

2024 CONVENING OF THE COUNCILS REPORT

EVOLVING TECHNOLOGIES: CHALLENGES AND SOLUTIONS



CONTENTS

03 FOREWORD

07 INTRODUCTION

10 EXECUTIVE SUMMARY

12 SYNTHESIS AND ANALYSIS

20 INDUSTRY SPOTLIGHTS

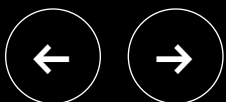
27 MARKET INSIGHTS
29 FIRE 36 ELECTRICAL 43 SECURITY

50 KEY INSIGHTS AND FINDINGS

84 RECOMMENDATIONS
AND CONCLUSION

86 METHODOLOGY

93 ACKNOWLEDGEMENTS





FORERWORD





It is not possible to give a definition of artificial intelligence (AI) because there isn't one and only one, but there are multiple AIs. When the pioneers of the field chose this name in the mid-50s, they believed, in their enthusiasm, that they could describe and imitate mathematically the functions of a neuron, then that of a neural network and, by extrapolation, make an artificial human brain that could then reproduce one of its abilities,

“intelligence.”

Apart from the fact that we could not then — or even today — agree on what “intelligence” really is, it would certainly have been more relevant from the beginning to use the terms “machine learning” (ML) or “expert system,” which describe much better the mechanisms used over the last 70 years and would have had the advantage of not making us fantasize about what the words “artificial intelligence” can mean.

AI is often not what the media, thriving on sensationalism for the past 20 years, has described, and even less what appears in Hollywood movies that present us with terrifying scenarios like in “Terminator,” or a certain idea of happiness like in “Her.”

AI is not part of the world of science fiction; it is science.



FOREWORD

If we really had to give a single definition that would allow us to better understand the subject, we could say that AI is nothing more than a toolbox — a toolbox that contains multiple, varied and specialized tools. Just as we will find a hammer, a screwdriver or a saw in a classic toolbox, we will find in AI tools as varied as speech recognition, music generation or the detection of cancerous tumors in medical images.

Like a hammer that can be used wisely to drive a nail or unwisely to drive a screw, an AI will be much more efficient — and perhaps much better than a human — to accomplish the task for which it was developed. That’s the very definition of a tool, but it could also be potentially very dangerous if used in another context. However, as with all tools, no matter how powerful they are, we are the ones who control them and decide how to use them.

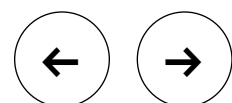
Recently, new tools have appeared, made available to everyone thanks to a particularly simple user interface — a “prompt” — where you can type your query of choice using everyday language. These are generative AIs, popularized by ChatGPT. Let’s stop for a moment to

make a point of vocabulary here, too. As much as using AI was, as we have seen, not very relevant, now that AI has entered the common language and we can hardly escape it, describing these new tools as “generative AIs” is, on the other hand, an excellent choice.

The mistake would have been to call them, as some do, “creative AIs,” because these AIs generate, but do not create anything. Creativity remains on the side of the human, on the side of the prompt or the means that are offered to us to interact with these generative AIs. Indeed, these AIs have become multimodal; that is to say that they can now be made to ingest not only text but also images, videos and music, and, in return, they can generate any of these media, but the texts that are presented to them — the series of images given as an input — are chosen by us. We are the ones who will say, “Draw me a green cow climbing the Eiffel Tower.” We will have created this image in our head, and the generative AI will offer us results, often different from the mental image we had of it but which will allow us to quickly refine the prompt again and again until it looks like what we had imagined.

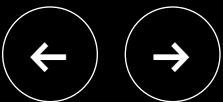
These generative AIs are as powerful as those that have been developed for decades; they are perhaps more powerful because of their ease of access and use, and therefore are potentially dangerous because they can generate “anything.” It’s easy to make up stories, fake news, deep fakes — those photos and videos that look so real — but also sometimes — often — they are just wrong because their *raison d’être* is to generate something, not to generate something true.

It would be useless to ban them; on the contrary, we must study them, learn how to use them, understand the strengths and weaknesses of these technologies, and collectively define their limits. This will undoubtedly involve new laws and regulations, which will also imply some educational virtues and ethical behaviors. It is for all these reasons that studying the risks and challenges of these emerging technologies is necessary to sharpen our critical sense and not be caught off guard in the wake of these multiple AIs that will continue to develop.





EMPOWERING
SCIENCE.
INSPIRING
PROGRESS.





INTRODUCTION

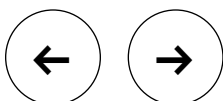
The Convening of the Councils (CoC) serves as a pivotal forum where UL Solutions, in tandem with UL Research Institutes and UL Standards & Engagement, brings together diverse advisory councils to collaboratively address emerging safety challenges.

On Monday, Nov. 11, 2024, the CoC gathered to address a variety of topics related to advancements in technology, exemplifying the three UL organizations' commitment to leveraging collective expertise to advance public safety in an era of rapid technological innovation.

The primary objective of the CoC is to foster interdisciplinary dialogue among experts from various sectors, including government agencies, regulatory bodies, academic institutions and industry organizations. This collaborative approach enables UL Solutions to anticipate and respond to safety concerns arising from new products and technologies, helping to ensure that safety standards evolve in tandem with innovation.

UL Solutions takes pride in its 130-year legacy committed to safety science — a legacy that has been at the forefront

of the evolution of emerging technologies. For over 110 years, we have convened industry councils across fire, security and electrical sectors, all with a singular goal: helping to ensure the safety of people and their property through science and collaboration. The inaugural Council of Underwriters Laboratories convened on June 8, 1911, marking the beginning of a structured approach to safety science collaboration. Over the years, these councils have played instrumental roles in shaping safety standards across various domains, including electrical systems, fire safety and consumer products. This unwavering commitment to “Empowering Science, Inspiring Progress” is not just a theme, but a guiding principle that will continue to steer our efforts as we navigate the complexities and possibilities that emerging technologies bring.





The CoC today encompasses several specialized councils, each focusing on distinct areas of safety science:

Electrical Council

Established in 1913, this council advises on safety considerations related to electrical systems and technologies. Its membership includes code authorities, independent experts, federal government officials and insurance representatives.

Fire Council

With a history spanning over a century, the Fire Council provides guidance on fire suppression equipment, building designs and materials. Members comprise academic experts, building officials, federal agencies, fire service members, independent fire safety experts and insurance industry representatives.

Security Council

Formed in 1921, this council focuses on safety considerations related to security and property protection products. Its membership includes representatives from the insurance industry, law enforcement, corporate security, the federal government and academia.



During the Nov. 11 convening, titled “Evolving Technologies: Opportunities and Challenges,” the agenda for discussion dove deeply into the world of technology innovation. The discussions help shape how our industry can collectively address the evolving risks posed by new technologies while capitalizing on their benefits.

In an era of remarkable technological advancement, the fire, security and electrical sectors face unique opportunities and complex challenges. They operate within a rapidly evolving landscape of emerging technologies, spanning AI, the Internet of Things (IoT) and advanced sensor technologies. These products and systems require interoperability and mitigate the cybersecurity risks associated with more connected ecosystems; this promises to revolutionize how we enable routines and protect people’s lives and property. Yet, these innovations also introduce new vulnerabilities and place new demands on the products, work force, regulatory frameworks and system architecture within industries.





The code authorities and industry professionals, who are the backbone of the standards that help safeguard our communities, play a pivotal role in addressing the challenges posed by emerging technologies. Their importance has never been more pronounced as they navigate the demands of technological advancements while upholding robust safety protocols in an increasingly interconnected and digital world.

The onus of the CoC meeting was simple: to test the hypothesis that the rapid evolution of technologies in the fire, security and electrical industries introduces both unprecedented opportunities and significant challenges. To address them holistically requires a comprehensive strategy that involves real-time adaptation, cross-sector collaboration and proactive regulatory alignment. UL Solutions' goal is to empower the next generation of safety standards, leveraging science and technological advancements to inspire progress and help protect the communities we serve.

This report captures the dynamic conversations and forward-looking insights co-created and curated during the CoC, with the intention of shaping a future where innovation and safety go hand in hand.





EXECUTIVE SUMMARY

In a world where technological advancements are evolving at breakneck speed, the 2024 CoC provided a unique platform to confront a critical question:

How can industries harness the transformative power of innovation without compromising safety, sustainability and ethics?

This year's theme, "Empowering Science, Inspiring Progress," reflects our commitment to advancing safety science and innovation in an increasingly interconnected world.





Key insights from the CoC highlight the transformative potential of emerging technologies such as AI, IoT and digital twins, while underscoring the urgent need for sustainable practices and adaptive regulatory frameworks. By convening diverse stakeholders — including industry leaders, academic experts, government representatives and regulatory bodies — the CoC has produced actionable strategies for helping to ensure safety and resilience in a rapidly changing technological landscape.

Major insights and themes

Harnessing emerging technologies

AI, IoT and digital twins are reshaping industries by enhancing predictive maintenance, real-time monitoring and operational efficiency. However, their adoption requires careful management of cybersecurity risks and system interoperability.

Building resilience and sustainability

The environmental impact of energy-intensive technologies, such as AI and IoT, looms large. Energy-efficient solutions, modular nuclear reactors and sustainable designs are critical for reducing the environmental impact of new technologies, aligning innovation with ecological stewardship and scalability.

Adaptive governance and standardization

The rapid pace of innovation demands dynamic, harmonized regulatory frameworks. Collaborative efforts are vital for aligning safety standards with global technological trends.

Democratizing access to knowledge

The promise of innovation is diminished when access is inequitable. The CoC underscored the importance of affordable, centralized and scalable training platforms to equip professionals across all sectors with the skills they need to adapt and thrive in this new era.

Ethical considerations in technology

Technology does not exist in a vacuum. As tools like AI become integral to decision-making, industries face ethical dilemmas around privacy, misinformation and equity. Embedding ethical frameworks into the design and deployment of these technologies will be essential.

Call to action

The CoC’s findings emphasize a collective obligation to innovate responsibly and inclusively. By aligning technological advancements with rigorous safety standards, stakeholders can navigate the complexities of modern challenges while driving progress that benefits society at large.

The CoC also generated actionable recommendations for industry leaders. Collaboration across sectors must become the norm, not the exception. Centralized platforms for standards and training are urgently needed to reduce fragmentation. Sustainability must move from aspiration to mandate, and regulatory agility must rise to meet the challenges of a fast-moving world. Above all, ethical considerations must anchor every decision, ensuring that technology serves humanity, not the other way around.

This report serves as both a testament to the power of collaboration and a road map for future resilience. Dive into the chapters ahead to explore practical recommendations, groundbreaking case studies and visionary strategies shaping the future of safety science.



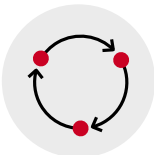
SYNTHESIS AND ANALYSIS

The 2024 COC synthesized critical insights from across the fire, electrical and security industries, combining expertise in emerging technologies, regulatory challenges and market trends.

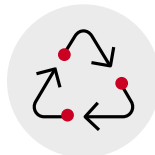
Five core themes emerged as pivotal for the future of these industries, informed by general session findings, notes and secondary research:



Harnessing emerging technologies to drive safety and efficiency



The interplay of regulation, standardization and innovation



Building resilience through sustainable practices



Democratizing access to training and standards



Addressing ethical and societal challenges of technology adoption

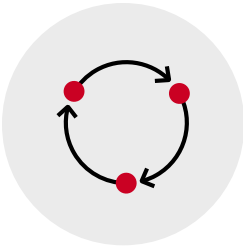


FIVE CORE THEMES



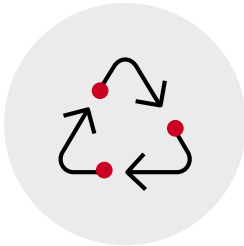
Harnessing emerging technologies to drive safety and efficiency

The adoption of AI, digital twins and IoT systems is transforming industries, offering enhanced safety, operational efficiencies and predictive capabilities.



The interplay of regulation, standardization and innovation

Agile, harmonized regulatory frameworks are essential to mitigate risks while enabling innovation. The growing complexity of technology demands global collaboration and adaptive governance.



Building resilience through sustainable practices

Industries must address the environmental impacts of energy-intensive technologies by prioritizing sustainable solutions like modular nuclear reactors and energy-efficient systems.



Democratizing access to training and standards

Accessibility and affordability of training, coupled with reliable information delivery, remain critical for broader adoption of safety protocols and best practices.



Addressing ethical and societal challenges of technology adoption

As technologies like AI and IoT scale, organizations must embed ethical considerations into their frameworks to manage data privacy, misinformation and equitable access.



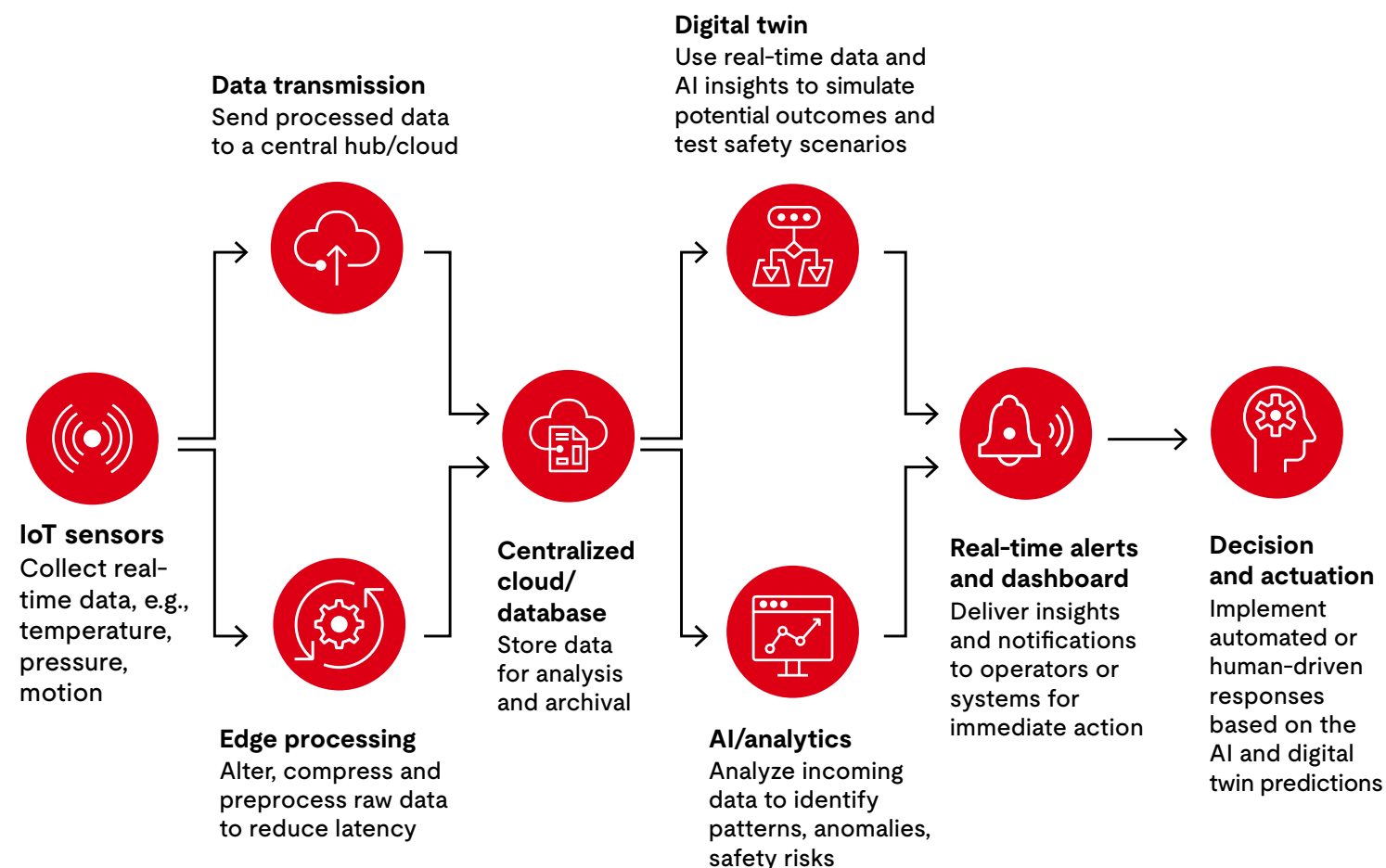
01

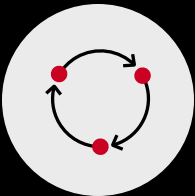
Harnessing emerging technologies to drive safety and efficiency

Key insight

AI, digital twins and IoT are reshaping industries by enhancing predictive maintenance, real-time monitoring and simulation capabilities. For instance, AI-enabled safety systems can identify anomalies faster than traditional sensors, while digital twins allow for realistic modeling of systems to preempt failures.

- **AI and automation** – AI is revolutionizing safety protocols by enabling predictive analytics, real-time monitoring and anomaly detection. For instance, smart cameras equipped with AI can identify safety risks and alert operators immediately.
- **Digital twins** – These virtual models allow industries to simulate and optimize operations before physical implementation. This is critical in sectors like energy, where digital twins enable predictive maintenance and mitigate system failures.
- **IoT integration** – IoT enhances data collection and sharing, providing a foundation for more intelligent safety systems. Examples include IoT-enabled fire safety sensors that provide real-time updates on environmental conditions.
- **Scalability and flexibility** – Emerging technologies offer scalable solutions to improve workflows and optimize resources across industries. Technologies like edge computing reduce latency and improve efficiency in data-heavy systems.



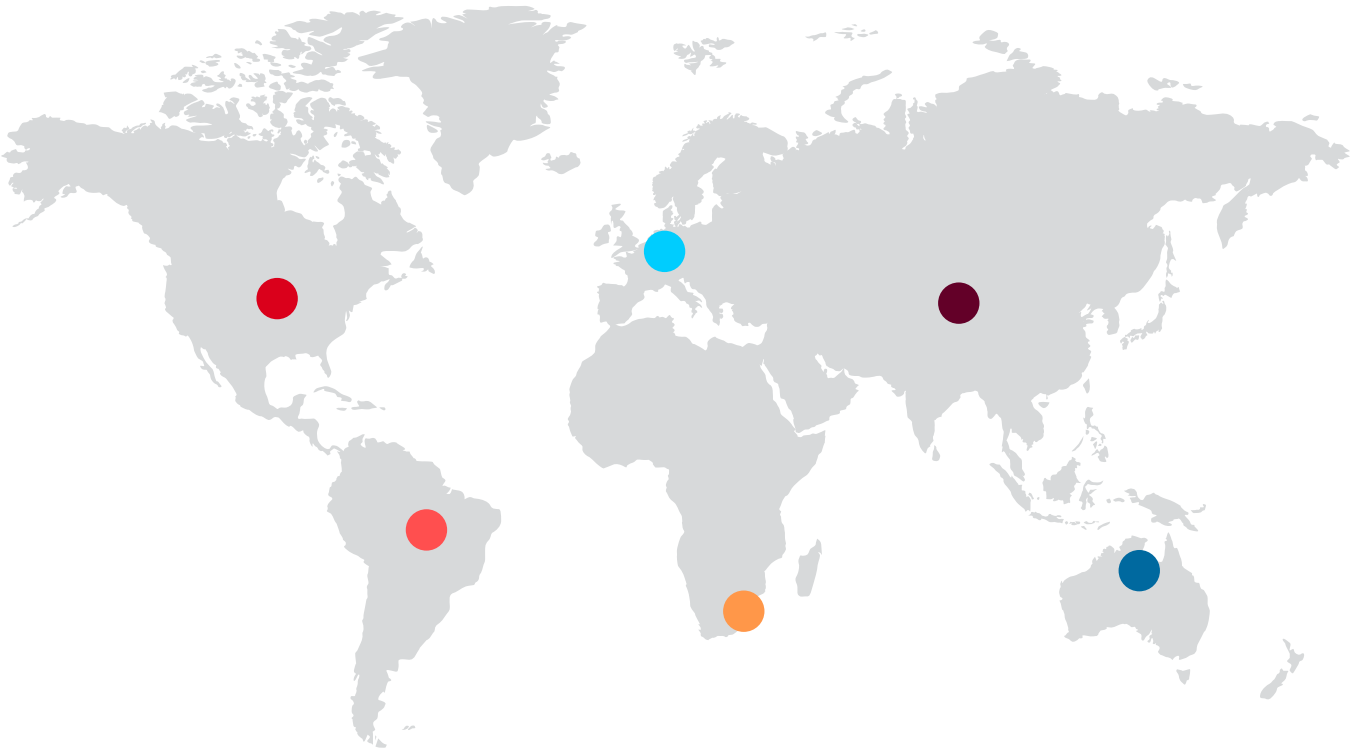


02

The interplay of regulation, standardization and innovation

Key insight
The rapid pace of technological advancement requires adaptive, harmonized regulatory frameworks. Initiatives like Outlines of Investigation demonstrate the value of dynamic approaches to address emerging challenges in AI and cybersecurity.

- **Dynamic standards** – As technology evolves rapidly, static regulatory frameworks are insufficient. More dynamic approaches, like Outlines of Investigation, allow for agile responses to emerging risks.
- **Global harmonization** – With differing regional standards — e.g., U.S. Cyber Trust Mark, EU AI Act — harmonization efforts are crucial for seamless technology adoption across borders.
- **Trial-based approaches** – Regulatory flexibility, such as permitting trial implementations, ensures that innovations can be tested and refined before large-scale deployment.
- **Industry collaboration** – Partnerships between developers, regulators and industry bodies help ensure that regulations support innovation while maintaining safety.



● **United States**
U.S. Cyber Trust Mark showcases adaptive and forward-thinking regulations

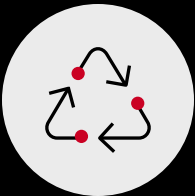
● **Europe**
The EU AI Act sets global standards for ethical and accountable AI use

● **China**
China's high-speed rail deploys advanced AI-driven systems to enhance passenger safety on the world's largest rail network

● **Brazil**
Brazil's Digital Transformation Strategy fosters innovation with secure citizen data practices

● **South Africa**
South Africa's Renewable Energy Independent Power Producer (IPP) program balances innovation with community safety

● **Australia**
Australia's National Road Safety Strategy advances cutting-edge technologies to reduce accidents

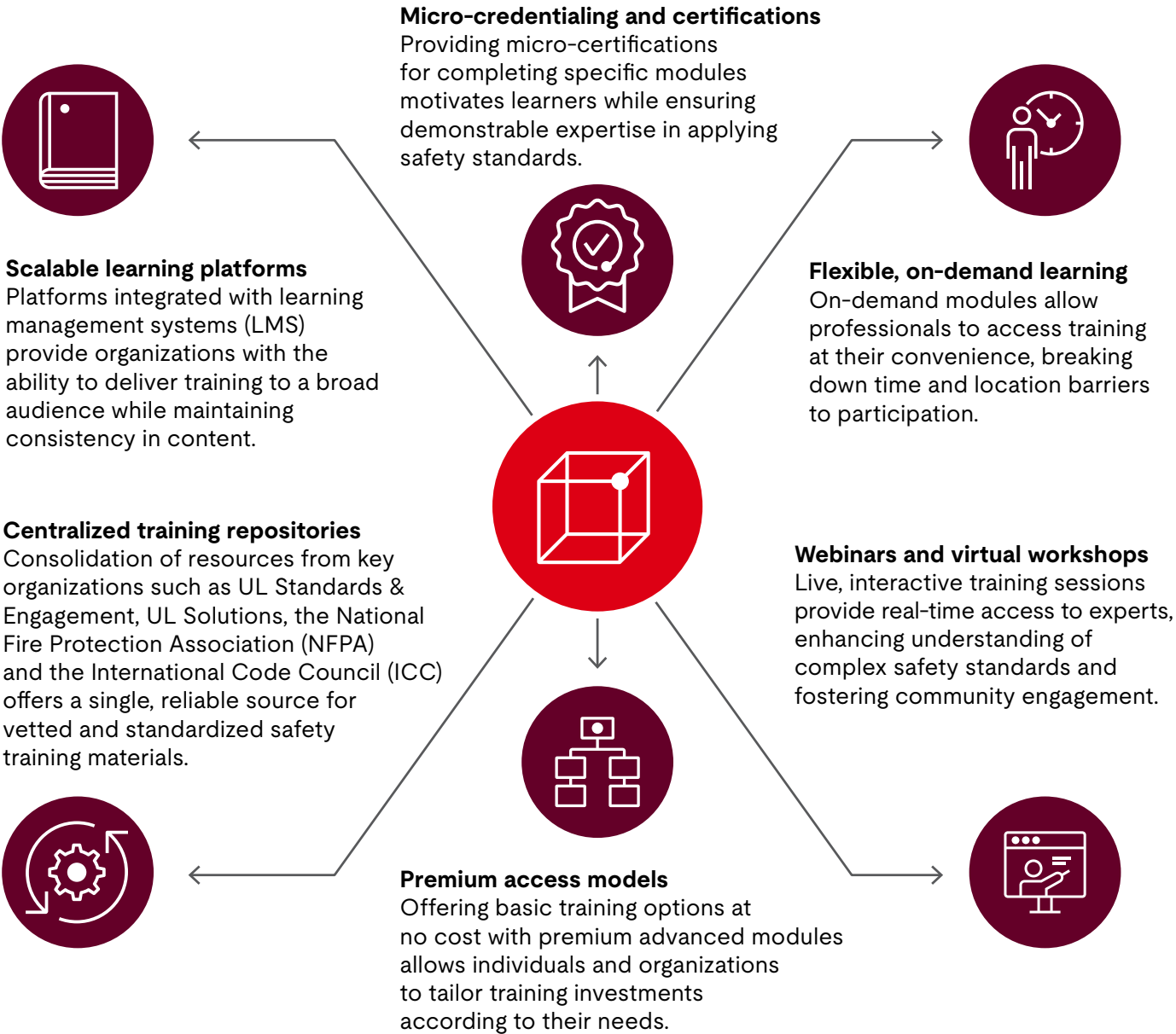


03

Building resilience through sustainable practices

Key insight
Sustainable energy solutions like modular nuclear reactors and energy-efficient edge computing are essential for mitigating the environmental impact of AI and IoT deployment. For example, switched-mode power supplies (SMPS) provide scalable energy without significant carbon emissions.

- **Energy demands of AI and IoT –** Technologies like AI require significant energy resources. Sustainable solutions such as SMPSs and edge computing are critical for managing environmental impacts.
- **Focus on efficiency –** Frugal models and energy-efficient systems can help industries reduce their carbon footprint while maintaining operational capacity.
- **Sustainable energy deployment –** Integrating renewable energy systems with advanced safety protocols helps ensure resilience and compliance with environmental regulations.
- **Circular design principles –** Companies must prioritize sustainability in product design and life cycle management to reduce waste and enhance long-term usability.



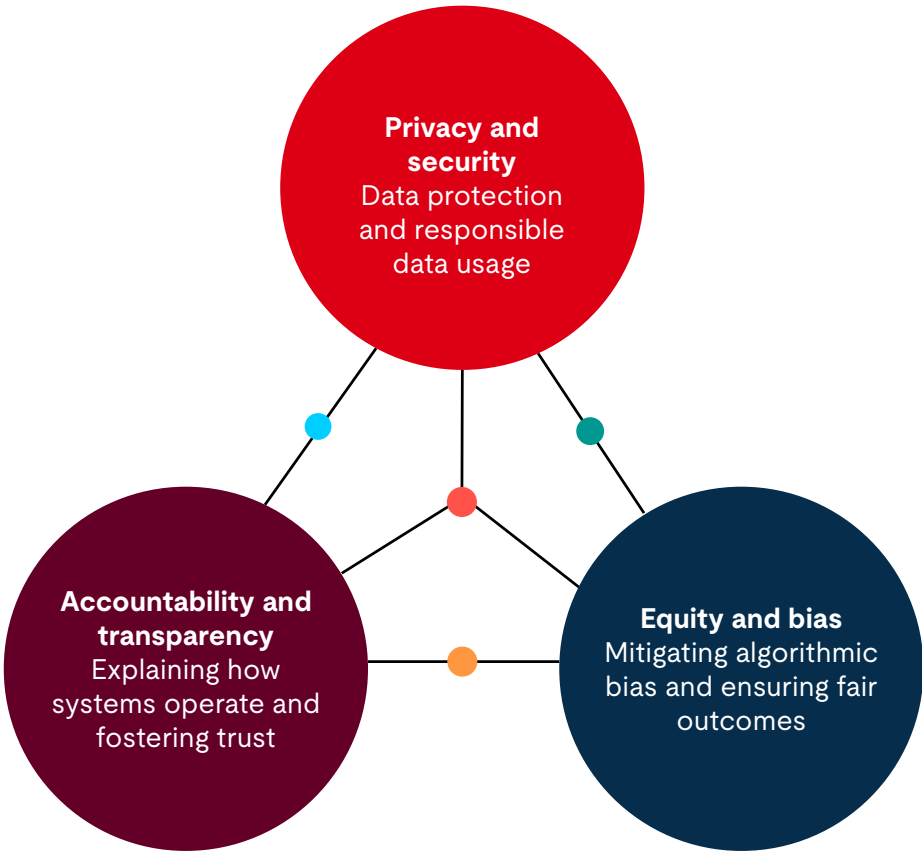


04

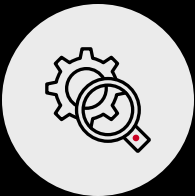
Democratizing access to training and standards

Key insight
Cost-effective and scalable training platforms that integrate into learning management systems can help ensure that professionals at all levels understand and implement safety standards effectively. Standardized, vetted resources are critical to reducing misinformation.

- **Accessibility** – Cost-effective and scalable training options are essential to bridge gaps for small and medium enterprises (SMEs) and under-resourced sectors.
- **Centralized platforms** – Consolidating training resources from organizations like the three UL organizations, NFPA and ICC enhances accessibility and consistency.
- **Focus on relevance** – Training must address specific challenges and provide practical, actionable insights, such as clarifying misunderstood code changes or their implementation.
- **On-demand learning** – Flexible, on-demand modules enable professionals to learn at their convenience, reducing barriers to participation.



- **Accountability and privacy**
Trust-building through transparent and secure data use outcomes
- **Ethical AI adoption**
A balanced integration of privacy, equity and accountability to ensure socially beneficial technology outcomes
- **Privacy and equity**
Responsible AI frameworks that protect data while minimizing bias
- **Equity and accountability**
Clear communication about fairness and ethical AI deployment



05

Addressing ethical and societal challenges of technology adoption

Key insight
Ethical AI deployment is critical to addressing challenges like bias, data privacy and misinformation. Organizations like UL Solutions are actively shaping frameworks to help ensure responsible adoption of these technologies.

- **Data privacy and security** – Technologies like AI raise concerns around data use and protection. Robust frameworks are needed to manage these risks responsibly.
- **Misinformation and bias** – AI systems must be designed to minimize bias and prevent the spread of misinformation, particularly in critical applications like safety and security.
- **Accountability and transparency** – Clear communication about how technologies operate is essential for building trust among stakeholders.
- **Ethical governance** – Embedding ethical considerations into the development and deployment of technologies ensures equitable and socially beneficial outcomes.

Applied sustainable practices in:	Before	After
Battery manufacturing	Lithium-ion batteries lacked robust end-of-life protocols, leading to environmental harm and safety issues during disposal.	Current standards now include solid-state batteries with enhanced safety features, longer life cycles and advanced recycling programs for material reuse.
Smart home devices	IoT devices consumed significant standby energy and were prone to cybersecurity vulnerabilities, increasing risks of energy waste and data breaches.	Current smart home devices incorporate edge AI for efficient data processing and on-device cybersecurity protocols, reducing both energy use and risks.
Building materials	Traditional concrete and steel production were energy-intensive, contributing significantly to carbon emissions.	Innovations like carbon-negative concrete and 3D-printed building materials reduce emissions while enhancing structural safety and resilience.
Renewable energy	Early renewable systems lacked integration with energy storage, leading to inefficiencies and downtime during peak demand.	Certifications now cover renewable systems integrated with advanced battery storage and microgrid technologies, supporting a consistent and safe energy supply.



SYNTHESIS AND ANALYSIS

Conclusion

Several themes central to advancing industry resilience, innovation and ethical governance emerge that will help guide all stakeholders toward sustainable growth and global alignment. As the industry landscape evolves, the following points encapsulate the core findings, offering a foundation for continued discovery, excellence and adaptability.

Key differences across industries

- Fire safety**
Focuses heavily on integrating IoT sensors and advanced suppression systems to improve detection and response
- Electrical**
Prioritizes industrial IoT and sustainable energy solutions for long-term growth
- Security**
Leverages AI for advanced surveillance and predictive analytics to enhance threat mitigation

Implications for stakeholders

- Invest in adaptable regulatory frameworks**
Align safety and innovation through collaborative governance models.
- Prioritize sustainable development**
Adopt energy-efficient practices to balance technological growth with environmental stewardship.
- Expand training accessibility**
Democratize access to affordable, reliable training to build capacity across the work force.

Future trends for 2025 and beyond

- AI-powered decision support**
Increased reliance on AI for real-time analytics and risk management
- Global standardization efforts**
Accelerated initiatives to harmonize safety and cybersecurity standards
- Sustainability as a mandate**
Industry-wide adoption of green technologies to meet regulatory and social expectations

By addressing these themes, councils will help ensure that industries remain resilient, innovative and aligned with the needs of a rapidly evolving world.



INDUSTRY SPOTLIGHTS

SIEMENS





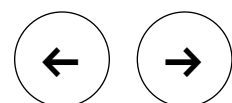
SPOTLIGHT

SIEMENS

Technology to transform the everyday, for everyone

Since 1847, Siemens has turned great inventions into innovative technologies and risen to the challenges of the day, transforming everyday life for people all around the world.

Siemens first began supporting U.S. customers more than 160 years ago, and today, the United States is the company's largest market. Siemens' technology is everywhere, supporting the critical infrastructure and vital industries that form the backbone of America's economy, from more agile and productive factories to more intelligent, resilient buildings and power systems and more reliable and sustainable transportation.



Great partnerships lead to a great future.

“The process of invention is useful and clearly successful only when it is closely linked to production for the purpose of solving today's problems.” (Werner von Siemens, 1886)

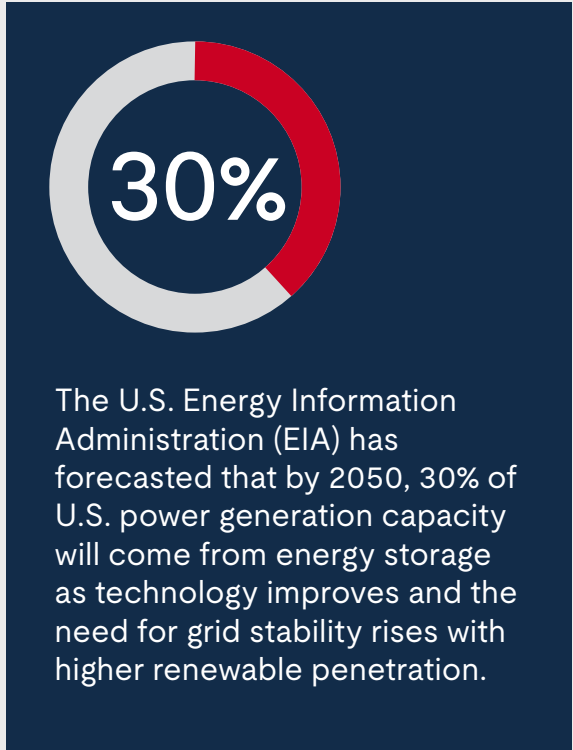
For 60 years, UL Solutions has supported Siemens with cutting-edge insights and world-class safety science expertise. From the first UL Certified Siemens industrial control equipment in 1964 to the first certification using digital model and simulation granted to Siemens in 2024, tens of thousands of its fire, electrical and automation products have been made safer, more secure and more sustainable with the support of UL Solutions.





A changing world

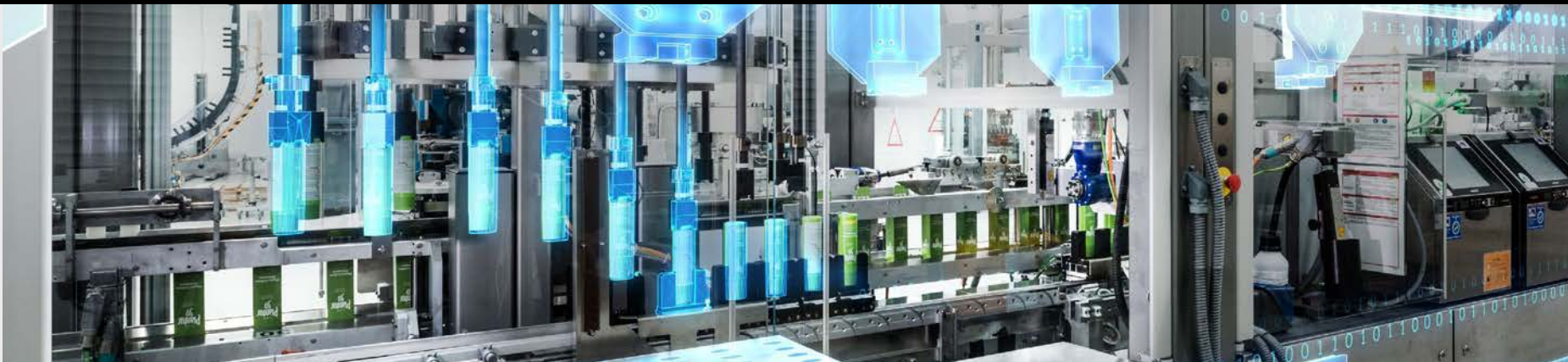
 **300 TWh** increase in U.S. electricity demand by 2030 (source: Rystad Energy)



72%
of companies have adopted AI in at least one business function (source: McKinsey)

8 million
manufacturing jobs will be unstaffed by 2030 (source: Korn Ferry)

20 billion
IoT endpoints in global manufacturing; growing by 16% per year (source: IOT Analytics)

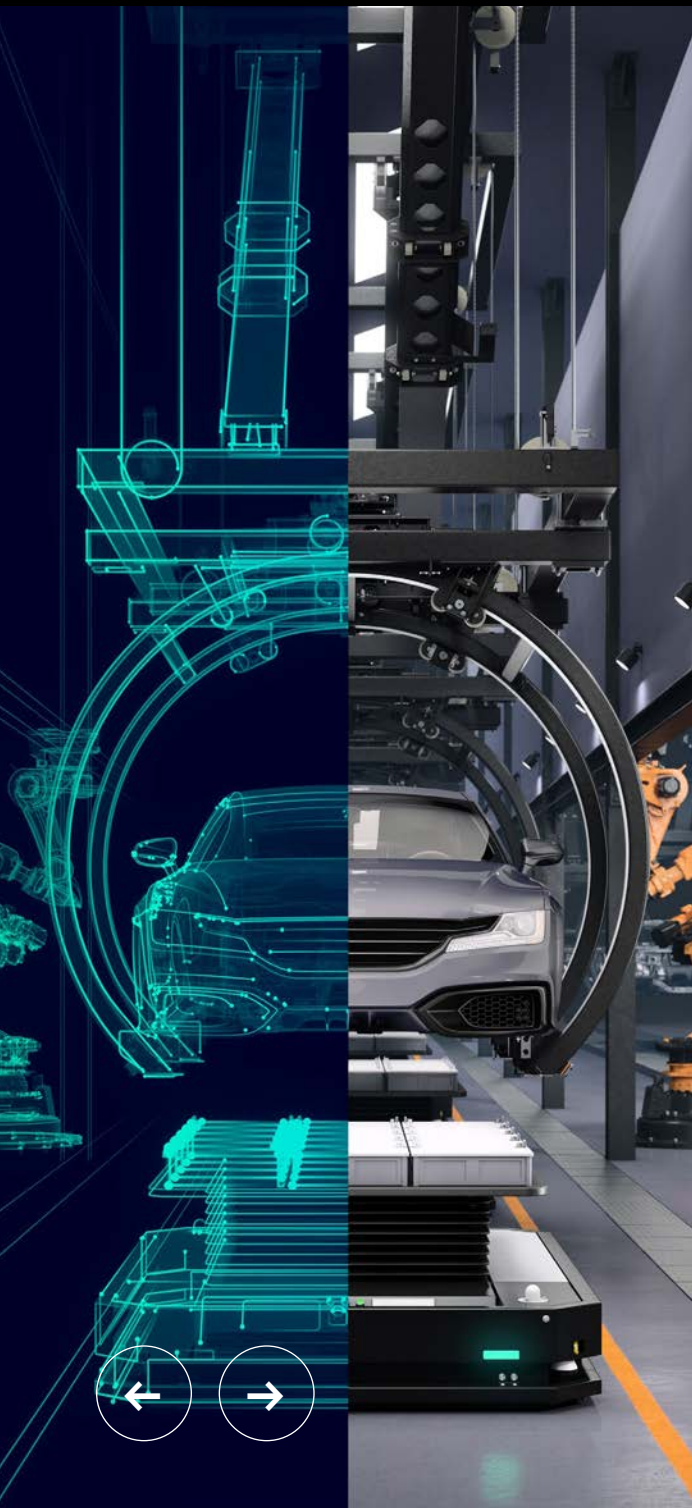


Trends in buildings and infrastructure

Reliable, safe and secure power and building infrastructure is not new. What is new is the incredible and insatiable demand for it. Over the last few years, AI and digitalization have surfaced in abundance, requiring more data centers and semiconductor manufacturing — both energy-intensive industries. Sustainability and federal policies are generating a supercycle of battery and electric vehicle factories and electric mobility infrastructure. This, along with the overarching transition to cleaner energy, has many sectors moving away from fossil fuels toward electrification. In turn, the electrification of everything is very much becoming more a reality than a pipe dream.

Trends in industrial manufacturing

Manufacturers have always faced productivity, cost, quality, speed and safety challenges. More sustainability and dramatically accelerated innovation cycles have joined the list, and in the background has been the looming work force turnover. LNS Research reports that since 2020, the average tenure of the manufacturing work force has fallen from 20 years to three years. Alarmingly, there has been a corresponding 9% increase in industrial fatalities in that same time frame. All that experience about how to get a job done safely is gone, and the new work force has not rounded the learning curve quickly enough. In response, industrial safety certification may need to evolve. It can no longer be only about the safety of the device; we must consider a less-experienced work force interacting in an environment full of devices, and elevate our standards view to that level.



Siemens' response

Companies see the need to become more resilient. They want to adopt new technologies that will help them address their safety and security challenges. They want to be able to do this at their own pace, according to their own needs, starting points and resource capacities. Yet, most companies — especially small and medium-sized businesses — are limited by the cost and effort required to get new technologies to integrate and play well with already-existing infrastructure. Siemens' answer to this is the world's first open digital business platform, Siemens Xcelerator. Everything on Siemens Xcelerator is open, interoperable and available as a service. This offers speed, flexibility and cost benefits to companies of all types and sizes as they pursue their technology agendas, whether optimizing the output from their factory floors, monitoring the safety and security within their buildings or managing the power of their electrical infrastructure.

You can learn more about
Siemens Xcelerator here:

<https://xcelerator.siemens.com/global/en.html>

Implications for standards and governance

Resilience is a shared responsibility between the value chain stakeholders, including technology suppliers, system integrators, end users, standards organizations and jurisdictional authorities. Governance frameworks and standards must adapt to the new realities in the emerging technology landscape with models that are clear and have deep real-world context. A very recent example of this kind of adaptation is UL Solutions' work with Siemens to achieve the world's first digital twin-based certification of an industrial device.

PRESS RELEASE

Siemens' commitment

Siemens is committed to remaining the leader in innovating and delivering technologies to help companies be more competitive and resilient. Not only is it an active member of the UL Standards & Engagement technical committees that are creating, improving and promoting American National Standards Institute (ANSI)-accredited standards for new technologies, but Siemens has also assembled an ecosystem of technology partners to ensure that its solutions fit into customers' environments with more speed and less complexity. The partners include SAP, Microsoft, Nvidia, Intel and thousands of solution and integration experts around the world. In many cases, Siemens is "customer zero" for its own technologies, ensuring that they are fully validated before offering them to the world.



SPOTLIGHT



“

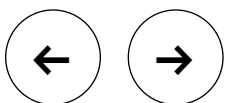
We are committed to delivering transformative solutions for our customers, employees, business partners and communities.

We believe in bold action and innovation to create a socially, environmentally and economically sustainable tomorrow.

Hanwha Group website

Established in October 1952, Hanwha has evolved into a global firm with a diversified portfolio spanning energy, defense, chemicals, robotics and finance.

Today, Hanwha is involved in tackling critical challenges in safety, sustainability and innovation. With an acute focus on advanced technologies such as AI, IoT and blockchain, Hanwha is leading initiatives that not only align with the COC mission but also set new standards in safety and resilience for global energy ecosystems.





Addressing grid and energy storage safety challenges

“AI will play a pivotal role in the energy industry and in the transformation of our energy systems.” (Hanwha Qcells CTO Danielle Merfeld)

In the rapidly evolving energy sector, Hanwha is addressing the critical issue of safety as renewable energy systems increasingly push grids beyond their originally intended unidirectional flows. Through innovations in digital twin technology, advanced simulations and AI-driven predictability, Hanwha is equipping operators with the tools to foresee and mitigate potential grid failures. Work emphasizes resilience, ensuring that energy storage systems and power generation units interact harmoniously and securely within increasingly complex grid systems. As the No. 1 market share holder in the U.S. in solar modules, Hanwha Group has invested \$2.5 billion (USD) in building a fully integrated, silicon-based supply chain in the U.S., pioneering the country’s biggest solar value chain in history.

Grid stability solutions

Hanwha’s AI models will enable predictive analysis of substation and transformer health, preventing catastrophic failures that could jeopardize regional power reliability.

Safety standards for bidirectional power

Recognizing the grid’s growing need to accommodate energy inputs from individual consumers, Hanwha is driving the development of technologies that ensure operational safety without compromising scalability or efficiency.

Pioneering safety in renewable energy deployment

Renewable energy systems often face adoption bottlenecks due to safety and regulatory concerns. Hanwha Qcells addresses these issues head-on by incorporating IoT-based energy management systems that allow real-time monitoring and fail-safe responses to operational anomalies. These solutions not only optimize performance but also help ensure compliance with emerging global safety standards.

Battery safety and optimization

Hanwha is tackling the complexities of energy storage safety through autonomous control technologies that enhance battery performance while reducing risks of thermal runaway, a key concern for battery storage systems.

Regulatory leadership

By engaging with regulators worldwide, Hanwha is shaping frameworks that balance the agility required for rapid technological deployment with stringent safety compliance.





Navigating the interdependencies of safety and regulation

Hanwha's safety-first approach is not limited to technology; it extends to the broader ecosystem of regulations, permitting and standardization. Hanwha advocates for agile regulatory models, where trial-based approaches replace rigid, one-size-fits-all approvals. This flexibility is critical in ensuring that emerging technologies can be safely deployed without unnecessary delays.

Collaboration with standards organizations

Hanwha is actively working with industry bodies to harmonize safety standards across regions, reducing the cost and complexity of compliance for multinational deployments.

Soft cost reduction

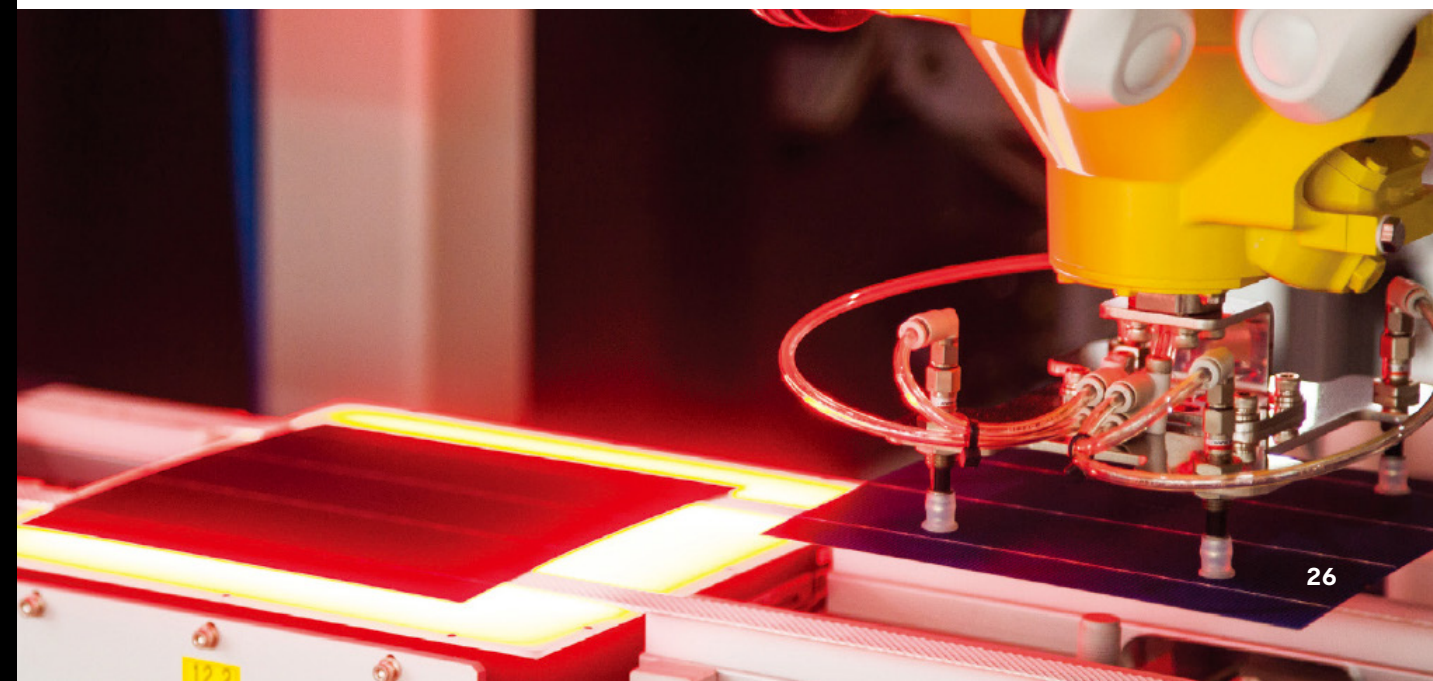
By addressing the regulatory complexities that account for up to 60% of soft costs in deploying residential energy management systems, Hanwha is accelerating safe adoption while reducing barriers to entry for consumers.

As emerging technologies such as AI and blockchain become integral to energy systems, Hanwha emphasizes the importance of "safety by design." Its investments in advanced modeling and simulation tools ensure that potential risks are identified and mitigated before deployment. For instance, in developing AI-powered battery control systems, Hanwha prioritizes fail-safe mechanisms to prevent cascading failures in interconnected grids. Hanwha is also pioneering the creation of safety codes for autonomous battery control systems, addressing a critical gap in current regulatory frameworks. These codes ensure that new technologies enhance, rather than compromise, grid safety.

A vision for resilient and safe futures

Hanwha's long-term vision is centered on creating resilient energy and technology systems that prioritize safety without compromising innovation. By embedding safety into every aspect of its operations — from design and simulation to deployment and compliance — Hanwha sets a high standard for the industry.

Hanwha's approach offers valuable lessons on how innovation and safety can coexist, ensuring that emerging technologies do not merely push boundaries but also uphold the trust and well-being of all stakeholders. As the global energy landscape evolves, Hanwha's leadership will remain instrumental in ensuring that safety and sustainability are not just priorities but imperatives.





MARKET INSIGHTS

Understanding the technological impact on safety-critical sectors

Technological advancements across the fire, electrical and security sectors are driving transformative changes in safety standards. Leaders must understand these shared dynamics to anticipate new risks, adopt proactive safety measures and ensure their standards remain relevant to current times.

This report delivers insights from the Convening of the Councils that empower companies to better safeguard people and assets, providing a data-driven foundation to meet today's challenges and future-proof standards. By applying these insights, leaders can address emerging threats, elevate safety practices and align with the latest technological advancements impacting the industry.







Implications for testing and inspection

Many organizations struggle with outdated safety protocols, insufficient hazard controls and reactive safety measures that only address incidents after they occur. Training is often inconsistent, leaving gaps in employee knowledge and response capabilities. Safety equipment may not be readily accessible or properly maintained, increasing the risk of workplace incidents. Safety experts should adapt to a challenging and changing safety landscape by imagining and shaping the future state of testing and inspection.

The goal is a proactive safety culture where potential hazards are identified and mitigated before incidents occur. Enhanced, regular training programs help ensure all employees are knowledgeable and capable of responding to emergencies effectively. Improved access to and maintenance of safety equipment, along with routine inspections, strengthens on-the-ground safety and reduces risks.

Achieving these improvements requires commitment from leadership, consistent auditing and the allocation of resources to help ensure sustained safety enhancements. A proactive safety culture will not only reduce incidents but also improve morale and compliance, showing employees that their well-being is a top priority.

Current state	Future state	Comments
 Environmental testing	AI-enabled testing, simulation-based testing	ML makes this possible; huge time saver
 Physical inspection	Remote inspection using cameras and drones; augmented reality (AR) inspection	Drone, image processing, object detection and ML will be used; safety, save on costs and time
 Periodic inspection	Real-time asset monitoring for safety; preventive maintenance	Sensors and cameras, along with ML and analytics, will be used; planned shutdowns, safety, save on costs and time
 Physical product testing	Physical and software product testing	Software is becoming more and more important as a result of connected and autonomous devices

Building a long-term safety intelligence framework

A plan for continuous research and updates is crucial as technology advances. Establishing a framework for longitudinal research will keep insights current, allowing safety leaders to adapt standards in real time. With consistent presentation across council areas, highlighting any urgent, safety-critical items, this approach aims to provide a clear, accessible view of ongoing trends and critical developments, enabling leaders to uphold high safety standards in a fast-evolving landscape.



FIRE INDUSTRY





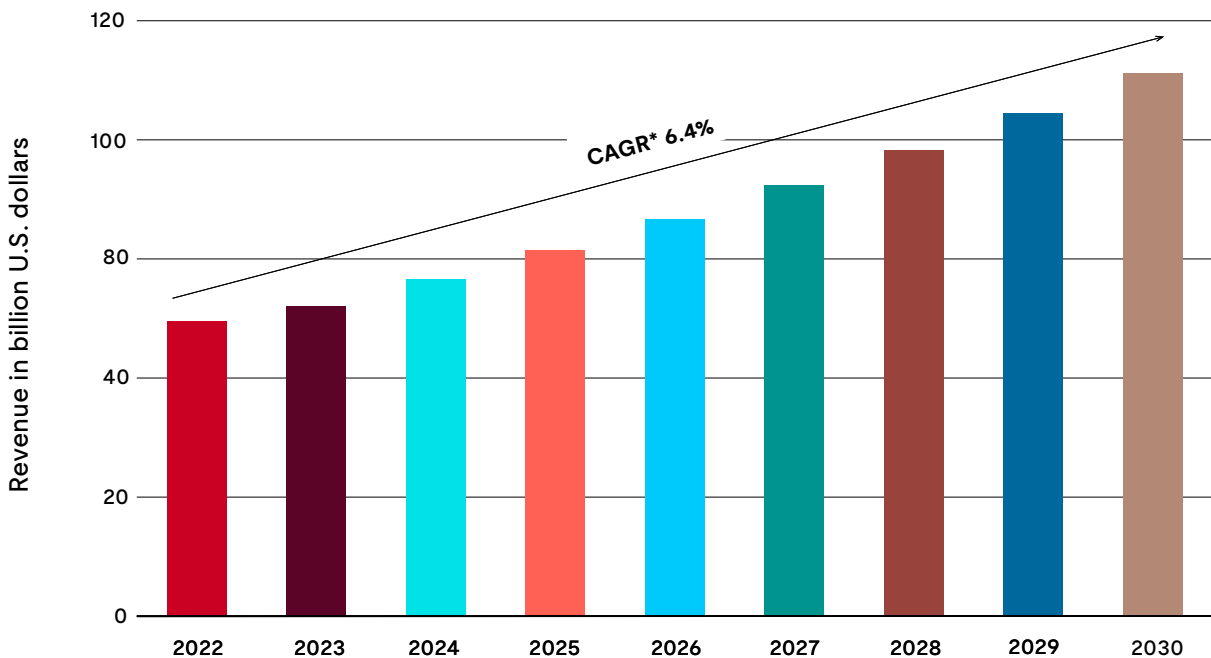
Global fire protection market

The global fire protection industry is expected to experience steady growth, with its global market value rising from \$67.9 billion (USD) in 2022 to an estimated \$111.3 billion in 2030.

This is largely driven by the increasing demand for fire safety systems across various sectors. The growth reflects heightened awareness and regulatory requirements around fire safety, particularly in industrial, commercial and residential buildings. Urbanization, infrastructure development and technological advancements in fire protection, such as automated suppression systems, are key factors driving this growth.

The fire protection industry is becoming increasingly crucial as businesses, governments and homeowners recognize the importance of preventing fire-related losses. Investment in fire protection is not only a regulatory necessity but also a preventive measure for safeguarding assets and lives.

Global fire protection system market size (2022-2030)



*Compound annual growth rate (CAGR)
Source: Composite of Fortune Business Insights™ and MarketsandMarkets™, Grand View Research



GLOBAL FIRE PROTECTION MARKET

Overall considerations for standards development

Integrated fire safety

Given the interconnected nature of these systems, standards should emphasize compatibility and integration across suppression, detection, response and analysis systems. Standards that promote interoperability enable seamless communication between different safety systems, enhancing overall fire response capabilities.

Technological innovation and digital transformation

With new technologies like IoT, radio frequency identification (RFID) and AI-driven analysis, fire safety standards need to evolve to include specifications for smart buildings. This can improve response times and enable predictive capabilities.

Environmental and sustainability standards

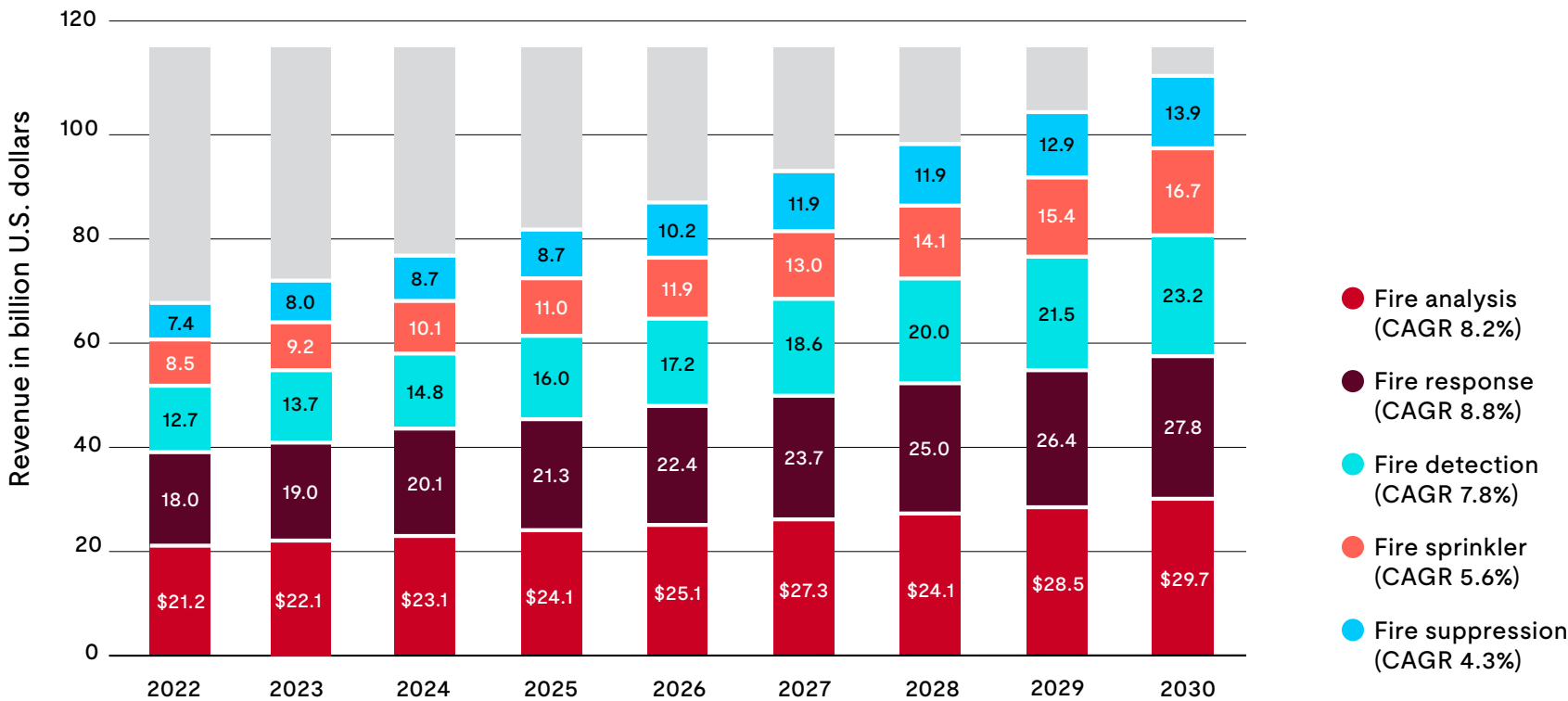
In light of global environmental concerns, standards should consider the environmental impact of fire protection systems, especially with suppression agents and disposal of old systems.



Global fire protection segments

The data table below shows fire suppression systems currently hold the largest market share among segments. Fire suppression systems are expected to continue leading in market size through 2030, but are followed closely by other segments with higher growth.

Global fire protection system market size by segment (2022-2030)



Source: Composite of Fortune Business Insights™, MarketsandMarkets™, Grand View Research, Market Research Future



GLOBAL FIRE PROTECTION SEGMENTS

By establishing rigorous, forward-looking standards across these segments, safety experts can drive the development of fire protection systems that are not only more effective but also sustainable, adaptable and in line with evolving technology.

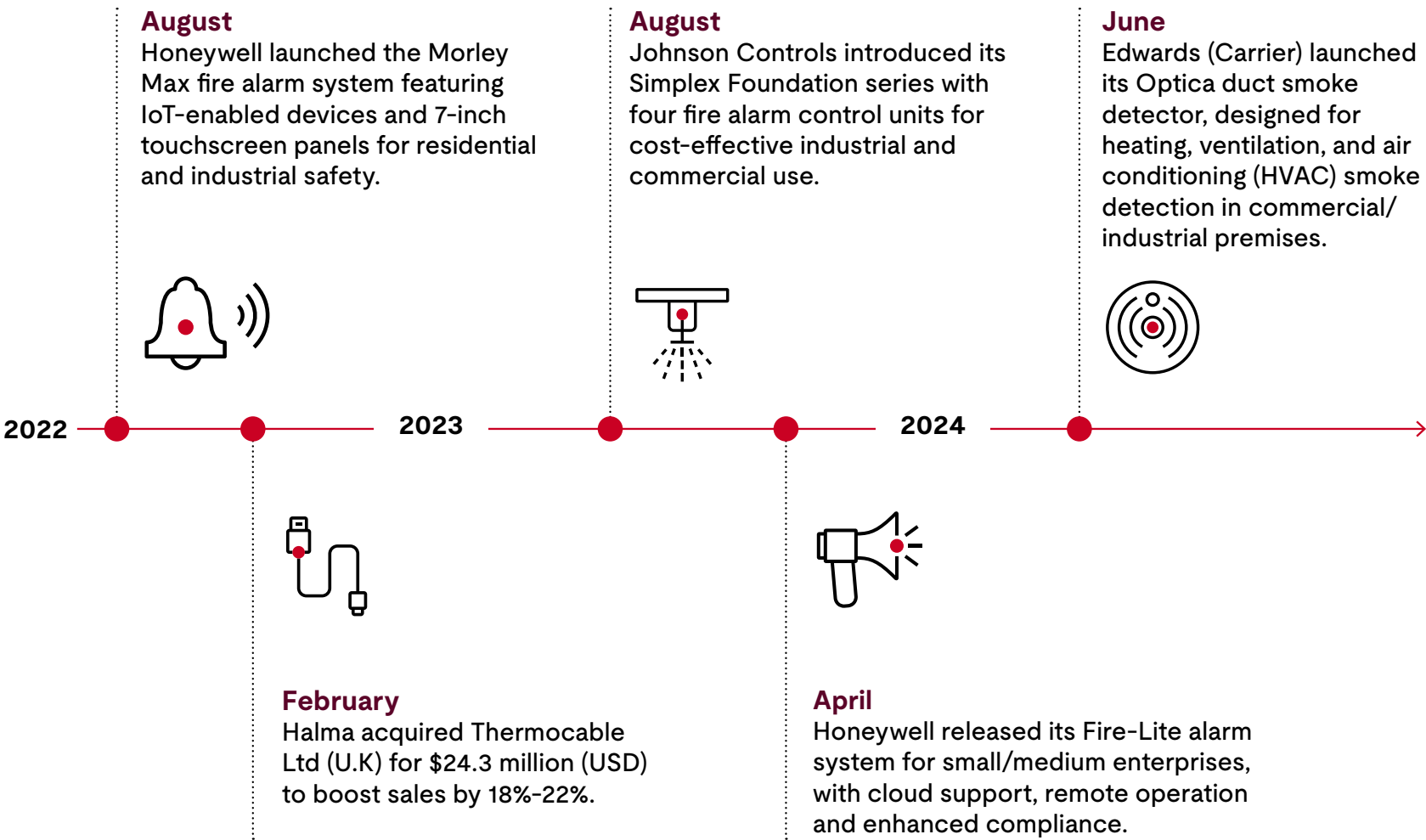
Fire suppression Fire suppression systems must be adaptable to various types of fire risks, including chemical, electrical and flammable liquid fires. Standards developers should emphasize environmental impact, particularly regarding clean agents that are less harmful to the environment, and consider updating suppression systems to align with sustainable and less hazardous agents.	Fire sprinkler systems Regulatory requirements and safety codes mandate sprinkler installations in commercial and residential buildings. Creating more stringent guidelines on sprinkler maintenance, conducting periodic testing and sub-segmenting standards by sprinkler type (wet-pipe, dry-pipe, pre-action, deluge) allows for targeted safety protocols based on specific system attributes, improving system effectiveness across different environmental conditions.	Fire detection Fire detection technology, especially with advancements in RFID and flame detection, plays a crucial role in early warning systems. The diversification into smoke, heat, RFID and flame detectors highlights the complexity of modern fire detection needs. Safety experts should ensure that detection standards consider technological advancements, particularly in RFID systems and flame detection. Standards should address detection sensitivity, response times and the integration of multiple detection types to improve accuracy and minimize false alarms.	Fire response The growth in critical communication and alert systems such as emergency lighting, voice evacuation and public alert systems reflects an increasing emphasis on coordinated, safe evacuations and timely emergency response. Standards should focus on interoperability and reliability, helping to ensure these systems perform effectively under extreme conditions. Establishing universal protocols for emergency lighting and public alert systems that consider building layouts, occupancy levels and evacuation pathways can enhance evacuation safety.	Fire analysis Fire analysis tools, including fire mapping and simulation software, are emerging as vital assets for predictive modeling and risk assessment. These tools enable safety experts to analyze potential fire scenarios and design preventive strategies accordingly. As this technology advances, there is a need to create standards around data accuracy, model validation and scenario testing. Setting guidelines for fire analysis software will improve the reliability of these tools, ensuring they provide actionable insights for fire prevention and response planning.
---	---	--	---	--



Key developments in fire protection

To the right, this timeline highlights recent key industry developments in fire protection. These milestones illustrate how innovations in technology, system integration and safety standards have evolved.

Experts should anticipate future advancements in detection accuracy, specialized suppression methods, integrated systems, data-driven compliance and sustainable practices. These can create a more reliable, efficient and adaptable fire safety industry, setting the stage for future innovations and enhanced safety standards.

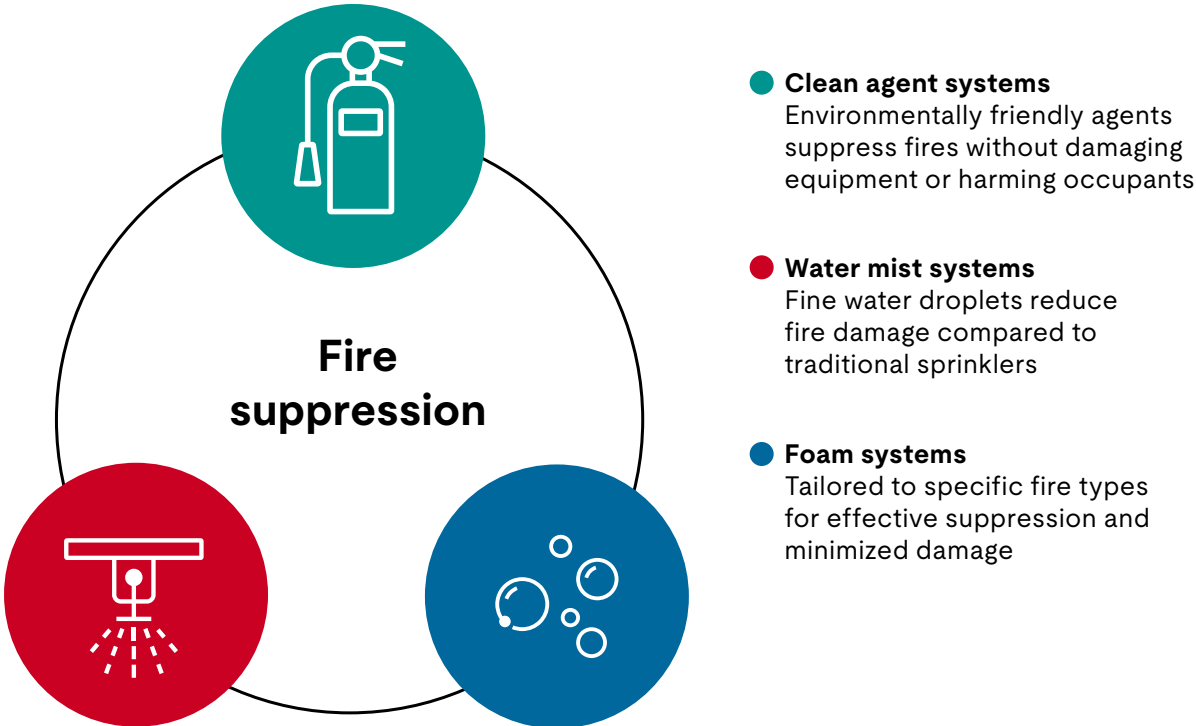
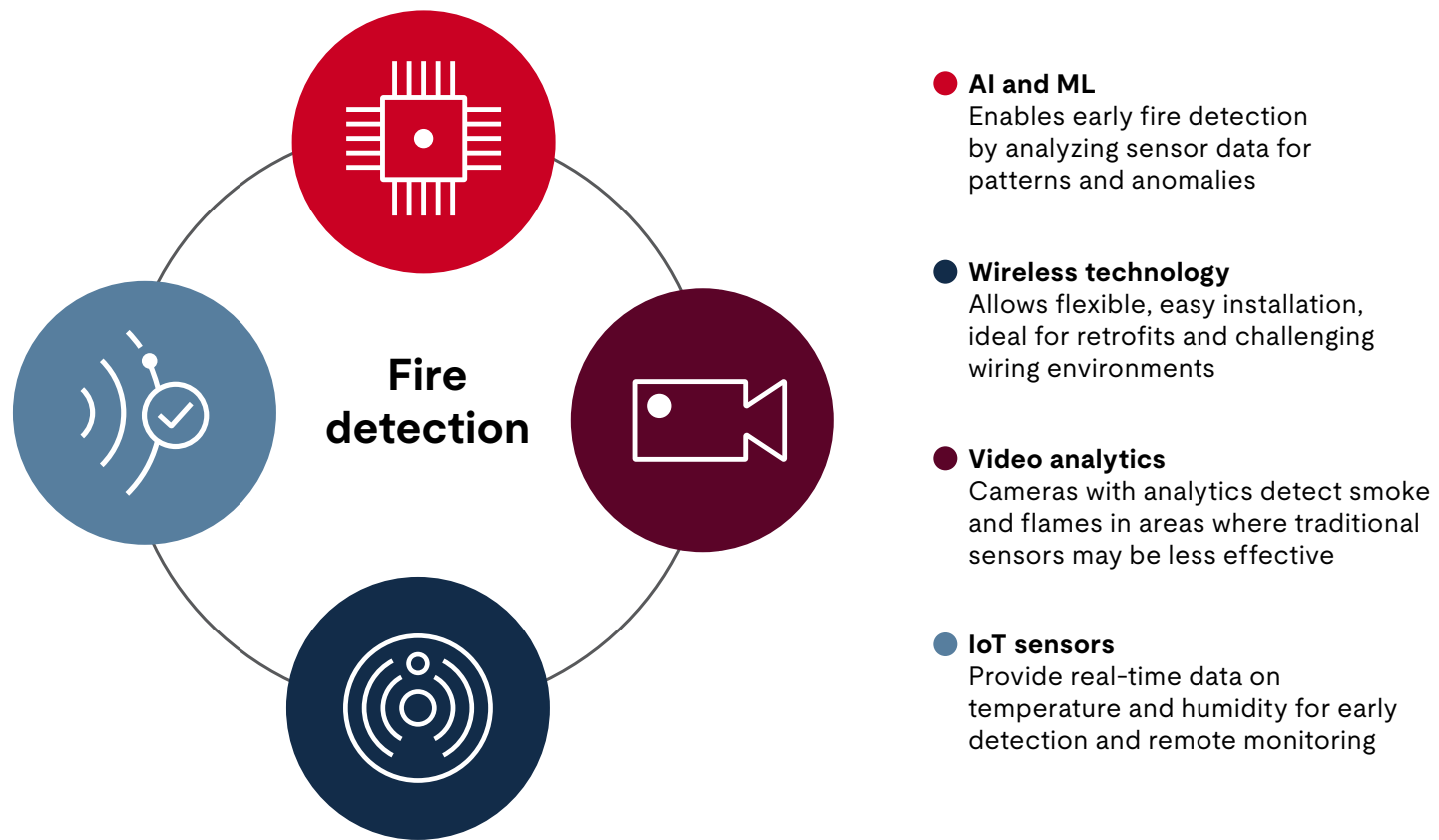


Source: Business Insights



Top fire protection industry trends

Together, these proactive industry trends form a robust fire safety framework, enhancing protection and minimizing potential damage across diverse settings.





Top fire protection takeaways

01

Strong market growth

The global fire protection industry is projected to grow significantly, from \$67.9 billion (USD) in 2022 to \$111.3 billion in 2030, indicating robust demand for protection products and services as well as respective improved standards.

02

Rising demand across sectors

Increased awareness and stricter regulatory requirements are driving demand for fire safety in industrial, commercial and residential sectors, but also suppression, sprinkler systems, detection, response and analysis segments.

03

Urbanization and infrastructure development

Rapid urban expansion and new infrastructure projects are creating a need for advanced fire protection systems to help ensure the safety of larger and denser populations.

04

Technological advancements

Innovations such as automated suppression systems and IoT-enabled fire detection are reshaping fire safety, allowing for faster, more effective responses to fire risks.

05

Investment as preventive measure

Investment in fire protection is seen not only as a regulatory requirement but also as an essential measure to protect assets and lives, making it a priority for businesses, governments and individuals alike.

06

Shift toward intelligent solutions

There is a growing emphasis on proactive, scalable and intelligent fire protection that adapts to evolving fire risks, enhancing overall safety in increasingly complex environments.





ELECTRICAL INDUSTRY

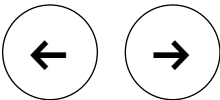




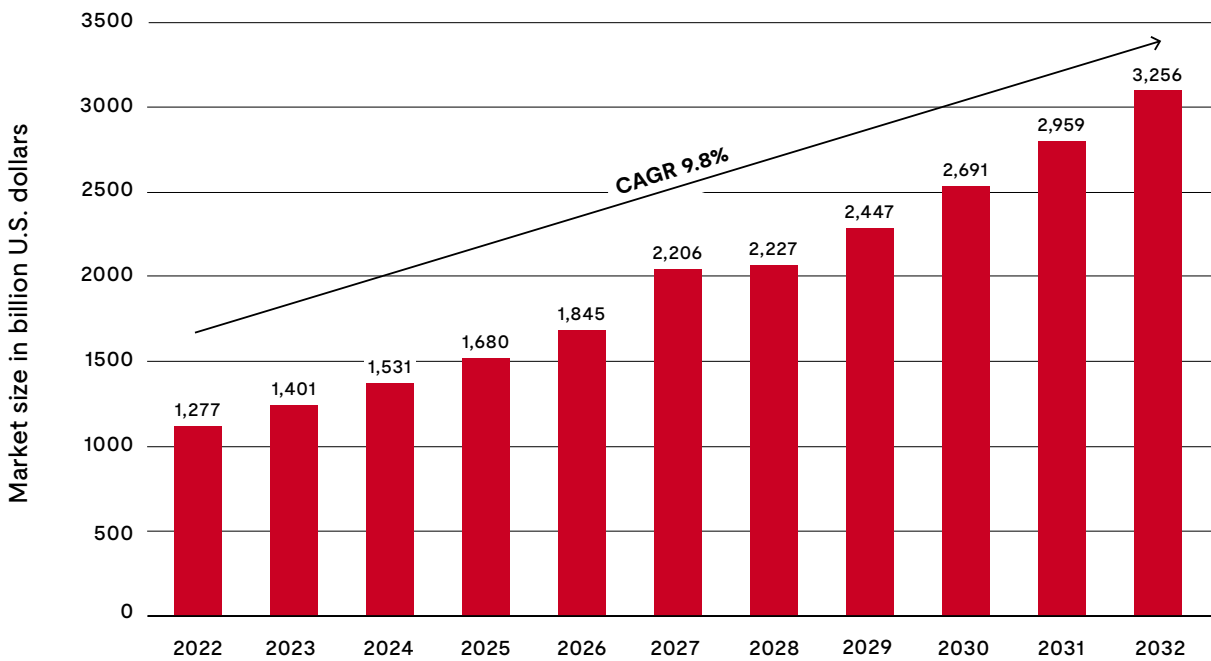
Electrical market size

The projected growth of the electrical equipment industry, from \$1,277 billion (USD) in 2022 to \$3,256 billion by 2032, highlights critical areas of focus for safety experts as demand surges across renewable energy, smart grids and expanding infrastructure.

With the shift toward renewable energy and electrification, there is an urgent need for updated safety standards to support rapidly evolving applications like electric vehicle (EV) charging and sustainable energy systems. Safety professionals will be essential in ensuring these systems meet rigorous standards amid changing regulations and technological advancements. The adoption of smart grids and IoT-enabled devices brings both efficiencies and new safety risks, particularly around cybersecurity and system resilience. Safety experts can play a key role in establishing protocols that address these complexities, working toward safe deployment and reliable operation. Expansion into emerging markets also presents diverse safety challenges due to varying regulations and infrastructure needs. External safety professionals can provide insights to create adaptable frameworks that maintain high standards globally. As the industry aligns with trends in electrification and digital transformation, safety experts will be critical in guiding its growth responsibly, supporting innovation while protecting infrastructure.



Global electrical equipment market size (2022-2032)



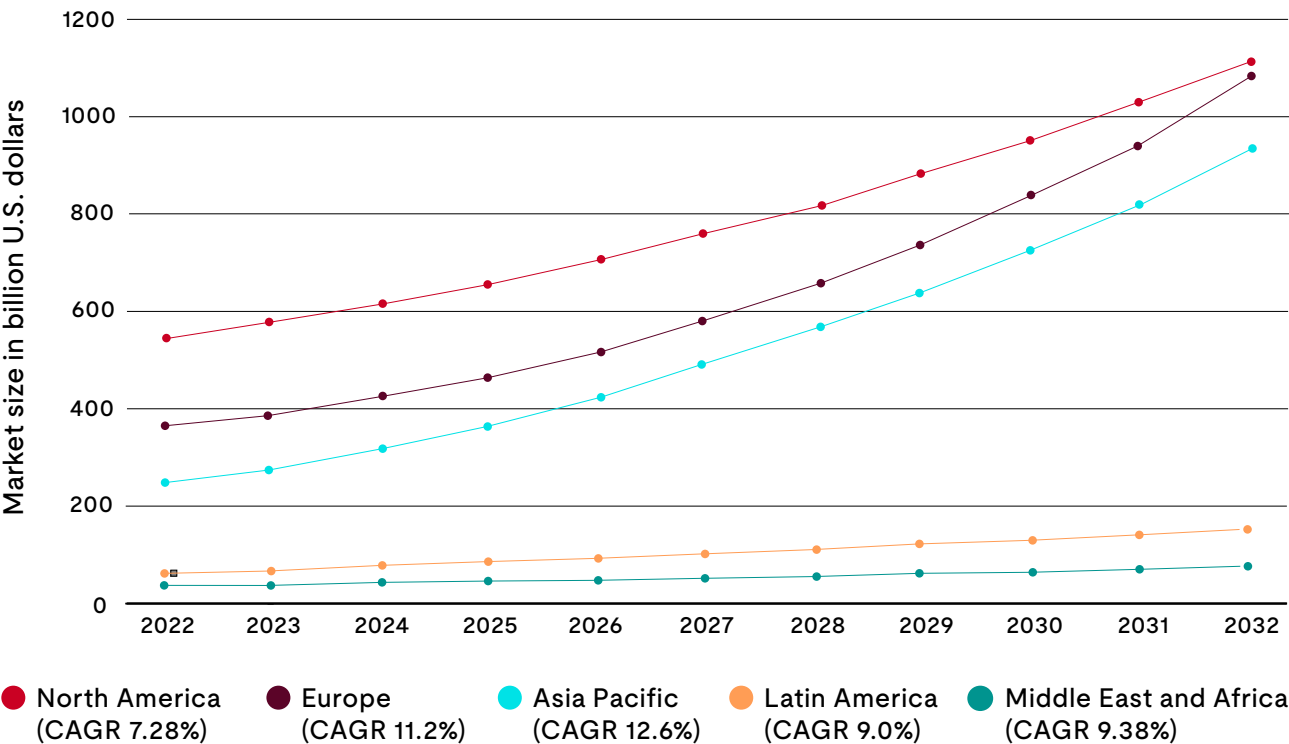
Source: Composite of Credence, Cognitive Market and Fortune Business Insights



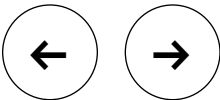
Electrical equipment global markets

Globally, the industry’s 9.81% CAGR reflects a blend of modernization in mature markets and new infrastructure in emerging regions, with sustainability and energy efficiency as core growth themes across all areas.

Global electrical equipment market size by geography (2022-2032)



Source: Composite of Credence, Cognitive Market and Fortune Business Insights



Asia Pacific

Asia Pacific’s growth is largely driven by massive infrastructure investments and urbanization, especially in China and India. The push for renewable energy and industrial automation is further fueling demand for advanced electrical equipment.

Europe

Europe has ambitious sustainability goals, including the European Green Deal. Investments in smart grids, energy-efficient infrastructure and EV adoption are creating significant demand for modern electrical equipment.

North America

North America’s mature market is driven by modernization, upgrades and government investment, focusing on energy efficiency, grid resilience and cybersecurity for industrial and commercial systems.

Latin America

Latin America’s growth is influenced by urbanization and the need for reliable infrastructure. Rising interest in renewable energy and distributed systems is creating demand for equipment that addresses both urban and remote needs.

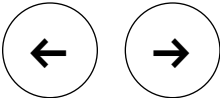
Middle East and Africa

Growth in the Middle East and Africa is fueled by infrastructure projects and energy diversification, especially in renewable energy. Electrification in rural Africa and solar investments in the Middle East are key drivers.

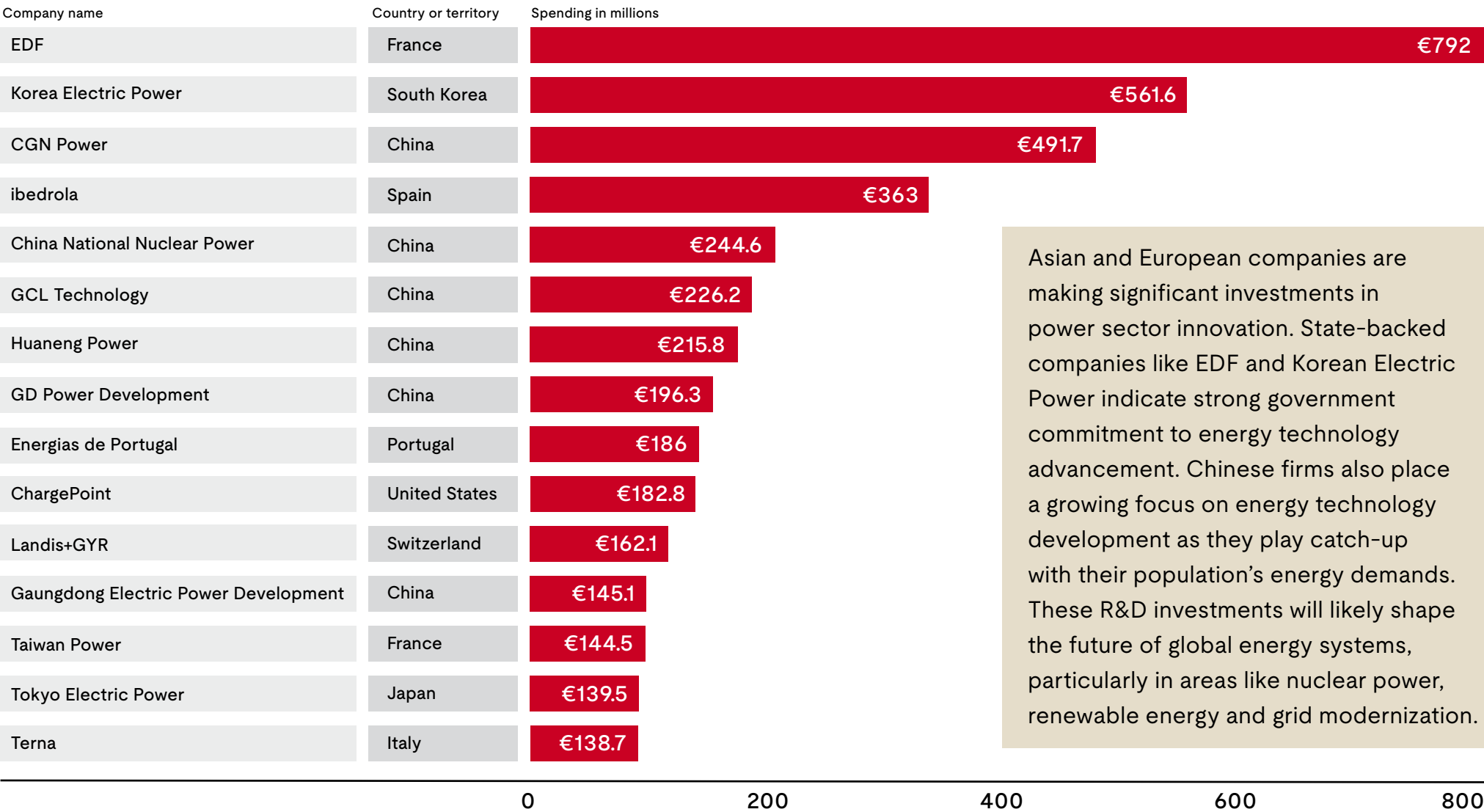


Electrical equipment research and development

Electrical R&D spending is crucial for advancing sustainable energy solutions, grid reliability and technological innovation. R&D in electrical equipment focuses on renewable energy integration, smart grid technologies, energy storage and improving power plant efficiency, among other items.



Electricity R&D spending in million euros



Asian and European companies are making significant investments in power sector innovation. State-backed companies like EDF and Korean Electric Power indicate strong government commitment to energy technology advancement. Chinese firms also place a growing focus on energy technology development as they play catch-up with their population’s energy demands. These R&D investments will likely shape the future of global energy systems, particularly in areas like nuclear power, renewable energy and grid modernization.

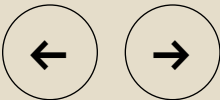
Source: statista.com



Consumer electronics overview

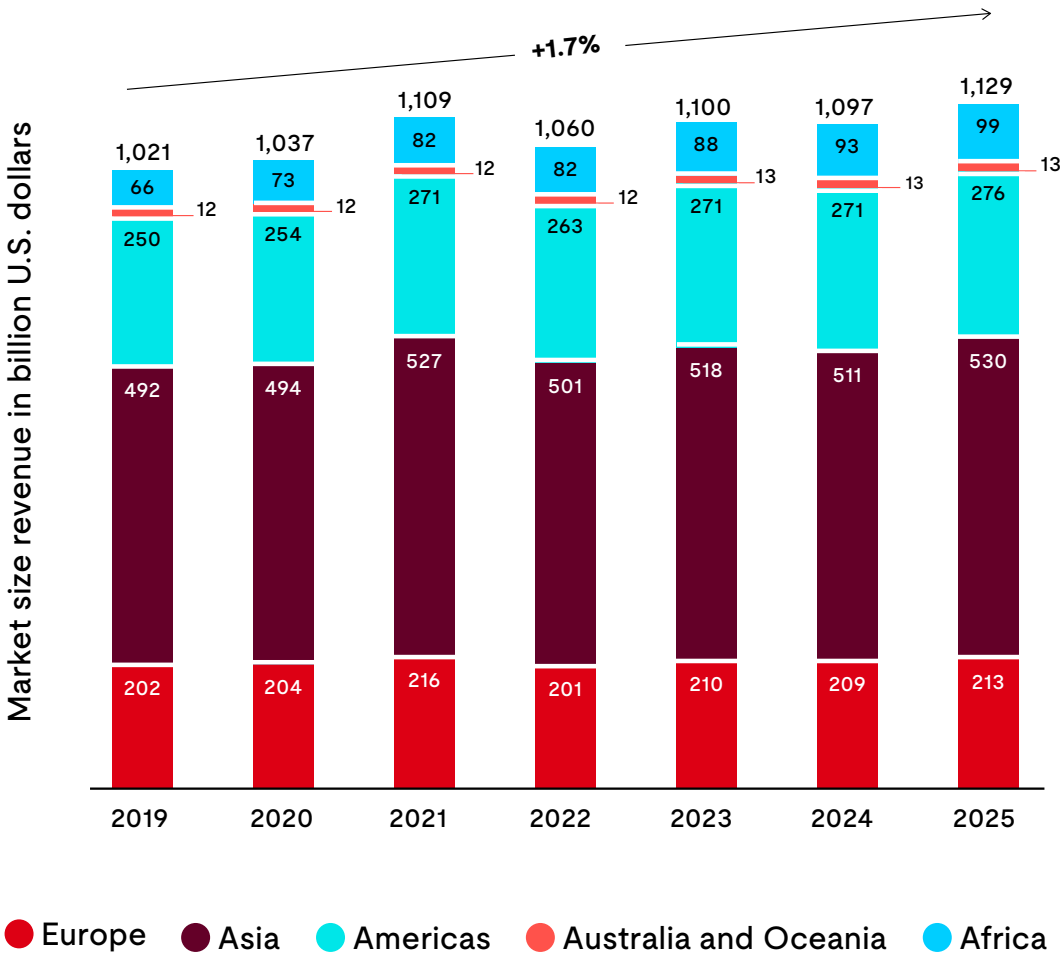
As the market for consumer electronics continues to grow steadily, safety experts must prioritize updating standards and protocols to keep pace. The increasing adoption of IoT-enabled devices, smart home systems and advanced energy storage solutions presents unique safety challenges, particularly around battery safety, electromagnetic compatibility and cybersecurity for networked devices.

Experts should focus on strengthening standards for high-capacity batteries, which are integral to modern electronics, by ensuring robust protections against overheating and thermal runaway risks. The growth in IoT means that enhanced cybersecurity guidelines are critical to protect consumer data and prevent unauthorized access to devices. As new technologies emerge and become widely adopted, continuous monitoring, regular updates to safety standards and strict compliance checks will be essential to supporting consumer protection while maintaining the pace of innovation in the industry.



Consumer spending on consumer electronics is expected to increase by 1.7% per year from 2019 to 2025.

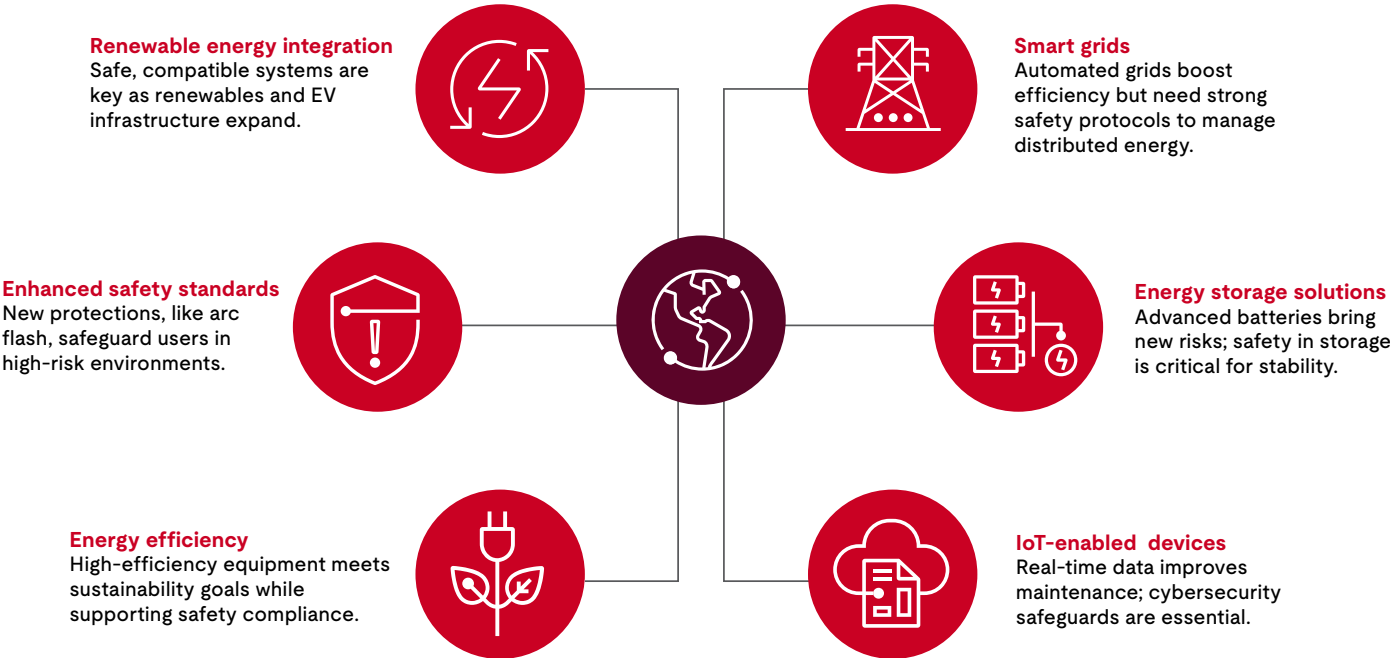
Market size revenue in billions USD





Top electrical equipment trends

The electrical equipment industry is evolving rapidly, driven by key trends like renewable energy integration, smart grid technology and advanced energy storage. As countries push toward clean energy, demand for equipment supporting solar, wind and EV infrastructure is rising. Meanwhile, smart grids and IoT-enabled devices are transforming the industry with real-time monitoring and automation, making energy systems more efficient and adaptable, but also raising new cybersecurity challenges.



Overall, the industry is shifting toward resources that are not only more sustainable and intelligent but also safer, meeting modern energy needs and regulatory expectations.

- **Renewable energy integration** – As clean energy grows, so does the need for safe, compatible equipment for solar, wind and EV setups. Safety protocols for integrating these sources into the grid will be critical to prevent overloads and ensure reliable power.
- **Smart grids** – Digital and automated systems in smart grids improve efficiency but require robust safety standards. Monitoring for faults and managing distributed resources minimizes risks and improves response times in incidents.
- **Energy storage solutions** – Advanced batteries are essential for balancing renewables but bring new risks, including thermal management and containment. Enhanced safety designs will be key to safe, reliable energy storage in high-demand environments.
- **IoT-enabled devices** – Real-time monitoring and predictive maintenance boost reliability, but widespread connectivity increases cybersecurity risks. Prioritizing security will be critical as networked devices become the norm.
- **Energy efficiency** – Demand for high-efficiency equipment, like smart meters and transformers, is rising under sustainability mandates. Ensuring that these technologies meet updated safety standards is crucial as they become widely adopted, and solar investments in the Middle East are key drivers.
- **Enhanced safety standards** – New safety measures, like arc flash protection, are essential as equipment and risks evolve. Ensuring compliance with these standards will protect users, particularly in high-risk and industrial settings.



Electrical equipment takeaways for executives

01

Strong market growth

The global electrical equipment market is expected to grow from \$1,277 billion (USD) in 2022 to \$3,256 billion by 2032, with a CAGR of 9.81%, driven by the expansion of renewable energy, smart grids and infrastructure projects worldwide.

02

Critical role of safety standards

As the industry shifts toward renewable energy and electrification, updated safety standards are essential for EV charging, smart grids and IoT-enabled devices. Safety experts play a crucial role in addressing new risks like cybersecurity and system resilience.

03

Regional growth variations

Growth drivers vary by region — Asia Pacific’s growth is fueled by infrastructure and urbanization, Europe’s by sustainability goals, North America’s by modernization and Latin America’s by urbanization and energy needs. The Middle East and Africa see growth through energy diversification and rural electrification.

04

Renewable energy integration

Demand for electrical equipment that supports solar, wind and EV infrastructure is increasing globally as countries set ambitious clean energy targets.

05

Technology-driven efficiency and resilience

Smart grids, IoT devices and advanced battery storage solutions are transforming the industry, making energy systems more efficient, adaptable and better able to manage renewable energy.

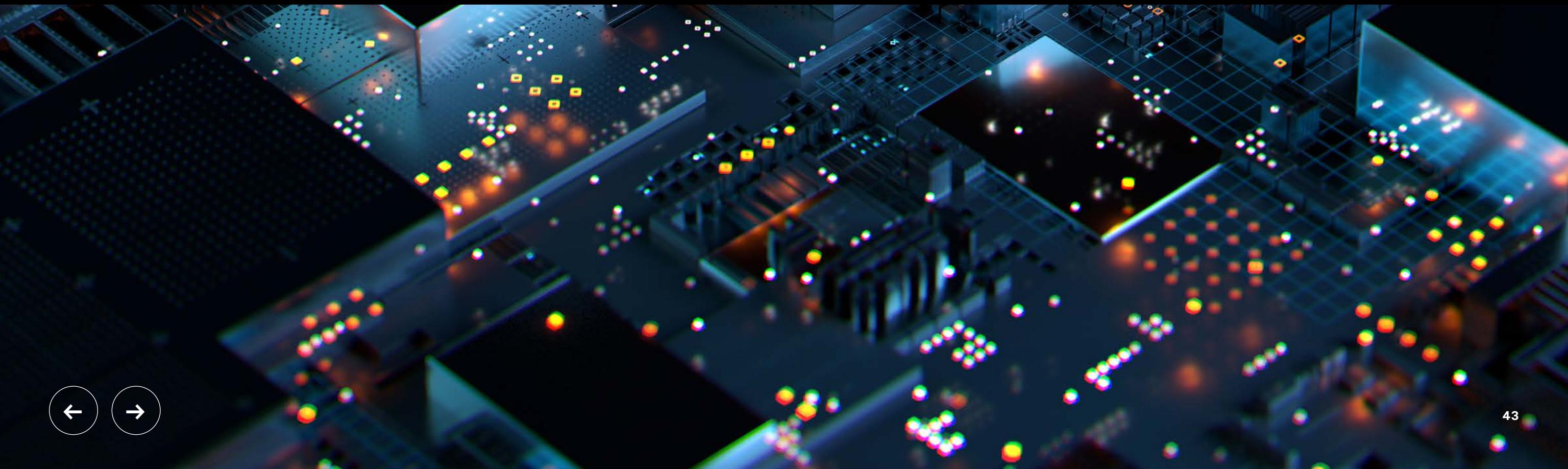
06

Focus on safety and compliance

Enhanced safety standards, such as arc flash protection, are increasingly necessary as electrical systems become more complex and widely deployed in high-risk applications, helping to ensure compliance and user protection.



SECURITY INDUSTRY



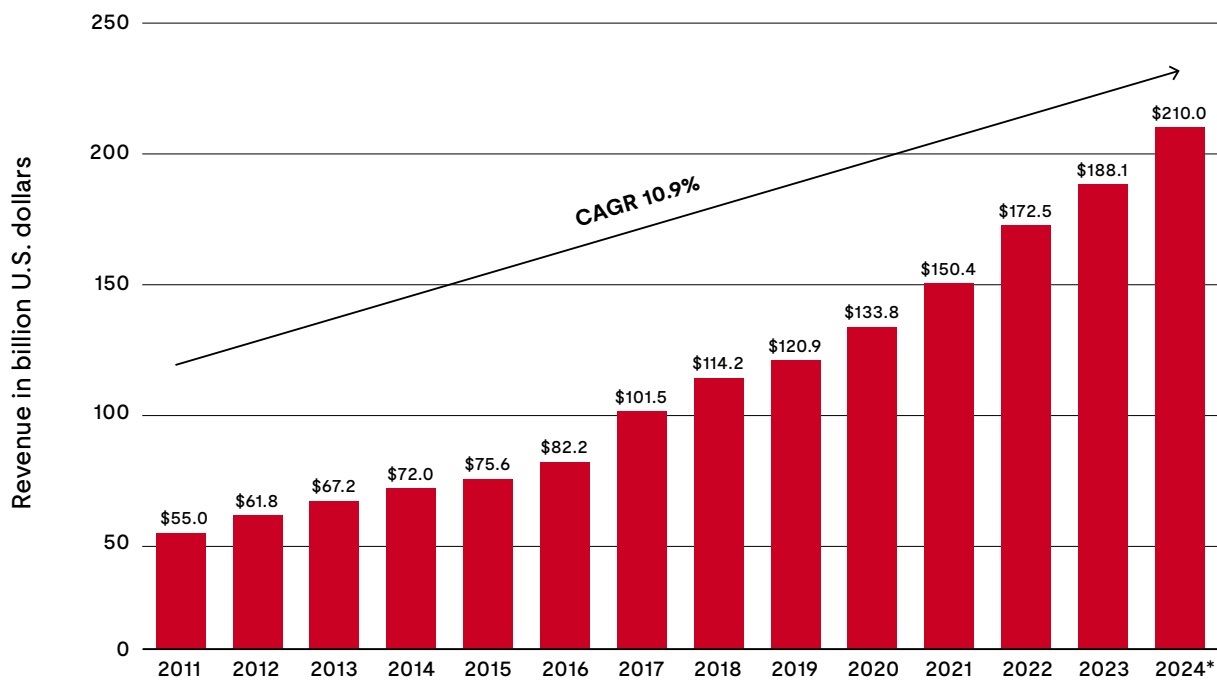


Security revenue

The global information security market has demonstrated consistent growth over the past decade, expanding from \$55 billion (USD) in 2011 to \$188.1 billion in 2023, with a projected revenue of \$210 billion in 2024.

This represents a CAGR of 10.9%, illustrating the robust demand for cybersecurity solutions as organizations increasingly prioritize protecting their digital assets. The steady upward trend highlights how rising cybersecurity threats, coupled with the growing complexity of digital infrastructure, have driven businesses and governments worldwide to invest heavily in comprehensive security measures.

Total revenue global information security market (2011-2024)



Source: statista.com



SECURITY REVENUE

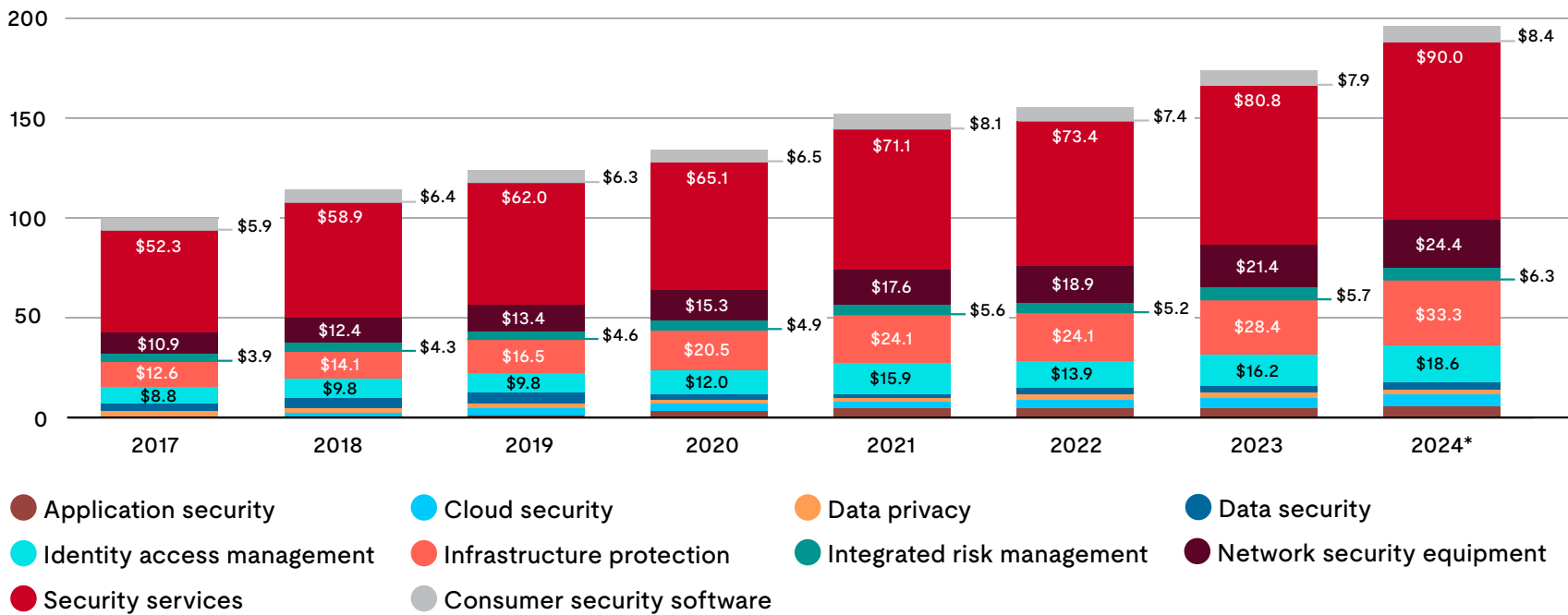
High-profile data breaches, regulatory changes and the rapid adoption of new technologies like cloud computing, IoT and remote work infrastructures all present new vulnerabilities that require specialized security solutions. The transition to remote work and increased reliance on cloud services during the COVID-19 pandemic amplified security risks, spurring a wave of investment in cloud security and remote access protections.

The market’s doubling over the past decade underscores strong investment in cyber defense as cybersecurity becomes not only a strategic priority but also a necessity in an increasingly digital and interconnected world. Organizations are recognizing that a reactive approach is insufficient; instead, they require proactive and scalable security solutions capable of addressing a dynamic threat landscape. This continued growth trajectory indicates that cybersecurity will remain a central focus for businesses and governments alike as they seek to secure their infrastructures, protect sensitive data and build resilience against sophisticated cyber threats.

Security segments revenue

Information security has undergone steady growth and diversification of the information security market from 2017 to a projected 2024, with security services, infrastructure protection, network security and identity access management accounting for the largest shares, reflecting their foundational role in cybersecurity.

Information security spending worldwide from 2017 to 2024, by segment (in billions, USD)



2017-2024 CAGR

Application security	Cloud security	Data privacy (*21'-24)	Data security	Identity access management	Infrastructure protection	Integrated risk management	Network security equipment	Security services	Consumer security software
25%	527%	15%	10%	16%	24%	8%	18%	10%	6%

Source: statista.com



SECURITY SEGMENTS REVENUE

The fastest-growing areas in information security from 2017 to 2024 are cloud security, application security and infrastructure protection, each driven by unique factors shaping the digital landscape. The growth in cloud security reflects the massive shift to cloud environments as businesses migrate critical systems and data, necessitating robust protections for cloud infrastructure against increasingly complex threats. Application security, growing at 25% CAGR, is also a priority as organizations rely more on software applications, making them key targets for cyber attacks and heightening the need for secure coding, vulnerability management and runtime protections. Infrastructure protection, with a 24% CAGR, remains essential as the backbone of digital operations, where any vulnerabilities can lead to widespread disruptions. The rapid growth in these areas underscores the heightened need for adaptive, scalable security solutions that can protect core systems and data across various platforms and environments.



The fastest-growing areas in information security



Cloud
security



Application
security



Infrastructure
protection

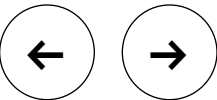
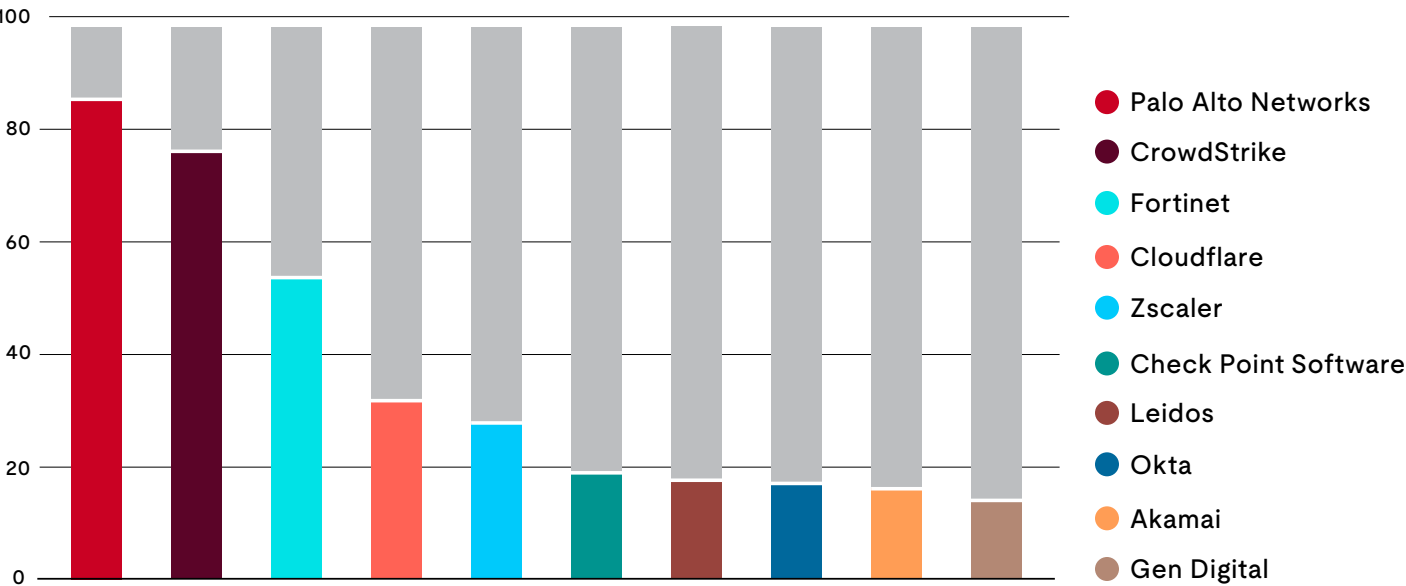
The rapid growth in these areas underscores the heightened need for adaptive, scalable security solutions.



Growing security firms

Cybersecurity has become of crucial importance and has brought with it the emergence of multibillion-dollar companies such as Palo Alto Networks, CrowdStrike and Fortinet. In 2024, California-based Palo Alto was the most valuable company in the cybersecurity sector, with a market capitalization exceeding \$87 billion (USD). Among the 10 leading cybersecurity firms in terms of market capitalization, nine were based in the United States.

Leading cybersecurity companies worldwide 2024, by market cap (billions USD)



As organizations accelerate their digital transformation, the need for robust security solutions has become paramount. This growth is fueled by several converging factors: the rise of sophisticated cyber threats, including state-sponsored attacks and AI-powered malware; the rapid adoption of cloud computing and remote work solutions; and increasingly stringent regulatory requirements around data protection and privacy.

Modern cybersecurity companies are now focusing on integrated, AI-driven solutions that can provide real-time threat detection and response across multiple attack surfaces. The rise of zero-trust architecture, championed by companies like Zscaler and Palo Alto Networks, reflects a fundamental shift in how

organizations approach security, moving from a “trust but verify” to a “never trust, always verify” mindset.

The emergence of new technologies like quantum computing and 5G networks is creating both opportunities and challenges for security providers, forcing them to innovate and adapt their solutions continuously. Investment in the sector remains robust, with venture capital firms and corporate investors pouring billions into cybersecurity startups and established players alike. The industry’s continued growth seems assured as digital transformation accelerates across all sectors, making cybersecurity not just an IT priority but a fundamental business imperative.



Top security trends

As cybersecurity threats continue to evolve in scale and sophistication, organizations are adopting new strategies and technologies to stay ahead. In 2024, several key trends are shaping the future of cybersecurity, focusing on proactive defenses, integrated security solutions and advanced threat detection capabilities. These trends reflect a shift toward more adaptive, automated and intelligence-driven approaches, designed to protect increasingly complex digital environments. Here are six trends transforming the cybersecurity landscape.

- **Zero trust architecture** – With the increase in remote work and cloud environments, zero trust models, which require continuous verification of users and devices, have become essential. This approach minimizes insider and outsider threats by assuming no user or device can be trusted by default.
- **Extended detection and response (XDR)** – XDR solutions integrate multiple security products into a single platform, allowing security teams to detect and respond to threats across endpoints, networks and cloud environments. This unified view helps to streamline incident response and improve threat detection accuracy.
- **Cloud security enhancements** – As more organizations move to cloud infrastructure, advanced cloud security tools are emerging to protect sensitive data, detect unusual activity and prevent unauthorized access. These tools provide automated protection tailored to the complexities of multi-cloud environments.
- **Ai-driven threat intelligence** – Artificial intelligence is increasingly used to analyze threat data and predict future attacks. AI-driven threat intelligence systems can detect complex attack patterns in real time, allowing for faster response times and more proactive defenses.
- **Security automation and orchestration (SOAR)** – SOAR platforms help organizations manage and respond to security incidents by automating routine tasks, reducing manual work for security teams and ensuring consistent, rapid response to incidents.
- **Identity and access management (IAM) evolution** – IAM solutions are becoming more sophisticated, incorporating biometric authentication, adaptive access control and advanced monitoring. These enhancements help organizations secure digital identities, reduce fraud and prevent unauthorized access to sensitive systems and data.





Security takeaways

01

Consistent revenue growth

The cybersecurity market has grown at a steady CAGR of 10.9%, from \$55 billion (USD) in 2011 to an anticipated \$210 billion in 2024, highlighting the essential role of cybersecurity as digital threats increase.

02

Investment in security segments

Cloud security, application security and infrastructure protection are among the fastest-growing security segments, with cloud security showing a remarkable CAGR of 527% from 2017-2024, driven by cloud adoption and remote work trends.

03

Diverse security spending

Security services, infrastructure protection, network security and IAM represent the largest areas of spending, emphasizing the foundational nature of these solutions in robust cybersecurity strategies.

04

Top cybersecurity trends

Zero trust architecture for continuous verification, XDR for integrated threat detection, advanced cloud security tools for multi-cloud protection, AI-driven threat intelligence for proactive defenses, SOAR for automated incident response and evolving IAM with biometrics and adaptive access control all reflect a shift toward proactive, scalable security strategies in response to evolving digital threats.

05

Proactive over reactive approaches

Organizations are shifting toward adaptive and scalable security strategies that address evolving digital threats, emphasizing proactive defenses over reactive responses.

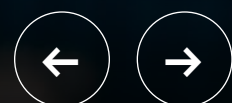
06

Investment opportunity

The cybersecurity market’s consistent growth and sector expansion has occurred as a result of strong demand, but also strong investment from outside firms, focusing on developing new products and services.



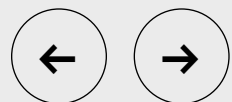
KEY INSIGHTS AND FINDINGS





KEY INSIGHTS AND FINDINGS

Building resilience in the age of technology





Introduction

In a rapidly advancing technological landscape, key stakeholders gathered to discuss pressing issues and emerging challenges in cybersecurity, artificial intelligence, IoT and safety standards. This conference aimed to foster a collaborative dialogue on strategies and innovations that enhance both resilience and safety across various industries.

Key findings

The need for enhanced cybersecurity measures
With the surge of interconnected devices, cybersecurity has emerged as a fundamental aspect of safety. Experts highlighted the vulnerabilities within IoT systems and the importance of standardized security protocols to protect users from cyber threats.

Challenges in interconnected systems
The integration of electrical and fire safety systems in smart buildings and cities presents unique challenges. Maintaining compatibility and safety across updates, particularly when legacy systems are involved, requires coordinated standards and robust testing.

The role of artificial intelligence in safety and automation
AI was discussed as both an opportunity and a potential risk. While AI enhances efficiency and predictive capabilities, concerns remain about the accuracy and security of automated decisions, especially within safety-critical systems.

The future of regulations and standards
The global regulatory landscape for cybersecurity and safety continues to evolve, with initiatives such as the U.S. Cyber Trust Mark setting a baseline for secure device standards. Harmonizing these standards internationally will be crucial for effective implementation.

The environmental impact of technology deployment
As the deployment of data-intensive systems like AI grows, so does the need for sustainable energy solutions to power them. Calls for “frugal models” emphasize the importance of energy-efficient technology that minimizes environmental impact.



Cybersecurity and IoT

The proliferation of IoT devices has brought unparalleled connectivity as well as significant security challenges.

The session highlighted that as more devices become interconnected, they create potential entry points for cyber threats. A primary focus was the recently introduced U.S. Cyber Trust Mark, an initiative designed to provide a cybersecurity baseline for consumer IoT products. This label aims to educate and reassure consumers while pushing manufacturers to prioritize cybersecurity.

The program requires products to meet NIST 8425 standards, which set baseline requirements for secure product capabilities and development practices, such as encrypted data transmission, secure update protocols and strict authentication and authorization measures. However, experts acknowledged that security needs differ greatly depending on the device's function, context and geographical deployment, complicating the path to global harmonization of standards. Participants emphasized that while such regulatory steps are important, ongoing collaboration between private and public sectors is essential to keep pace with rapidly evolving cyber threats.



System integration in smart buildings

With the rise of smart cities and buildings, system integration has become critical to maintaining safety, especially in structures where fire safety, electrical, HVAC and security systems are now interconnected.

Panelists pointed out that while these integrated systems bring improvements in energy efficiency, occupant safety and building management, they also add layers of complexity that increase the risk of system failure, particularly when different systems are not fully compatible.

A major concern in smart buildings is backward compatibility — ensuring that new updates or devices can function seamlessly with older, existing systems. Misalignment in compatibility can lead to issues like failed emergency response procedures if systems do not communicate effectively. Further, automatic updates introduce potential vulnerabilities if they interfere with the stability of life safety systems like smoke alarms or sprinkler controls. To address these challenges, experts recommend rigorous testing and certification requirements, such as UL 5500, the Standard for Remote Software updates, which defines protocols for remote software updates and requires authentication and validation processes to verify the integrity of updates to critical systems.





AI's role in advancing and complicating safety

AI technology offers promising advancements in fields like predictive maintenance, automated response and even real-time hazard detection.

However, the session stressed that while AI systems provide efficiency gains, they also raise concerns regarding decision reliability and accountability in safety-critical applications. AI models are prone to “hallucinations” or errors when interpreting data, which could lead to inappropriate responses in high-stakes environments such as healthcare or autonomous vehicles.

Experts warned against the misconception that AI technology can entirely replace human oversight. Instead, AI should be seen as a tool that augments human decision-making rather than replaces it. This was illustrated with examples of AI applications in industrial safety systems, where real-time data can help identify potential risks but still requires human interpretation to respond appropriately. The panelists also highlighted the ethical dimensions of AI, urging organizations to prioritize transparency and accountability, especially when using AI to make or inform critical safety decisions. Establishing regulatory frameworks for responsible AI use was considered an urgent priority as AI systems become more embedded in essential services.





“

The integration of smart technology in safety-critical applications is not without its risks. We must continually adapt our standards to meet new challenges.

Regulatory developments and standardization efforts

The session underscored that the global regulatory landscape for cybersecurity and technology-driven safety systems is both fragmented and complex.

Harmonization is key to making global cybersecurity practices effective, but differing standards across regions pose substantial challenges. The Cyber Trust Mark in the U.S., CE certification in Europe and various regional standards in Asia represent efforts by individual countries or regions to standardize cybersecurity practices, but inconsistencies make it difficult for manufacturers to ensure global compliance.

Harmonization efforts, like those underway in International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) committees, aim to reduce these inconsistencies, but this is a gradual process. In the meantime, companies must navigate a patchwork of regulations, adapting products to meet local standards while ensuring baseline security and interoperability. For the safety-critical sectors, especially those dealing with personal data, experts called for more alignment among regulatory bodies globally to simplify compliance and safeguard consumer trust. This collaboration would not only protect users but would also provide a clearer path for manufacturers looking to innovate across borders.



The environmental impact of technology deployment

“

With cybersecurity now integral to national security, regulatory frameworks must evolve just as swiftly as the technology they govern.

As the deployment of data-driven and energy-intensive technologies like AI and IoT grows, so does the environmental impact associated with them.

The energy consumption required to support large-scale AI models, for instance, has become a significant concern. It was noted that training a single large AI model can consume as much electricity as a small town, leading to a considerable environmental footprint. In response, experts advocated for the development of “frugal models,” which prioritize energy efficiency and focus on achieving specific, narrow objectives rather than broader, generalized applications.

Another approach discussed was edge computing, which processes data closer to the source rather than relying on large data centers, thereby reducing transmission energy costs. Attendees agreed that as new technologies are introduced, organizations must assess the environmental costs alongside their operational benefits. They called for collaborative efforts between regulatory agencies, the tech industry and environmental groups to establish standards and incentives that prioritize sustainable technology deployment.



BUILDING RESILIENCE IN THE AGE OF TECHNOLOGY

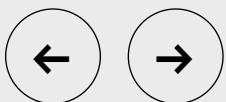
Conclusion

In closing, the conference reiterated the importance of a collective approach to tackling complex safety challenges in an era of rapid technological change. By fostering collaborative standards and innovative solutions, stakeholders can work together to create a future where technology serves humanity safely and sustainably.



KEY INSIGHTS AND FINDINGS

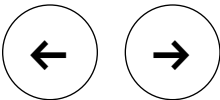
Global standards and sustainability in the era of AI and automation





Introduction

The second session of the CoC showcased dynamic discussions on the transformative advancements in technology and their implications for safety and innovation. Experts and panelists delved into critical topics, including AI, quantum computing and sustainable energy, emphasizing the crucial balance between technological progress and maintaining safety standards.



Key findings

AI and automation: A dual-edged sword

Advances in AI, automation and robotics create transformative opportunities to improve safety, efficiency and workflows. However, they also introduce challenges related to safety, privacy and ethics. Proactive collaboration among developers, regulators and end users, coupled with rigorous oversight, is essential to responsibly harness the potential of these technologies.

The rising importance of energy sustainability

The growing energy demands of AI and quantum computing emphasize the urgent need for sustainable solutions. Innovations such as small modular reactors (SMRs) and energy-efficient technologies like edge computing can help balance technological advancements with environmental stewardship. Companies must prioritize practices that mitigate environmental impacts while supporting innovation.

Collaboration: The key to effective governance

A collaborative approach across developers, regulators and consumers is critical for establishing trust and addressing challenges in the adoption of emerging technologies. Engaging safety scientists and industry stakeholders early in the development process helps ensure that technologies are designed with a comprehensive understanding of risks and real-world applications.

Global standards and harmonization challenges

The rapid evolution of AI, IoT and cybersecurity technologies necessitates adaptive, agile and globally harmonized standards. Unified frameworks are essential to mitigate risks, support innovation and address regional regulatory differences. UL Solutions’ dynamic approaches, such as Outlines of Investigation, provide a flexible approach to emerging technological challenges.

Ethical and societal considerations for AI

AI’s societal implications, including data privacy, misinformation and ethical challenges, require robust governance frameworks that consider public risks and cultural nuances. By embedding ethical considerations into risk management and regulatory processes, organizations can help ensure that AI technologies are developed and deployed responsibly to benefit society.



“

Safety allows innovation to have its intended impact. Without it, fear stifles potential progress.

AI and automation: A dual-edged sword



AI is reshaping industries by enabling automation in robotics, drones and autonomous vehicles.

A prime example is Waymo’s driverless taxi program, which has completed over 150,000 trips in cities like San Francisco and Austin. Panelists noted that these advancements promise increased safety in hazardous conditions, reduced operational costs and more efficient workflows. For instance, drones equipped with AI could perform inspections in dangerous environments, mitigating risks for human workers.

However, this progress comes with its own set of challenges. AI systems introduce risks related to safety, security, privacy and ethics. Autonomous vehicles must navigate complex environments without causing harm, while robotics and drones need secure, fail-proof systems to prevent malfunctions or cyberattacks. Generative AI technologies, which power applications like language models and content creation tools, have transformative potential but also pose risks such as bias, hallucinations and harmful outputs. For example, cases of AI-generated nonconsensual imagery illustrate the darker side of unchecked innovation.

Panelists emphasized the importance of integrating safety protocols into product development and testing phases. Transparency and collaboration among developers, regulators and end users were highlighted as key to fostering trust and ensuring that AI’s benefits outweigh its risks.



The rising importance of energy sustainability

The rapid adoption of AI and quantum computing is driving unprecedented energy demands.

Training large AI models like ChatGPT requires immense computational power, consuming an energy equivalent to that of small nations like Ireland. Such levels of energy consumption are unsustainable and conflict with global carbon reduction goals.

To address this, companies are turning to innovative solutions like SMRs. Google and Microsoft have announced partnerships to deploy SMRs for powering data centers, emphasizing their potential to provide scalable and sustainable energy sources. Additionally, advancements in energy-efficient technologies, such as edge computing, were discussed as ways to reduce the energy costs associated with data transmission and storage.

Panelists stressed the need for proactive measures to balance technological innovation with environmental stewardship. By investing in energy-efficient solutions and promoting sustainable practices, organizations can mitigate the environmental impact of emerging technologies while continuing to innovate.



Collaboration: The key to effective governance

The complexity of emerging technologies like AI and IoT demands a collaborative approach across multiple stakeholders. Panelists identified three key areas for effective collaboration:

Product development

Involving safety scientists, regulators and end users early in the development process helps ensure that AI products are designed with a comprehensive understanding of risks and real-world applications. By integrating diverse perspectives, companies can create safer, more reliable technologies.

Standards and regulation development

Collaboration among technical professionals, regulators and industry representatives is essential to develop standards that address the concerns of all stakeholders. For example, AI benchmarks recently introduced by UL Solutions aim to establish clear criteria for evaluating AI safety and performance, promoting transparency and trust.

Bridging research and industry

Panelists noted a critical gap between academic AI research and its practical applications in industry. Industry-focused conferences often exclude academic research, while academic conferences prioritize theoretical advancements over applied solutions. Bridging this gap would enable a more holistic understanding of technological advancements and their practical implications.

Panelists also emphasized the importance of building public trust by fostering transparency and explainability in AI systems. This involves clear communication of how AI algorithms operate and active engagement with users to address concerns and misconceptions.





Global standards and harmonization challenges

The fragmented nature of global regulations poses a significant challenge to the adoption of AI, IoT and cybersecurity technologies.

While frameworks like the EU AI Act, the U.S. executive order on AI and China's draft AI law share common principles — such as data privacy, accountability and performance predictability — regional differences complicate harmonization efforts.

Panelists proposed adaptive governance models as a solution to this challenge. Dynamic standards that can evolve alongside technological advancements are critical for ensuring that regulations remain relevant. For instance, Outlines of Investigation allow for nimble adjustments to emerging risks while laying the groundwork for formalized standards.

Collaborative efforts among international regulatory bodies, such as the IEC, were highlighted as key to creating globally aligned standards. By fostering a unified regulatory framework, stakeholders can enable seamless innovation across borders while addressing regional cultural and societal nuances.





Ethical and societal considerations in AI

“

AI advancements are reshaping industries, but ethical and societal concerns must guide their adoption.

The societal impacts of AI extend beyond technical challenges, encompassing ethical dilemmas such as data privacy, misinformation and psychological effects.

For instance, cultural differences in privacy norms, ranging from Europe’s strict General Data Protection Regulation (GDPR) to China’s minimal privacy expectations, complicate the creation of universal standards.

Panelists highlighted the need to incorporate societal and cultural dimensions into governance frameworks. For example, the UL organizations’ AI safety investigation includes measures to identify and mitigate risks related to disinformation and polarization, which are increasingly recognized as critical societal concerns.

Another challenge lies in addressing the ethical use of AI in research and open-source applications. Panelists cited examples of generative AI being used to create harmful content, such as nonconsensual imagery or AI-generated child exploitation materials. These cases underscore the importance of implementing safeguards to prevent the misuse of AI tools.

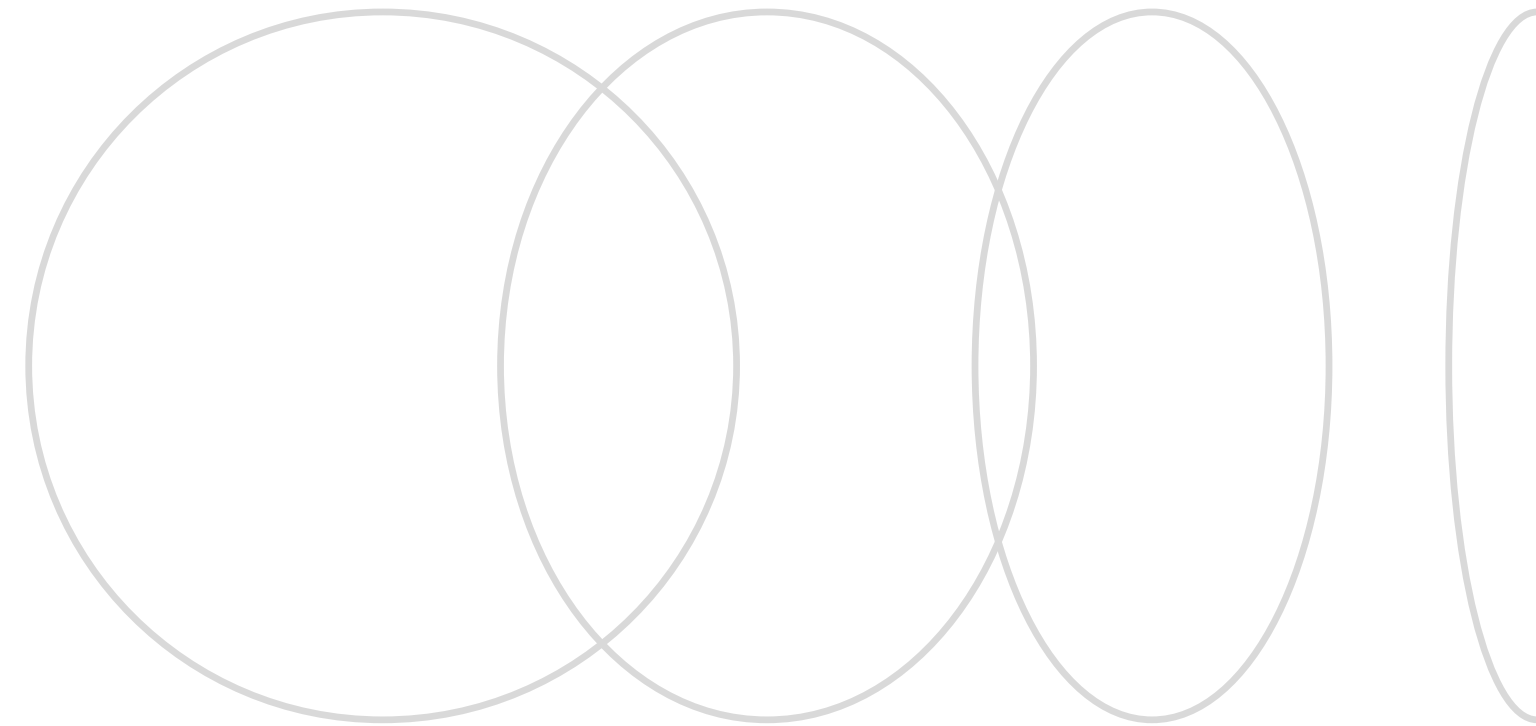
By embedding ethical considerations into regulatory and risk management frameworks, organizations can ensure that AI technologies are developed and deployed responsibly, benefiting society as a whole.

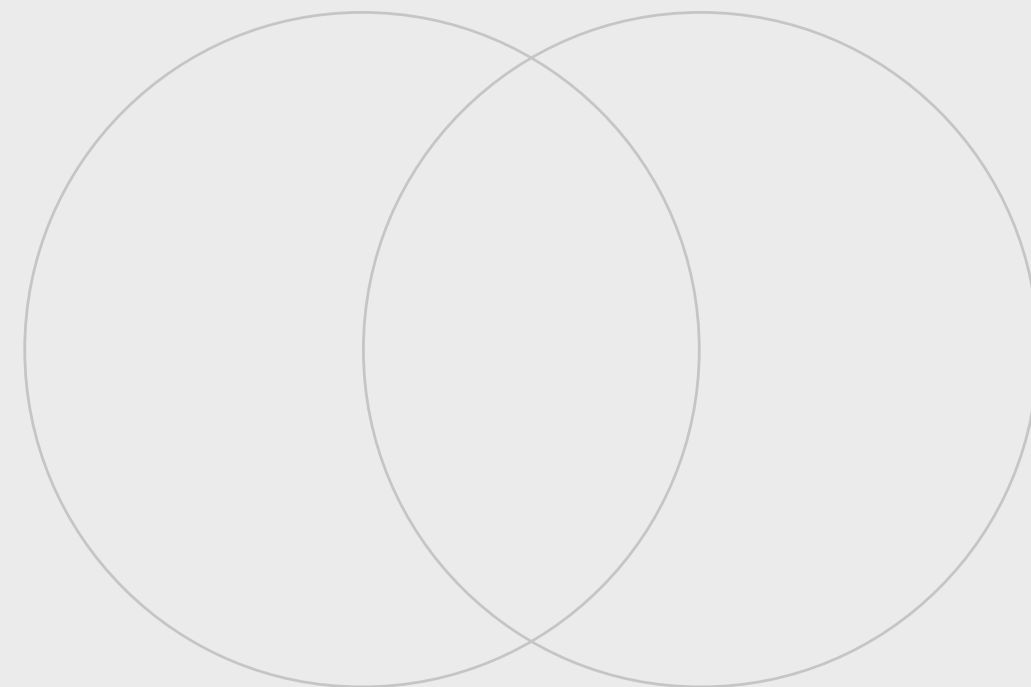


GLOBAL STANDARDS AND SUSTAINABILITY IN THE ERA OF AI AND AUTOMATION

Conclusion

The discussions highlighted the critical need to balance innovation with safety through collaborative, adaptive and ethically grounded approaches. By prioritizing transparency, fostering trust and promoting global cooperation, stakeholders can effectively address the complexities of emerging technologies while maximizing their positive impact on society.





KEY INSIGHTS AND FINDINGS

Digital twins, AI and the industrial metaverse shaping the future





Introduction

The third session of the CoC brought together industry leaders to explore how emerging technologies are transforming industries while redefining safety, collaboration and governance frameworks. The session offered valuable insights into the challenges and opportunities of adopting technologies such as AI, digital twin simulations and industrial metaverse applications, underscoring the pivotal role of cross-ecosystem collaboration in driving innovation and ensuring safety.

Key findings

The digital twin revolution and its role in innovation

Digital twin technologies are transforming industries by enabling realistic simulations, predictive modeling and operational efficiency. Their adoption is vital for improving safety and reducing costs, but requires strong foundational systems.

Democratizing technology to bridge inequality

Smaller enterprises face unique challenges in adopting emerging technologies due to budget constraints and work force readiness. Democratizing access to technology can level the playing field and enhance innovation across sectors.

Collaboration as a catalyst for safety and standardization

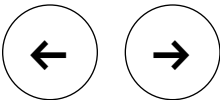
Effective collaboration across developers, regulators and industries is essential for creating safety standards that support innovation without stifling creativity or adoption.

Regulation and governance in a rapidly changing landscape

The agility of regulatory frameworks is critical to accommodating rapid technological advancements. A balance between safety, innovation and market demand is essential for future success.

The industrial metaverse: A vision for the future

The industrial metaverse combines digital twins, simulation and real-time data to optimize operations and help ensure safety in ways never before possible.





The digital twin revolution and its role in innovation



“

Digital twin technology is transforming industries by enabling realistic simulations and predictive modeling, paving the way for safer, more efficient innovations.

Digital twin technology emerged as a cornerstone for the future of innovation during the panel.

A digital twin is a virtual representation of a physical product, process or system, enabling organizations to test scenarios, predict outcomes and optimize performance without physical prototypes. For example, Siemens recently achieved certification for a drive using primarily digital twin technology, reducing costs and increasing accuracy in development.

These models are critical for industries like automotive, where reducing physical prototypes not only cuts costs but also enhances safety by allowing simulations to identify potential failures before production. Another application discussed was the use of digital twins in life sciences, where the Food and Drug Administration (FDA) partnerships have demonstrated how digital twins streamline regulatory compliance and accelerate product approvals.

However, successful implementation of digital twins depends on robust foundational systems, such as digital threads that connect data across an organization. Without these systems, companies risk optimizing in silos, undermining the full potential of digital twins.



Collaboration as a catalyst for safety and standardization



The panel underscored the importance of collaboration in addressing safety and standardization challenges.

In complex ecosystems, partnerships between developers, regulators and standard organizations like UL Solutions play a pivotal role in creating globally recognized frameworks.

In renewable energy, for instance, regulatory complexities and soft costs account for nearly 60% of deployment expenses. Streamlining permitting and trial-based approaches to regulation could accelerate adoption and reduce costs for consumers.

The integration of hardware and software also requires standardization to ensure interoperability across global markets. Standardized data communication protocols — likened to a “language translator” for digital threads — were highlighted as a way to enhance collaboration and facilitate ecosystem-wide innovation.



Democratizing technology to bridge inequality

Adopting emerging technologies poses unique challenges for SMEs, which often lack the resources of larger corporations.

SMEs, which employ 75% of the U.S. manufacturing work force, face barriers such as limited budgets, work force readiness and the cost of replacing legacy systems.

Panelists emphasized that technologies like AI could serve as an equalizer, providing SMEs with tools to access expertise and innovate more effectively. For example, AI-driven tools can enable smaller companies to analyze data, optimize operations and reduce time to market for new products.

Efforts to democratize technology must also address work force training and education. Ensuring that employees can effectively use new tools is as critical as the tools themselves. By investing in accessible technologies and work force development, industries can foster broader participation in the innovation ecosystem.





Regulation and governance in a rapidly changing landscape

Rapid technological advancements demand regulatory frameworks that are both agile and adaptive.

Traditional approaches to regulation, which can take years to develop, risk the regulations becoming obsolete by the time they are implemented. Panelists called for a shift toward more dynamic, living standards that evolve alongside technologies.

For example, the energy sector faces unique challenges as new materials and autonomous technologies like battery optimization systems are introduced. Clear safety codes and regulatory guidelines are often lacking, creating uncertainty that slows adoption. A collaborative approach between industry leaders, regulators and standards organizations can bridge this gap, enabling faster and safer implementation of emerging technologies.

Agility in governance also requires global harmonization. Divergent regional standards can impede innovation and create inefficiencies for multinational corporations. Panelists stressed the need for unified international standards that balance safety with market needs.



The industrial metaverse: A vision for the future

“

The industrial metaverse offers a photorealistic environment for optimizing operations, ensuring worker safety and democratizing access to cutting-edge technology.

The industrial metaverse represents the next frontier in combining digital twin technology, simulation and real-time data.

Unlike consumer-focused metaverse applications, the industrial metaverse is rooted in realistic modeling and practical use cases.

In this environment, companies can simulate entire production facilities, optimize processes and help ensure worker safety through virtual commissioning. For instance, industrial metaverse applications can preprogram safety protocols for robotic systems, shutting them down automatically when workers enter restricted zones.

The benefits extend to auditing and compliance as well. With photorealistic simulations, companies can audit facilities remotely, reducing the need for on-site inspections. This technology also has profound implications for training, allowing workers to practice tasks in a risk-free, virtual environment before applying their skills in the real world.

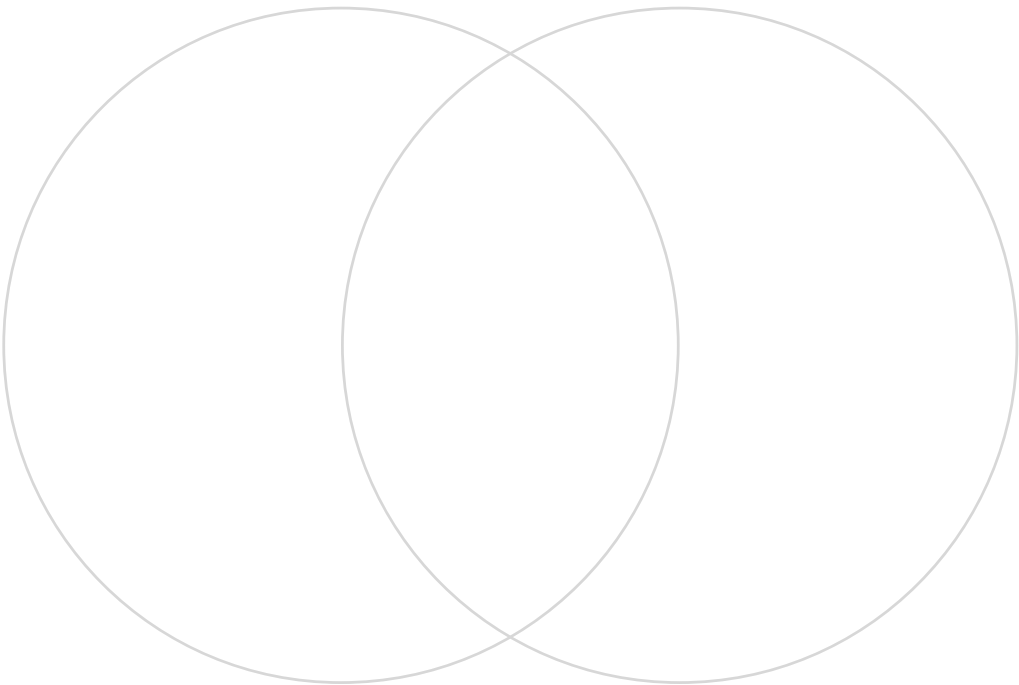
While still in its early stages, the industrial metaverse offers transformative potential for enhancing safety, efficiency and collaboration across industries.



DIGITAL TWINS, AI, AND THE INDUSTRIAL METAVERSE SHAPING THE FUTURE

Conclusion

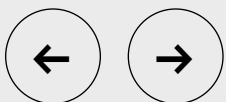
The discussion highlighted the transformative potential of emerging technologies like digital twins, AI and the industrial metaverse. These innovations promise to revolutionize industries, but their success depends on collaboration, democratization and adaptive governance frameworks. By working together, stakeholders can navigate the complexities of technological change and unlock a safer, more sustainable future.





KEY INSIGHTS AND FINDINGS

Enhancing and expanding relevance





Introduction

The CoC focuses on generating actionable insights and findings gathered during collaborative sessions focused on improving communication, accessibility and understanding of code changes and training for professionals in the fire safety and building industries.

Key areas explored

Challenges in accessing code updates and training

Understanding the challenges stakeholders face in keeping their teams updated and trained on evolving codes and technologies while balancing limited resources and competing priorities

Tailored information delivery

Identifying effective ways to deliver relevant and impactful information to authorities having jurisdiction (AHJs) in the field to support their daily decision making and responsibilities

Team awareness and adoption

Examining how AHJs can navigate complex updates to determine actionable steps for compliance and effective jurisdictional implementation

A comprehensive exploration of these themes provides stakeholders with strategies to bridge gaps in information dissemination, foster collaboration and support effective implementation of code changes. It serves as a resource for organizations to enhance safety, compliance and stakeholder engagement within their communities.



Challenges in accessing code updates and training

Professionals across the fire safety and building industries rely on a diverse array of sources to stay informed about code changes and training opportunities.

Trusted organizations like the NFPA, ICC and the three UL organizations serve as the backbone of this knowledge, offering newsletters, workshops and webinars that cater to varying levels of expertise. However, despite the breadth of options, significant challenges persist:

- One major obstacle is cost. Students, universities and smaller organizations frequently find the price of subscriptions and training prohibitive, creating accessibility gaps. Additionally, while networking with peers and attending conferences are highly valued, these opportunities are not always feasible due to scheduling conflicts or resource constraints.
- Another common frustration is the inconsistent quality of available training. Manufacturer-led sessions, while abundant, are often viewed with suspicion due to their commercial bias. Similarly, online resources like third-party webinars and newsletters vary widely in credibility. Professionals have called for more rigorous vetting processes and publicly available ratings for training programs and instructors.
- The disconnection between field units and broader resources poses a unique challenge, particularly for fire services. Without centralized or well-integrated information systems, field inspectors often miss critical updates or rely on ad hoc sources like consultants or hotline support.

To address these issues, there is growing demand for on-demand learning options that fit into busy schedules, as well as more structured collaboration between organizations. Trial-based regulatory approaches and enhanced use of digital tools like vetted newsletters and professional webinars could streamline access to critical information.



Below are commonly mentioned sources for code changes and training:

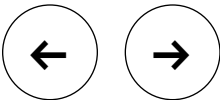
- Trusted organizations – Professional bodies such as the NFPA, the Society of Fire Protection Engineers (SFPE), the ICC, UL Standards & Engagement, UL Solutions and state departments are primary sources for updated codes and training.
- Diverse information channels – Newsletters, bulletins, emails, professional societies and direct communication with code authorities are common channels.
- Networking and peer sharing – Word of mouth, discussions with colleagues and networking with designers, AHJs and manufacturers serve as key informal sources.
- Training sessions – A mix of live events, on-demand recordings, workshops and third-party webinars is used, though quality varies widely.
- Consultants and external expertise – Many professionals hire consultants or attend lunch-and-learns to stay current on changes.
- In-person learning – Conferences, conventions and code hearings remain critical for direct engagement with updates and experts.

By addressing these gaps and fostering collaboration across stakeholders, the fire safety and building industries can foster more equitable access to reliable, high-quality training and code updates, ultimately enhancing safety and compliance outcomes.

“

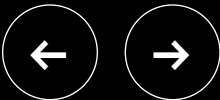
[I would like to see] the availability of training in emerging technologies earlier in its use. Technology is changing so quickly it is difficult if not impossible to keep up with and will be more so in the future.

– Council participant





Preferred ways to receive updates regarding codes and standards



Accessing updates on codes and standards is critical for professionals to stay informed and compliant in their fields. However, the methods and channels for receiving these updates vary based on individual preferences, convenience and effectiveness.

Below are the key formats identified for how professionals prefer to receive and engage with updates, highlighting both trusted sources and the challenges they face in accessing relevant information and training. These insights underscore the importance of clarity, accessibility and flexibility in communication and delivery methods.

- **Newsletters and e-letters** – Regular newsletters with links to more detailed information are appreciated, especially when written in plain language.
- **On-demand content** – Access to training modules, commentary and webinars that can be consumed at one’s convenience is essential.
- **Peer networks** – Word of mouth, networking and colleague recommendations remain trusted sources of updates.
- **Searchable and accessible resources** – Searchable documents and easy-to-navigate websites for finding specific information are key.
- **Social media and digital platforms** – Platforms like LinkedIn, Twitter (X) and YouTube are effective for sharing major updates in concise formats.
- **Regional and local engagement** – Regional meetings, state-specific notifications and local representatives offering updates foster direct community engagement.
- **Interactive and consolidated updates** – Workshops, trade shows and consolidated interactive webinars are preferred for in-depth engagement.
- **Continuing education opportunities** – Professionals value continuing education classes that are aligned with updates and offer practical insights.

The need for clear, accessible and flexible communication methods is critical. By leveraging these preferred formats, ranging from webinars and newsletters to peer networks and on-demand content, organizations can effectively meet professionals where they are.



Desired types of information for delivery

Tailored and practical communication are critical for professionals to stay informed and efficient in their roles. The key to effective information delivery lies in clarity, relevance and usability.

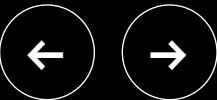
Concise, accessible summaries are paramount. Professionals appreciate the “keep it simple, stupid” (KISS) approach, with updates that provide a high-level overview of significant changes and direct users to more detailed resources. Clarity on impact and implementation is equally important; users need to understand what the changes mean for them, when they will take effect and any associated challenges.

Another priority is the rationale behind updates. Professionals value insights into the “why” behind the changes, including the intent of technical committees and the reasoning behind new standards. This transparency helps them better align their work with industry goals and anticipate future trends.

Below are favored forms of information as indicated by industry professionals:

- **Concise summaries** – Short, easily digestible summaries of important changes with links to more details
- **Impact and implementation** – Clear explanations of what changes mean for users, including timelines and implementation challenges
- **Ongoing debates and trends** – Updates on current proposals, timelines, emerging trends and notable evaluations
- **Training opportunities** – Information on training options, both online and offline, ideally consolidated across organizations
- **Practical tools and resources** – Resources to assist in day-to-day tasks, such as contact lists, case studies or FAQs
- **Regional and topic-specific updates** – Updates tailored to regional needs or specific topics, including trends and industry-specific insights
- **Product and investigation results** – Data on fully evaluated products, notable investigation results and product failures to inform decision making
- **Interactive feedback channels** – Surveys, requests for input and opportunities to engage on specific topics

By focusing on these needs, organizations can deliver information that enhances understanding, fosters compliance and drives engagement across the professional community.





Ensuring team awareness and understanding of code changes

Ensuring that teams are well-informed and understand the practical implications of code changes is a multifaceted challenge for organizations in the fire safety and building industries. Clear, consistent communication is critical for addressing these challenges effectively.

- A key priority is the standardization of messaging and training materials. Consistent formats and styles, such as bullet-point summaries, key takeaway reports or content packages for learning management systems, simplify communication and improve adoption rates. Flexibility in delivery methods is also essential.
- Teams emphasize the importance of explaining the rationale behind changes, as understanding the “why” fosters better engagement and application. This is especially important for changes that introduce complex or unfamiliar requirements, where practical impact statements and implementation guides are invaluable.
- Time constraints remain a pervasive issue, with many professionals finding it difficult to balance day-to-day responsibilities with the demands of ongoing training. To mitigate this, organizations are increasingly relying on lunch-and-learn sessions, weekly huddles and concise, on-demand resources that fit into busy schedules.
- Another common challenge is information overload, particularly when dealing with multiple updates or complex codes. Simplifying content and focusing on key points helps ensure that critical information is not lost in translation.



Below are best practices for ensuring team awareness and understanding of code changes:

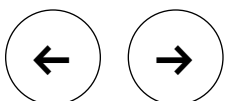
- **Clear messaging and standardization** – Standardizing communication methods with consistent formats and messaging helps ensure easier adoption.
- **Simple, actionable training** – Clear and concise training with defined key takeaways is critical, especially given time constraints.
- **Practical impact explanation** – Teams benefit from detailed explanations of the change’s implications, including how it affects daily responsibilities and why it is necessary.
- **Flexible training approaches** – Depending on the significance of the change, strategies range from short memos for minor updates to full-day training sessions for larger impacts.
- **Workshops and team meetings** – Regular team meetings, workshops and lunch-and-learn sessions provide opportunities for discussion and clarification.
- **Content for internal systems** – Providing learning content packages that integrate into existing learning management systems helps ensure consistency and scalability.
- **Localized adjustments** – State and local amendments add complexity, requiring tailored communication and accessible expertise.
- **Accessibility for questions** – Ensuring immediate access to support, such as a hotline or AHJ, helps address lingering questions and uncertainties.

By adopting these strategies and addressing the challenges of time, complexity and retention, organizations can ensure that their teams are not only informed but also empowered to implement changes effectively in their daily work.

“

[I would like to see] opportunities to engage across disciplines — AHJs with technology leaders, fire AHJs with electrical, etc. — to share how each discipline is handling their different but parallel challenges.

– Council participant



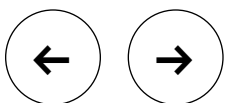


ENHANCING AND EXPANDING RELEVANCE

Conclusion

The insights and strategies outlined in this document provide a road map for enhancing communication, accessibility and understanding of code changes and training within the fire safety and building industries. By addressing key challenges such as cost barriers, inconsistent training quality and fragmented resources, and by emphasizing the importance of clarity, tailored delivery methods and flexible learning opportunities, organizations can better equip professionals to navigate an ever-evolving landscape.

Furthermore, fostering collaboration among stakeholders, leveraging technology and prioritizing vetted, practical information will bridge critical gaps in knowledge dissemination. These efforts not only enhance compliance and safety outcomes but also strengthen industry-wide engagement and trust. As the demands of these industries continue to grow, the adoption of these strategies will support a more resilient, informed and prepared professional community capable of meeting future challenges head-on.





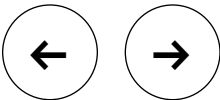
RECOMMENDATIONS

The 2024 Convening of the Councils showcased how innovation and safety intersect in a rapidly evolving technological landscape.

AI, IoT and digital twins present transformative opportunities for improving safety and operational efficiency across the fire, electrical and security sectors. However, they also demand proactive measures to mitigate risks, adapt regulatory frameworks and align global standards.

AHJs stand at the forefront of this transformation. By collaborating with testing, inspection and certification (TIC) organizations and industry stakeholders, AHJs can shape safety frameworks that meet the challenges of emerging technologies. The following recommendations and actions provide a road map for leadership and collaboration in this dynamic ecosystem.

Recommendation	Action	Add your plans for implementation here
Drive cross-sector collaboration	Establish multi-stakeholder working groups to address interoperability, aligning AHJs, TIC organizations and industry players on unified goals.	
Integrate emerging technologies safely	Pilot programs with AI- and IoT-based systems to evaluate their impact on safety protocols and refine best practices for broad implementation.	
Enhance accessibility of standards	Develop centralized platforms for on-demand access to code updates, training modules and technical resources for professionals and inspectors.	
Promote sustainability in safety practices	Partner with industry leaders to create standards emphasizing innovations such as environmentally friendly fire suppression agents and energy-efficient designs.	
Strengthen adaptive regulatory frameworks	Implement dynamic regulatory models that can evolve with technological advancements, using trial-based approaches to assess and refine standards.	





CONCLUSION

The 2024 CoC underscored the transformative potential of integrating emerging technologies into safety-critical industries.

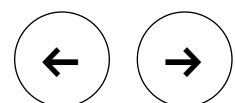
Key discussions highlighted the dual nature of innovation, offering unprecedented opportunities for predictive analytics, automation and efficiency while introducing complexities in governance, cybersecurity and environmental impact. For example, AI-enabled systems and digital twins have revolutionized simulation capabilities, but their full potential can only be realized through collaboration and aligned standards.

The fire, electrical and security sectors are at a pivotal moment. Attendees explored how sustainable practices, such as modular nuclear reactors and energy-efficient systems, can balance technological growth with environmental stewardship. Discussions also emphasized the importance of democratizing training resources and embedding ethical considerations into technology deployment.

A recurring theme was the need to democratize access to training and resources, ensuring equitable knowledge dissemination across all professional levels. Ethical considerations were also front and center, with attendees stressing the importance of transparent and accountable frameworks for deploying transformative technologies.

The CoC is more than an event; it is a longitudinal effort to shape the future of safety standards. By fostering continuous engagement through follow-up sessions, case studies and ongoing collaboration, the CoC provides a platform to monitor progress, refine strategies and adapt to new challenges. Future conferences will build on the foundations laid here, enabling stakeholders to leverage insights, strengthen partnerships and drive impactful actions.

In addition to participating in the next CoC and similar convenings, join The Code Authority (www.UL.com/TCAcommunity) and reaffirm your commitment to proactive leadership and collaborative innovation. Together, we can help ensure that safety remains a cornerstone of technological advancement, creating a sustainable and more secure future for all. Let us continue this journey, harnessing the power of collective expertise to turn challenges into opportunities and inspire transformative progress.





M E T H O D O L O G Y

Effective stakeholder engagement is pivotal for the success of initiatives like the CoC.

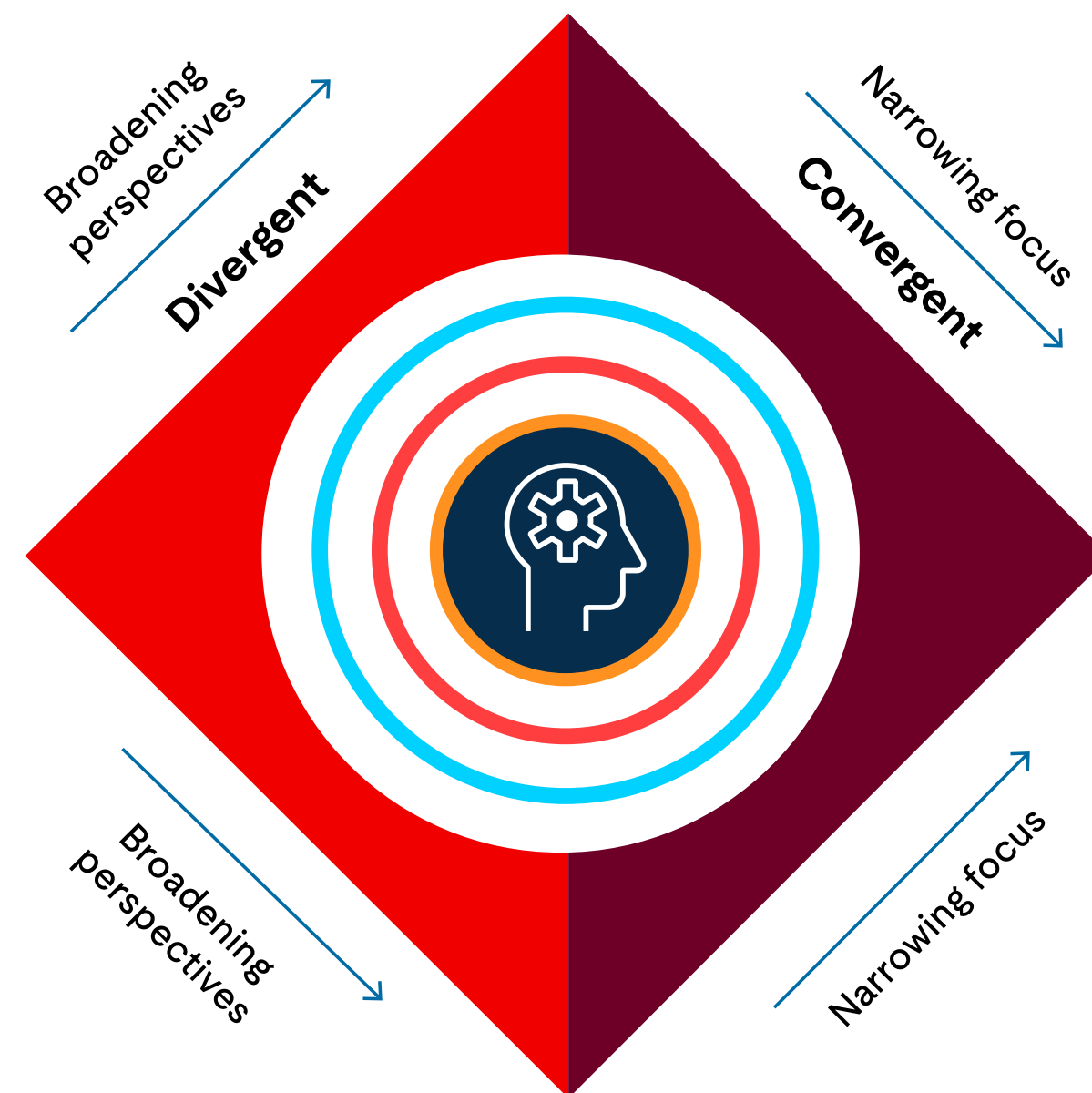
A structured methodology helps ensure that diverse perspectives are harnessed to address emerging safety challenges comprehensively. This methodology integrates established facilitation techniques — notably, the divergent and convergent thinking processes exemplified by the “diamond approach” — to foster inclusive and productive discussions.

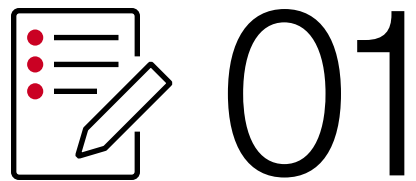
● Divergent thinking

Divergent thinking refers to the process of generating a wide range of ideas, solutions and perspectives. In the context of innovation, it involves encouraging participants to explore multiple — often unconventional — pathways when discussing challenges and opportunities. This broad, open-ended approach helps stimulate creativity, uncover hidden insights and challenge existing assumptions. During the CoC, divergent thinking is essential for expanding the dialogue, helping to ensure that participants consider a variety of possibilities when addressing the complexities of emerging technologies in the fire, security and electrical industries.

● Convergent thinking

Convergent thinking, on the other hand, is the process of refining and focusing ideas and selecting the most viable and relevant solutions from the range of possibilities generated during divergent thinking. Convergent thinking helps participants distill insights, synthesize the dialogue, and identify the key opportunities and challenges that will drive actionable results. It is crucial for bringing the discussions to a point of clarity and consensus, ensuring that the innovation process is not only exploratory but also delivers focused, implementable outcomes.





Preparation and planning

Before convening stakeholders, meticulous preparation is essential.

Stakeholder identification and mapping

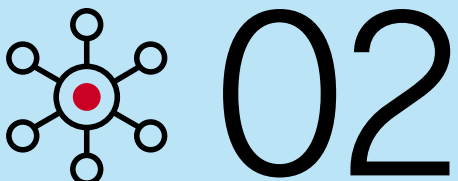
Identify all relevant stakeholders, including government agencies, regulatory bodies, academic institutions, industry organizations and consumer representatives. Mapping these stakeholders helps clarify their interests, influence and potential contributions. This step helps ensure that the engagement process is inclusive and considers all pertinent viewpoints.

Defining objectives and outcomes

Clearly articulate the objectives of the engagement. Establishing specific, measurable outcomes guides the process and provides benchmarks for evaluating success. This clarity helps ensure that all participants have a shared understanding of the goals.

Logistical arrangements

Plan the logistics, including selecting a neutral venue, scheduling sessions at convenient times and ensuring necessary resources are available. Attention to these details creates an environment conducive to open dialogue.



Facilitating divergent thinking

Divergent thinking encourages the generation of a wide array of ideas and perspectives.

Brainstorming sessions

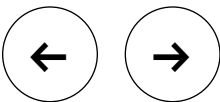
Facilitate sessions where participants freely share ideas without immediate evaluation. This openness fosters creativity and helps ensure that unconventional solutions are considered.

Mind mapping

Utilize mind mapping techniques to visually represent ideas and their interconnections. This approach helps in organizing thoughts and identifying relationships between concepts.

Encouraging diverse perspectives

Create an inclusive environment where all participants feel comfortable sharing their views. Diversity in thought leads to more comprehensive problem solving.





Navigating the “groan zone”

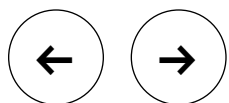
The transition from divergent to convergent thinking often involves navigating the “groan zone,” a phase characterized by confusion and frustration as the group processes diverse ideas.

Acknowledging the phase

Recognize that the “groan zone” is a natural part of group decision making. Acknowledging this helps participants remain patient and committed to the process.

Structured facilitation

Employ facilitation techniques such as summarizing discussions, clustering similar ideas and revisiting objectives to help the group move through this phase. These strategies provide clarity and direction.



Facilitating convergent thinking

Convergent thinking focuses on narrowing down options and making decisions.

Prioritization techniques

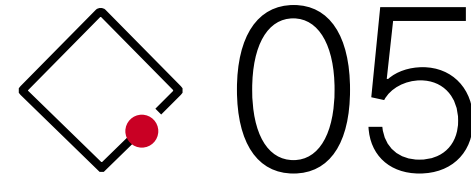
Use methods like multi-voting or dot voting to identify the most promising ideas. These techniques help in objectively assessing options.

Criteria development

Establish clear criteria for evaluating ideas, such as feasibility, impact and alignment with objectives. This helps ensure that decisions are made systematically.

Consensus building

Facilitate discussions aimed at reaching consensus, striving to make sure that all voices are heard and considered. This collaborative approach fosters buy-in and commitment to the decisions made.



Implementing the diamond approach

The “diamond approach” visually represents the process of divergent and convergent thinking.

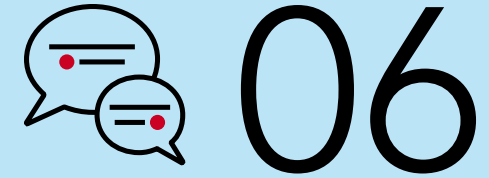
Divergence phase

The first half of the diamond represents the expansion of ideas, where the focus is on generating a broad spectrum of possibilities.

Convergence phase

The second half signifies the narrowing down of options, focusing on selecting and refining the most viable solutions.

This approach supports a balanced process that values both creativity and critical evaluation.



Continuous engagement and feedback

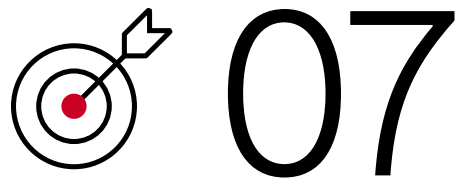
Maintaining ongoing engagement with stakeholders is crucial.

Regular updates

Provide stakeholders with consistent updates on progress and how their input is being utilized. Transparency builds trust and demonstrates the value of their contributions.

Feedback mechanisms

Establish channels for stakeholders to provide feedback throughout the process. This iterative approach allows for continuous improvement and responsiveness to stakeholder needs.



Evaluation and reflection

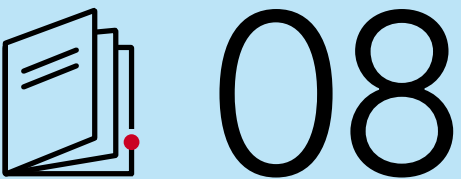
After the engagement process, evaluate its effectiveness.

Assessing outcomes

Compare the results against the predefined objectives to determine success. This assessment provides insights into what worked well and areas for improvement.

Reflective sessions

Conduct debrief sessions with stakeholders to gather their perspectives on the process. This reflection fosters learning and enhances future engagements.



Documentation and reporting

Thorough documentation helps ensure that insights and decisions are recorded.

Comprehensive records

Maintain detailed records of discussions, decisions and rationales. This documentation serves as a reference and supports transparency.

Accessible reports

Prepare reports that are accessible to all stakeholders, summarizing key findings and outlining next steps. Clear communication of outcomes reinforces stakeholder engagement.

A rigorous and thoughtful methodology for convening stakeholders and incorporating structured facilitation techniques and continuous engagement is essential for addressing complex challenges effectively. By embracing both divergent and convergent thinking processes and navigating the “groan zone” with structured facilitation, the Convening of the Councils can harness diverse expertise to develop comprehensive and innovative safety solutions.



Additionally, consistent with market best practices, the CoC was structured to allow for further analysis of industry challenges and opportunities, as well as leading actions being deployed in service of addressing them.

Specific techniques used to analyze the CoC include:

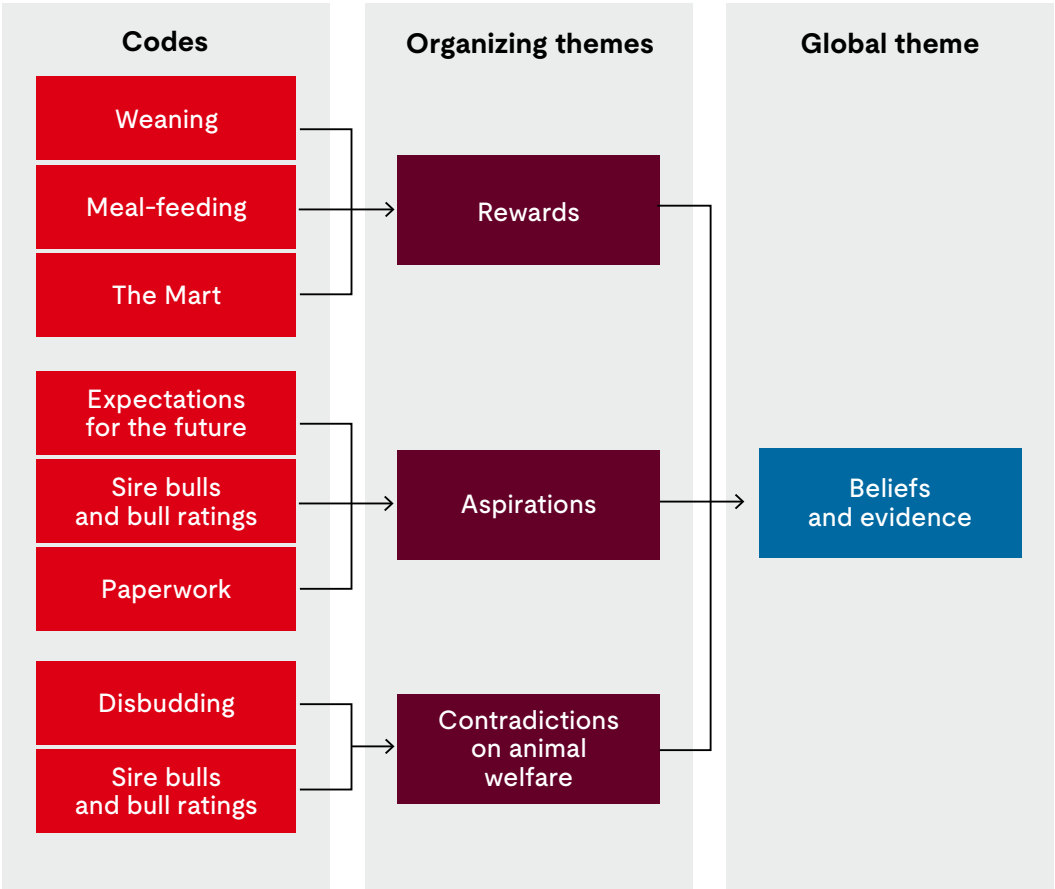
Thematic analysis

Objective

Identify recurring themes in the workshops around the challenges and solutions associated with evolving technologies.

Process

- Transcribe and segment the discussions into manageable units, e.g., key points or statements.
- Use coding techniques to tag relevant themes such as “system integration challenges,” “cybersecurity threats,” “AI deployment hurdles,” etc.
- Group similar codes into categories and identify overarching themes like technological complexity, regulatory gaps and innovation potential.
- Develop a narrative around each theme, analyzing how they relate to industry growth or obstacles.



Example of a thematic analysis



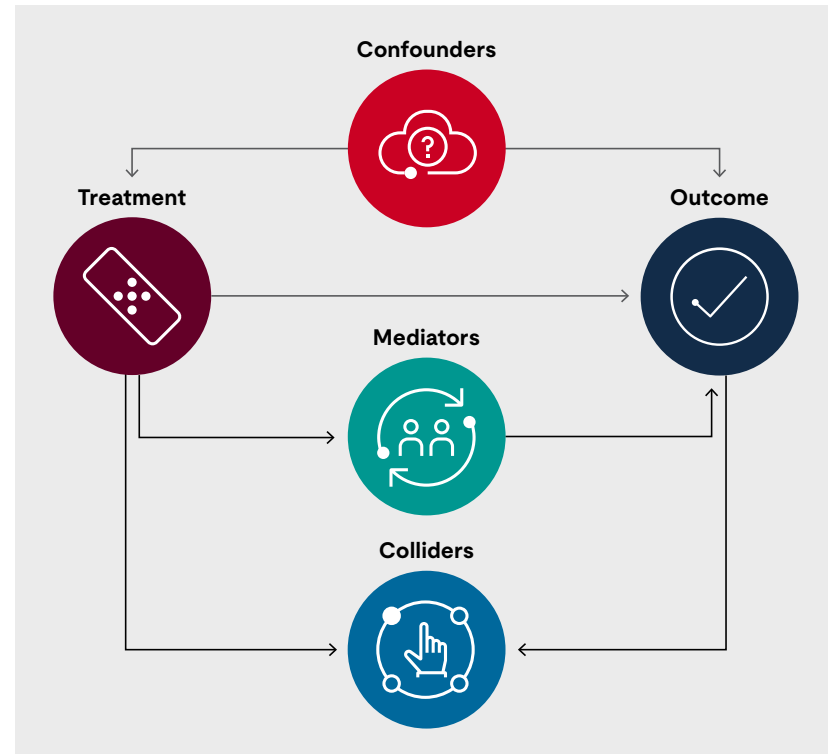
Causal diagrams

Objective

Visualize the cause–effect relationships between different factors discussed in the workshops, e.g., how the implementation of AI might increase system integration challenges or alleviate certain cybersecurity issues.

Process

- Identify key variables from the discussions, e.g., cybersecurity threats, system integration complexity and AI innovations.
- Map the relationships between these variables to understand how challenges in one area might drive or mitigate issues in another.
- Use these diagrams to show how emerging technologies interact and influence industry operations.



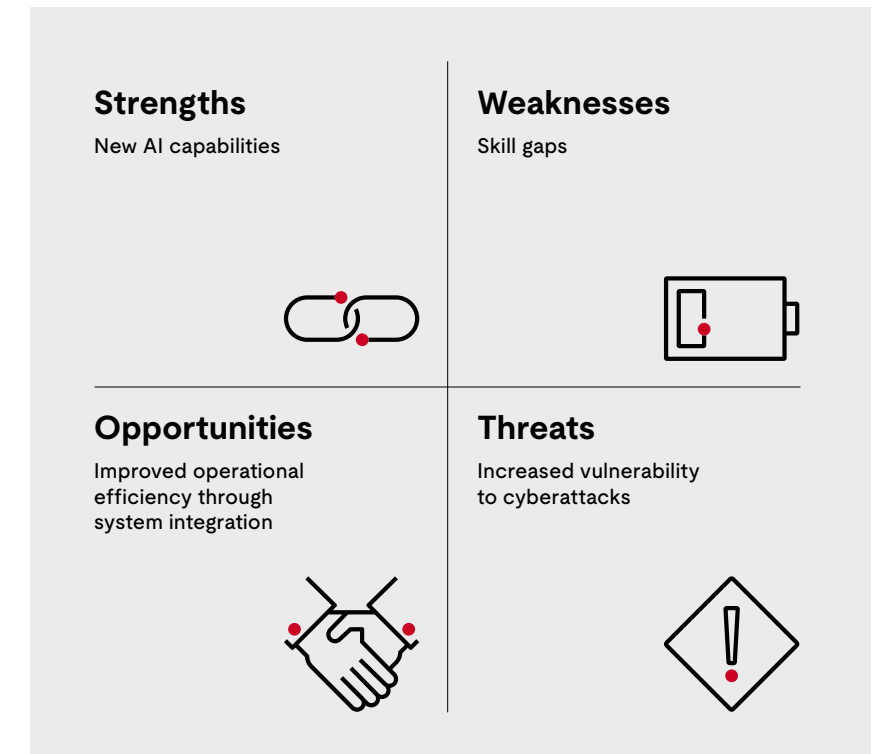
SWOT analysis

Objective

Analyze the strengths, weaknesses, opportunities and threats related to evolving technologies in these industries.

Process

- Categorize the insights from the workshops into strengths, e.g., new AI capabilities; weaknesses, e.g., skill gaps; opportunities, e.g., improved operational efficiency through system integration; and threats, e.g., increased vulnerability to cyberattacks.
- Summarize this analysis to provide a clear strategic outlook for the industries.



Example of a SWOT analysis



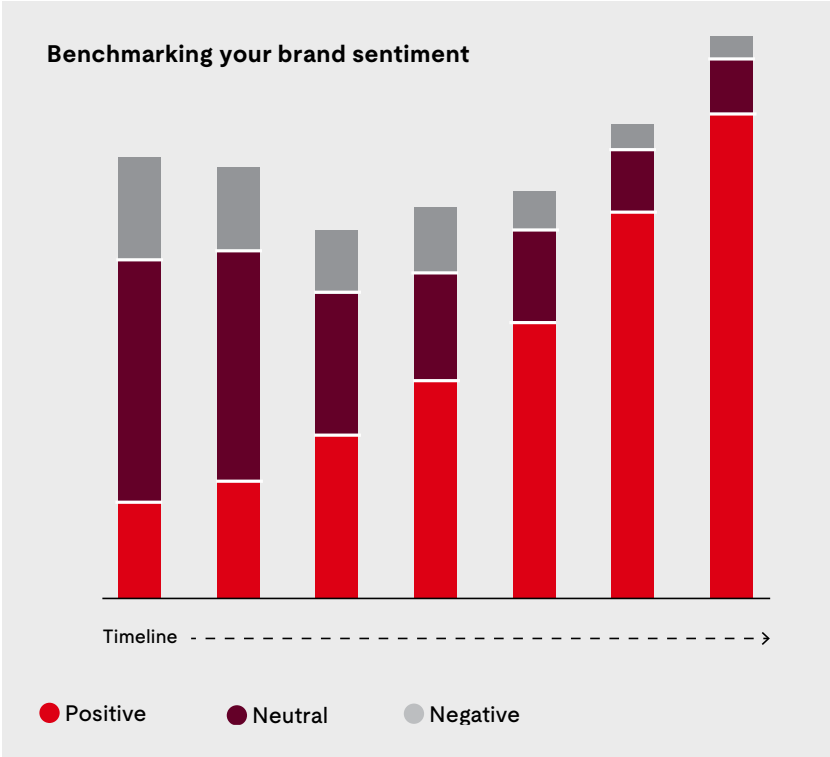
Sentiment and trend analysis

Objective

Gauge the overall sentiment (positive, neutral or negative) around specific technologies and their impact.

Process

- Use qualitative sentiment analysis tools (manual or software-based) to determine how participants feel about specific topics like AI and cybersecurity.
- Identify trends that may emerge, such as growing optimism toward AI-driven solutions or increased concern about regulatory frameworks.



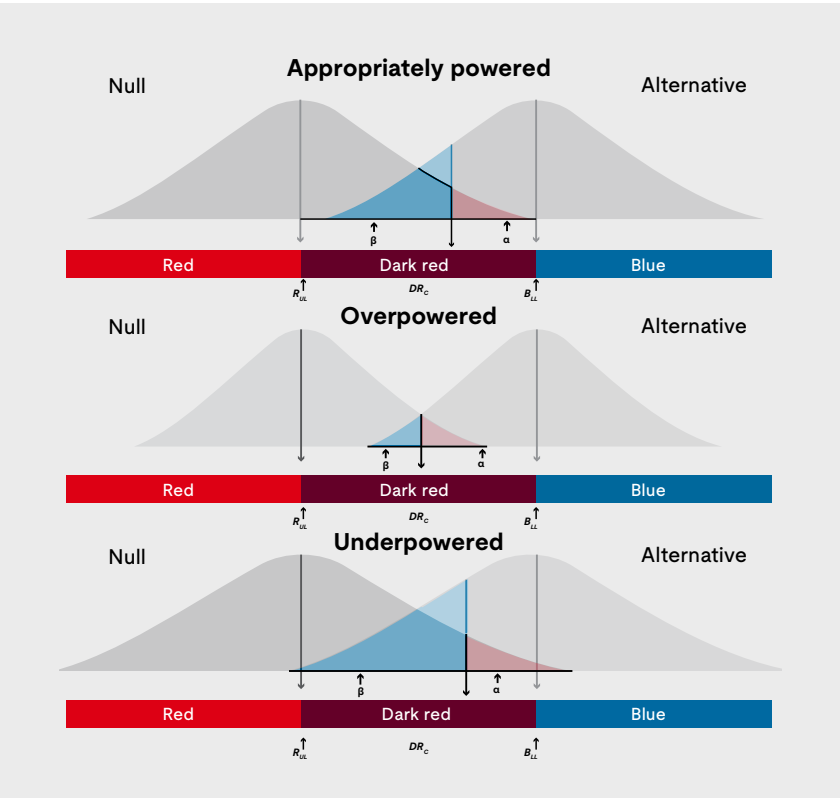
Hypothesis testing

Objective

Validate or challenge the hypothesis based on workshop insights.

Process

- Review workshop discussions against the proposed hypothesis by examining participant feedback on key technologies, challenges and potential solutions.
- Cross-reference findings from the thematic analysis and causal diagrams to assess whether the hypothesis holds or if adjustments are necessary.



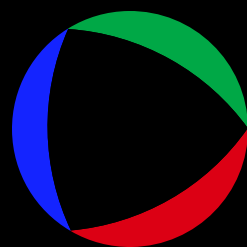


ACKNOWLEDGEMENTS

We would like to express our sincere gratitude to all UL enterprise team members and industry partners who contributed to the 2024 Convening of the Councils research report, “Evolving Technologies: Opportunities and Challenges.” The tremendous support and enthusiasm of the Event, Create and Design, Commercial, and Digital teams enabled us to thoroughly understand and analyze the past, current and future industry implications surrounding technology. We are deeply appreciative of the dialogue, survey responses and warm welcome that were given to our teams throughout this event and research experience. Without their support, this research would not have been possible.

- | | | | |
|---------------------------|---------------------|-------------------------------|-------------------------|
| • Melissa Albrecht | • Beverly Glass | • Jill Lively | • James M. Shannon |
| • George Borlase, Ph.D. | • Alexis Gniewek | • Thomas Manning | • Sanjana Sharma |
| • Kenneth Boyce | • Paul Hayes | • Susan Nadeau | • Sudhi Ranjan Sinha |
| • Meredith Carruthers | • Howard Hopper | • Christopher Nicastro | • Rajiv Sivaraman |
| • Louis Chavez | • Sims Hulings | • Deb O’Connor | • Dwayne Sloan |
| • Corinne Chocolaad | • Giles Jacknain | • Robert Osborne | • Robert V. Slone, Ph.D |
| • Chiara Clemente | • Christopher James | • Youngchoon Park, Ph.D. | • Gourav Srivastav |
| • Del Costy | • Luc Julia, Ph.D. | • Suresh Parmachand | • Dan Staresinic |
| • Chris Cramer, Ph.D. | • Lee King | • Bob Pollock | • Chris Stevens |
| • Jill Crisman, Ph.D. | • Darlene Knauss | • Gloria Pumpuni-Lenss, Ph.D. | • Dave Stinton |
| • Kristen Delphos | • Carter Kofman | • Chad Reynolds | • Alberto Uggetti |
| • Katie Denis | • Myranda LaVigne | • Timothy J. Rivelli | • Kim Vranas |
| • Phil Doherty | • Young Lee, Ph.D. | • Elissa Roach | • Ann Weeks |
| • Katie Even | • Bridget Letchos | • Cody Rogers | • George A. Williams |
| • Charlotte Farmer, Ph.D. | • Alec Lewis | • Jennifer F. Scanlon | • Katie Williams Ferris |
| • Marianne Gawlas | • Steven Liu | • Gitte Schjøtz | • John Wisniewski |

We thank you for your continued support and your efforts to contribute to the UL enterprise's mission of creating a safer world.



EMPOWERING
SCIENCE.
INSPIRING
PROGRESS.



UL Research Institutes, UL Standards & Engagement, and UL Solutions are three independent organizations that evolved from a single company, advance safety science and share a common mission: working for a safer world.