Humans can invent new things, including all the technologies that have ushered in the era of artificial intelligence. AI can only take that data, compare it, come up with new combinations and presentations, and predict trends based on previous sequences.

As far as the fear that AI will take away jobs, it is estimated that just 8% of companies plan on using AI-based systems to fill roles.[4] AI is more likely to create new jobs, as it frees humans up to design and develop new products and business.

Misconception #2: AI is dangerous and threatens privacy

Machine learning models are not inherently 'dangerous'. Most AI-systems can still only follow instructions, such as solving a specific problem or analyzing historical data. In physical security, protecting personally identifiable information (PII) in solutions such as facial recognition technology has been a subject of great debate because of concerns about how to balance the demand for security with the importance of privacy. But technology has come a long way and well-architected solutions offer nearly infallible protection of PII and against cyber threats:

- No data or PII is stored in the device
- No Ethernet accessibility to the public
- Designed with cyber protection and data encryption
- Enhanced with anti-spoofing liveness detection

Misconception #3: It's not natural and you can tell the difference between AI and human-powered interactions

Many people are surprised to learn that AI is already being used to write financial news, sports stories and weather reports. Unfortunately, AI is also producing "deep fake" videos that feature computer-generated faces that some people think are real – which naturally is fodder for the notion that AI is dangerous. This is why anti-spoofing liveness detection in AI-powered solutions is so important.

	Human Intelligence	Artificial Intelligence
Energy Efficiency	25 watts with human brain	2 watts for modern machine learning machine
Universal	Humans usually learn how to manage hundreds of different skills during their life	While consuming kilowatts of energy, this machine is usually designed for a few tasks
Multi-tasking	Humans can work on multiple responsibilities	The time need to teach a system each task is considerably high
Decision Making	Humans can learn decision making from experienced scenarios	Even the most advanced robots can barely compete in decision mobility
State	Brains are analogue	Computers are digital

Well-architected AI solutions enhance human intelligence

We've been working alongside AI solutions for decades, and we will continue to enjoy the benefits of AI embedded across business applications. In fact, a staggering 80% of midsize companies intend to increase their annual AI investments.[5]

Understanding what AI is and what it is not plays an essential role in helping a business clearly define where AI can help increase value:

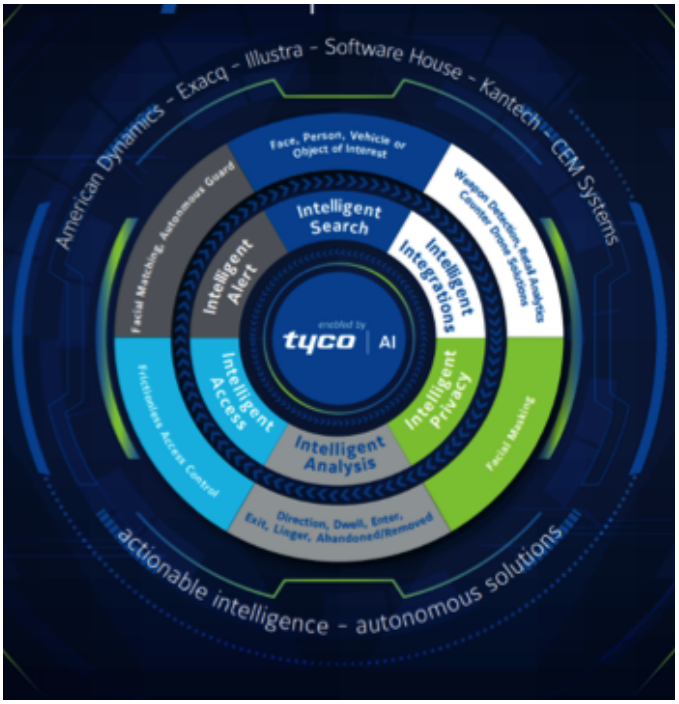
- **Automate** a process or function that would normally be done by a human
- **Optimize** the efficiency of a process or function
- **Enhance** the ability of individuals to accomplish tasks or enable them to do something they typically could not

In physical security, using AI solutions from a single provider can ensure easier adoption of future modules, quicker upgrades to newer technologies, and faster reactions to situations human intelligence simply can't anticipate.

A growing number of organizations are tackling AI-related risks head-on:

- Bank of America has embraced the approach of collaborating on AI ethics. It has also created a new role—enterprise data governance executive—to lead AI governance for the firm and collaborate with the chief risk officer on AI governance.
- Robert Bosch GmbH, which plans to embed AI across its products by 2025, is training 20,000 executives and software engineers on the use of AI, including a recently developed AI code of ethics.
- Workday, a provider of cloud-based enterprise software for financial management and human capital management, has committed to a set of principles to ensure that its AI-derived recommendations are impartial and that it is practicing good data stewardship.

Source: Deloitte's State of AI in the Enterprise, 3rd Edition



Johnson Controls

References

1. International Data Corporation. Worldwide Artificial Intelligence Systems Spending Guide, September 4, 2019. https://www.idc.com/getdoc.jsp?containerId=prUS45481219
2. McKinsey and Company. The state of AI in 2020. November 17, 2020. https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/global-survey-the-state-of-ai-in-2020
3. EDUCBA. Artificial Intelligence vs Human Intelligence. https://www.educba.com/artificial-intelligence-vs-human-intelligence/
4. Lionbridge AI. 5 Common Misconceptions About Artificial Intelligence. June 10, 2019https://lionbridge.ai/articles/5-common-misconceptions-about-artificial-intelligence/
5. Deloitte. Thriving in the era of pervasive AI. Deloitte's State of AI in the Enterprise, 3rd Edition. July 14, 2020. https://www2.deloitte.com/us/en/insights/focus/cognitive-technologies/state-of-ai-and-intelligent-automation-in-business-survey.html

About Johnson Controls AI solutions

Tyco AI is an ever evolving, deep learning solution from Johnson Controls infusing Artificial Intelligence into the Tyco security technology portfolio. With these new capabilities, Tyco AI provides a new, more autonomous approach to alerts, searches, privacy and access, leveraging a facility's surveillance infrastructure and reducing the need for operator intervention. Enabled by the powerful algorithms in Tyco AI, object classification and behavior and facial recognition analytics become exponentially faster and more accurate, enabling the industry-leading suite of Tyco's automation solutions for access control and video surveillance to produce critical and customizable operational intelligence data for nearly any customer application.

About Johnson Controls

Johnson Controls is a global diversified technology and multi-industrial leader serving a wide range of customers in more than 150 countries. Our 120,000 employees create intelligent buildings, efficient energy solutions, integrated infrastructure and next generation transport systems that work seamlessly together to deliver on the promise of smart cities and communities. Our commitment to sustainability dates back to our roots in 1885, with the invention of the first electric room thermostat.

For additional information, please visit www.swhouse.com or follow us on Facebook, Twitter, and LinkedIn.

AD1318-WP-202105-R01-HS-EN