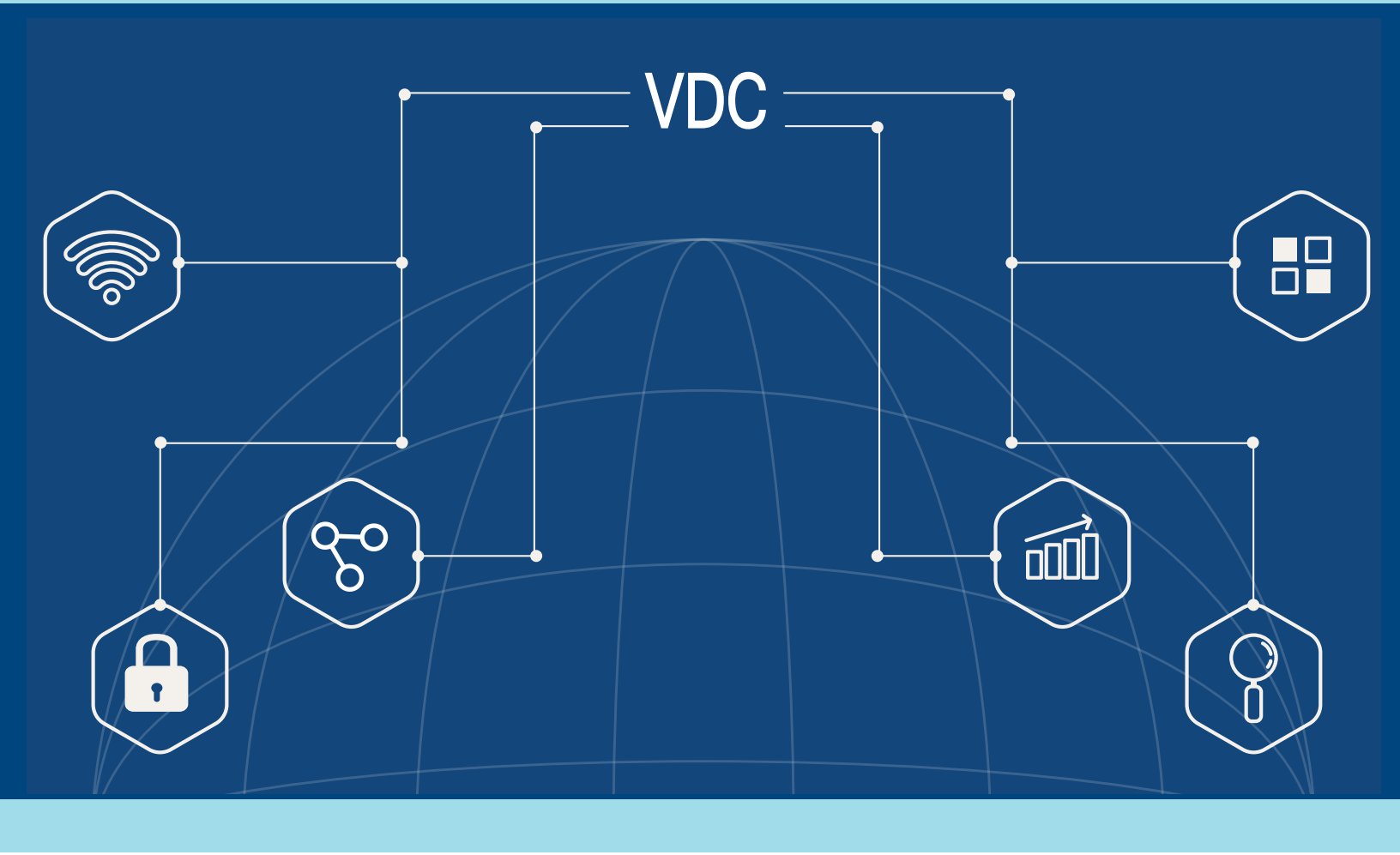
2024 IoT, Embedded & Industrial Technology Predictions



VDC|VIEW

VDC|Research

January 2024
by Chris Rommel, EVP, Steve Hoffenberg, Sr. Director,
Dan Mandell, Director, Jared Weiner, Director,
Brendan Bradley, Associate, and Joe Abajian, Associate

THE VIEW INSIDE

While IoT, embedded, and industrial markets saw dramatic growth and change over the past twelve months, the year ahead is set to redefine how computing products and solutions are designed, developed, and brought to market. This View highlights a variety of these emerging themes and trends that will help shape hardware and software markets in 2024 and beyond.

VDC'S IOT, EMBEDDED & INDUSTRIAL MARKET PREDICTIONS FOR 2024

- Labor Challenges Drive Automation, OpEx Investments
- Cloud-native Development Solutions Spread
- Digital Thread Fueling Next Generation of MBSE & M&A
- AI-based Remediation Tools Shine in Cybersecurity & Software Development
- Edge AI Hardware Becomes More Application Oriented
- AI Moves Even Further to the Edge
- Embedded Modules Take Off for OEM Development
- IoT Monetization to Drive Investment in New Platforms
- Regulatory Pressures Propel Global Cybersecurity Investment
- A High-Profile Breach Will Fuel Industrial Cybersecurity Concerns
- Shift Begins to Post-Quantum Cryptography
- OTA Standardization Efforts Creep Out of Automotive

VDC'S VIEW

LABOR CHALLENGES DRIVE AUTOMATION, OPEX INVESTMENTS

Manufacturing and other industrial organizations have long used control systems, sensors, machines, and other automation solutions to augment their operations. Unfortunately, the extent to which automation is deployed by any given organization remains limited by the cost of implementing automation technologies on a large scale. The result is an industrial landscape in which most small- to medium-sized organizations have been unable to fully take advantage of the benefits that modern industrial automation can provide. While the world's largest industrial organizations will continue to lead the charge in terms of technology adoption and innovation, 2024 will be a year in which many smaller organizations will be able to take significant steps forward in their automation journey.

Beginning in the aftermath of the COVID-19 pandemic, labor shortages and the ensuing rise in labor costs have left many organizations in a struggle to fully staff their operations. As such, these organizations have begun exploring alternative strategies for ensuring the capacity of their operations is able to meet production demand. Though advanced automation equipment such as fully automated, AI-driven robots will likely remain out of reach for many of these organizations, the availability of easily-deployable, IIoT-driven automation solutions has begun to proliferate in the marketplace. With subscription-based pricing models that allow deploying organizations to justify expenses on an OpEx basis—rather than seeking corporate approval for a large capital expenditure—solutions such as those for machine health monitoring and predictive maintenance will help organizations to overcome the labor gap by automating diagnostic and other maintenance-related activities while also improving the output, efficiency, and safety of their operations.

CLOUD-NATIVE DEVELOPMENT SOLUTIONS SPREAD

The COVID-19 Pandemic and resulting lockdowns and quarantines served as a proving ground for the successful use of cloud-native software development solutions, whose collaborative features led to a shift away from the traditionally local development that occurs within embedded organizations. Combined with the rapid emergence of artificial intelligence (AI) coding tools, many of which are cloud-native, the embedded engineering community is rapidly becoming familiar with this development paradigm.

The availability of commercial solutions for these solutions remains nascent, with commercial spend being dominated by just a few leading vendors. The general interest in and embrace of these solutions, combined with the massive amount of resources that developer organizations spend on software engineering labor, presents the cloud-native software development solutions market as a lucrative opportunity for both legacy software development vendors and startups to enter. Established vendors such as Arm and Texas Instruments (TI) will continue to "cloudify" their existing IDEs, compilers, and debuggers, using these modified existing assets to rapidly enter the market. At the same time, net-new cloud-native solutions will emerge from both legacy vendors and newcomers, serving to capture a share of this market with more intentional solutions. The availability of solutions for specific industries and use cases will emerge as vendors seek to differentiate their offerings as well as maintain a hold on the consumer bases they had previously services through traditional development tools.

The electronic design automation (EDA) market stands as a likely area for the introduction of commercial cloud-native solutions, having experimented with cloud nativity to varying degrees through Synopsys' CloudEDA and Cadence's Palladium/Protium Cloud. While these solutions focused on hardware development in the cloud, Renesas Electronics officially jumped into the cloud-native software development landscape with the announcement of a planned virtual environment platform that will offer access to its system-on-chip (SoC) and microcontroller unit (MCU) hardware for software development, debugging, and evaluation. Other semiconductor vendors such as AMD/Xilinx, who have already brought cloud nativity into their portfolios via other tools, will likely choose to push their existing software development solutions to the cloud.

DIGITAL THREAD FUELING NEXT GENERATION OF MBSE & M&A

'Digital thread' evolved from IoT-focused buzzword to a data-driven tenant of sound engineering practice. In practice, it is now viewed as a core goal of true system engineering and traditional approaches like MBSE. While it is recognized as necessary, the depth and value of underlying requirement and asset traceability often falls short. However, this dynamic is now changing. More engineering organizations are placing a premium on the ability to elicit higher degrees of visibility and traceability of design requirements and changes throughout the entire system engineering workflow. The recent announcement by Synopsys of their planned acquisition of Ansys echoes prior moves by other engineering tool market stalwarts like Siemens/Mentor Graphics and PTC/MKS/Intland (and even Ansys' own acquisition of Esterel).

Beyond issues associated with technical obstacles, challenges from integration and changes in specifications outpace those imposed on engineering organizations by simple human resource issues. Ultimately, a project must start integrated to stay integrated. Engineering problems are confounded when this issue is not addressed out front. This means one must start testing early and continuously refine test cases across all hierarchy layers down to implementation. With project execution and content creation requirements growing faster than ever, organizations are under more pressure than ever before. Now, OEMs must leverage and align more organizational IP. But clearly one of the fundamental and largest challenges is the managing of those assets across domains. Now, there is the new challenge of managing all classes of engineering assets in common source of record.

These considerations should include reevaluating and recasting approaches like MBSE (Model-based Systems Engineering). Unfortunately, existing implementations of MBSE have largely fallen short of the needs of the industry and the vision of its early design, falling victim to a combination of antiquated processes, cultures of conservatism, sub-system and engineering domain fiefdoms, as well as well-intentioned but obsolete and/or inadequate tooling technology. Looking forward, MBSE must be reimagined as Model-based Cybertronic Systems Engineering (MBCSE). An enlightened and re-intentioned approach is required to evaluate shortcomings of incumbent practices and focus on data integrations across engineering domains. Software-intensive cybertronic systems need to manage innovation and change across both software and hardware systems. Next-generation systems engineering will require investments in process and tool platform changes to maximize success against engineering and enterprise goals.

AI-BASED REMEDIATION TOOLS SHINE IN CYBERSECURITY & SOFTWARE DEVELOPMENT

Threat detection and triaging solutions are in the midst of a critical evolution. The final step in the vulnerability remediation process, which has previously been the sole responsibility of software developers, is now being integrated into cybersecurity and software tools. In the market for software composition analysis (SCA) tools, automatic vulnerability remediation has begun to extend beyond sourcing code patches from databases into tailored AI-generated remedies. The SCA tools of the future will help directly replace improperly licensed or vulnerable code with custom code that doesn't disrupt the rest of the code base, regardless of whether surrounding code is proprietary or third-party. The test automation space is undergoing a similar revolution. Leading static analysis tools already use generative AI to recommend fixes, but the testing tools that simultaneously identify and remedy problems will define the future of software testing.

Commercial cybersecurity solutions are on the same trajectory. Unlike SCA and static testing tools that analyze the code in controlled environments, cyberattacks can directly affect live device function. In safety-critical markets such as automotive, threat remediation and response time is a matter of functional safety. With cars becoming more connected and software reliant, cyberattacks can disable essential physical components (e.g., brakes, headlights, transmission) making rapid remediation critical. The complete integration of AI into threat remediation solutions invites risk that the automotive industry has avoided thus far, but AI-generated threat responses and threat prediction tools are emerging as alternatives to slow and costly OTA updates or physical recalls.

AI and machine learning integration will be essential to the success of software development tools and cybersecurity solutions in 2024.

EDGE AI HARDWARE BECOMES MORE APPLICATION ORIENTED

The embedded and edge AI market has grown dramatically over the past few years for nearly all form factors to support a variety of workloads with both general-purpose and more AI-dedicated hardware solutions. Demand for edge AI workload support ranges nearly as wide as application processing itself – from sub-milliwatt MCUs up to multi-accelerator servers and infrastructure. To first address this fragmented need for AI processing capabilities, embedded hardware suppliers launched broad market solutions meant to support as many customer types and industry workloads as possible. Suppliers wanted their AI hardware to be known as "jack-of-all-trades" solutions in a time when OEMs were launching first- and second-generation devices featuring AI capabilities to solidify themselves as early movers in a hot market. However, AI hardware suppliers, just as they had to with their general embedded hardware offerings, need to take the next step in making their solutions more optimized for specific industry application deployments to avoid the second half of that popular saying (i.e. "master of none").

To avoid becoming a generic solution looking for a problem, embedded and edge AI hardware providers in 2024 will take their offerings to the next level with more form factor-specific and bundled support (e.g., accelerator type, software platform, frameworks, models, vision transformers, brownfield integration, etc.) for processing common datasets and workload types in specific edge AI deployments. Part of this move is driven by the expanding portfolios of safety-certified and secure hardware platforms featuring AI acceleration, particularly in areas such as aerospace and defense, automotive, energy/utilities, industrial automation, medical, and transportation. Another contributing factor is the intensifying collaborations between processor providers and system or server vendors, which are together harmonizing hardware and accelerator integration into optimized (and sometimes rugged) configurations for specific industries or deployment environments.

AI MOVES EVEN FURTHER TO THE EDGE

Over the past several years, artificial intelligence has been steadily creeping from cloud datacenters to the network edge. Most industry participants consider AI with respect to "the edge" to mean local servers, industrial PCs, intelligent gateways, and similar devices, into which machine learning inference can be downloaded and applied based on training that occurred in datacenter servers. For example, a product developer or customer could use AWS SageMaker in the cloud to train AI, then load the inference into local devices via AWS Greengrass.

At VDC, we use "the edge" to include the furthest and smallest reaches of the IoT, i.e. embedded devices. Many microprocessors (CPUs, MPUs, and even MCUs) embedded in IoT devices are now sufficiently powerful to support models developed via AI frameworks such as TensorFlow and PyTorch, enabling them to serve such local machine learning inference functions as well as run the IoT devices.

Further toward the edge, "AI sensors" have been widely discussed for several years, but mostly in the context of a raw sensor and a separate microprocessor together in the same embedded device acting collectively as a smart sensor system. The concept can extend even further, in what is more specifically "AI-on-sensor," implementing machine learning inference directly in processing circuitry on IoT sensors, without the inference processing in separate chips. Such an approach has the potential to reduce hardware costs and power consumption, and more importantly improve reaction time, which could be especially beneficial in certain industrial and safety-critical scenarios.

Back in 2020, Sony announced a high resolution image sensor, IMX500, with integrated AI, for use in its high-end digital cameras and in industrial and commercial applications. And in December 2023, Korean chipmaker SK Hynix announced an image sensor with on-sensor AI processing, although as far as we know it has not been publicly demonstrated. Samsung is reportedly working on similar technology for its image sensors. At CES in January 2024, we encountered the first working demonstration we have seen of low-cost AI-on-sensor. It was in the form of a "SmartEdge ML" 6-axis MEMS sensor from TDK, which generated motion data used for (off-sensor) ML training, with ML inference subsequently downloaded back into the sensor, such that the sensor itself could recognize specific motion patterns.

Our prediction for 2024 is significant expansion and adoption of AI-on-sensor appearing in shipping IoT products, including for both imaging and non-imaging applications. This will help spread the distribution of AI technology into a greater number of IoT systems and enhance utility of devices using those sensors in the Internet-of-AI-Things.

EMBEDDED MODULES TAKE OFF FOR OEM DEVELOPMENT

While some computer-on-module (CoM) and system-on-module (SoM) suppliers have seen dramatic growth in their related businesses and portfolios in recent years, such as Avnet Embedded, congatec, NVIDIA, and Toradex, the broader market is set to carve out more OEM design mindshare and budgets in 2024. OEMs and system designers are dealing with mounting complexity in their projects with stricter requirements for application performance, power consumption, connectivity, and security, which are straining all facets of product development. Embedded modules are increasingly being sought to simplify hardware and software integrations and provide engineering organizations with more initial building blocks and tools for development to accelerate time-to-market and save on project costs. On the supply side, material and component shortages and challenges to availability are subsiding, allowing for module suppliers to better address the pent up demand for module hardware.

The predominately Arm-based SoM market is finding greater traction driven by maturing standards (e.g., Open System Module standard by SGET), deepening partnerships between key silicon providers such as NXP and ODMs and board/module suppliers, and the evolution of software platforms to support trusted, accelerated, and interoperable computing architectures. The growth of Linux support for Arm processors will be a major contributor to accelerating SoM adoption this year and moving forward. As a result, the Arm architecture is also growing within the CoM market behind the SMARC architecture, which is a standard supporting both Arm and x86 processor technology targeting high-performance, space-constrained applications at the edge.

In the CoMs arena, COM-HPC is ramping up after the initial specification rollouts for the client and server types over the past couple of years. COM-HPC features much greater levels of performance than other specifications for not just computing (e.g., Intel Xeon and high-end Intel Core) but also for I/O, memory, and interfaces. The increased availability of COM-HPC products, and variants thereof, from several leading CoM suppliers, such as Advantech, ADLINK, congatec, and Kontron, greatly expands the addressability of modules for high-performance edge infrastructure – particularly for heterogeneous servers and their dynamic needs for hardware acceleration.

IOT MONETIZATION TO DRIVE INVESTMENT IN NEW PLATFORMS

IoT-fueled differentiation has become critical for product sales and, as a result, corporate success. OEMs are under increasing pressure to embrace IoT simply to keep pace with evolution of the competitors' portfolios. In fact, over one-third of engineers indicated that they intend for IoT to help them sell more products, albeit less often with a related premium. However, the biggest appeal of IoT transformation is the ability to offer new connected services. In fact, 75% of engineers currently or plan to deploy IoT services. The use of data to augment both business intelligence and business models is becoming increasingly critical in markets with shrinking margins. With many of these services provided on demand or as a function of use, the value and need to change business models are even more apparent. As a result, new processes and automation platforms are often needed to manage new IoT business functions such as IoT commerce, Service Level Agreements (SLAs), and more complex software supply chains.

Many organizations are also monetizing both simple and more advanced functionality and otherwise looking for ways to resell IoT services to add new value and or increase their customer retention. However, these companies have not traditionally needed to manage let alone think about these issues. Often then they do not have (or even yet recognize) the need for an infrastructure and dedicated solutions to manage these new services and functionality.

With this level of service transformation, engineering organizations must focus on things other than monetization. Licensing and its management should effectively be invisible to both engineering teams developing IoT devices as well as the end users of those devices. To that end, it is critical to identify partners with platforms that can address this need and that also have expertise navigating this transition – allowing OEMs to better focus on the differentiating parts of their IoT system/value stack.

REGULATORY PRESSURES PROPEL GLOBAL CYBERSECURITY INVESTMENT

Perceptions of cybersecurity as an issue of national defense have pushed lawmakers across the world to strengthen commercial cybersecurity requirements. Many embedded markets are undergoing regulatory transformations because of industry-specific legislation and general overhauling of cybersecurity requirements. Demand for commercial automotive cybersecurity solutions, for example, will remain strong as cybersecurity standards are integrated further into the design process, stringent regulations are passed by especially cautious countries, and technical deadlines approach for major United Nations regulations. In addition, China has a keen understanding of both the benefits and risks posed by connected vehicles. To maximize productivity while minimizing cyber risk, China is developing its own comprehensive set of automotive cybersecurity regulations, which are intended to increase Chinese demand for tailored cybersecurity solutions.

In the medical device market, cybersecurity requirements have become a significant barrier to entry. As a result of the Food and Drug Omnibus included in the Consolidated Appropriations Act (2023), all new medical devices in the US must meet foundational cybersecurity requirements for FDA approval, which includes requirements such as keeping a software bill of materials (SBOM). Concerns about the security of third-party and open source code are especially present in the medical industry but have encouraged SBOM tool requirements and demand across several verticals. For example, Executive Order 14028 (2021) requires connected devices used by the US government to provide an SBOM as a commitment to improving the nation's cybersecurity. In Europe, the Cyber Resiliency Act, which is expected to finish its legislative journey in the early months of 2024, will require all connected devices to include an SBOM.

The commercial market for embedded cybersecurity will grow at accelerated rates as device manufacturers demand assistance with regulatory compliance. SBOM and cybersecurity oriented SCA tools will experience the bulk of interest from device manufacturers. Especially in non-safety-critical markets, device makers will look for low-cost tools that help them check compliance boxes with little time investment.

A HIGH-PROFILE BREACH WILL FUEL INDUSTRIAL CYBERSECURITY CONCERNS

Over the years, several high-profile breaches have drawn attention to the consequences of inadequately secured OT networks and systems. Though attacks explicitly targeting OT networks remain relatively rare, the steadily increasing connectivity between OT, IT, and other external networks has led to an increased frequency of such attacks. Stuxnet remains particularly infamous due to the mainstream notoriety it received at the time, and several incidents in the last several years— the Colonial Pipeline Ransomware Attack (2022) and Dragos's discovery of the Pipedream attack framework (2022), among others—continued to serve as cautionary tales for industrial organizations. Collectively, these breaches have and will continue to influence regulatory and compliance guidelines, drive government policy, and generate significant business for providers of industrial cybersecurity software and services.

The indisputable certainty of additional breaches will continue to provide growth opportunities for suppliers of industrial cybersecurity solutions, with the rapidly growing number of connected industrial systems and the mounting awareness regarding the risks and vulnerabilities of these systems continuing to push industrial organizations to implement more robust cybersecurity protections. Additionally, because the market for these solutions remains relatively immature, solution providers still have an opportunity to elevate their brand throughout the industrial community by becoming prominent advocates for cybersecurity best practices.

Vendors such as Claroty and Palo Alto Networks, for example, have embraced Zero Trust Architecture (ZTA), an approach to cybersecurity that dictates that no device is considered trustworthy without the continual verification and validation of the identity and status of the device, nor without the authentication of its users. Relatively new in the OT space, ZTA effectively corrects the antiquated presumption that everything inside an organization's own network is inherently trustworthy. Industrial cybersecurity evangelism and thought leadership campaigns will be a critical component of many vendors' growth strategies, with heavy participation in industry groups, regulatory committees, and security conferences common among leading vendors in this market.

SHIFT BEGINS TO POST-QUANTUM CRYPTOGRAPHY

The RSA encryption algorithm is at the heart of today's public key infrastructure, used to secure all manner of communications, data, and financial transactions on the Internet and elsewhere. The asymmetric RSA algorithm employs a pair of encryption keys—typically 2048-bits each in today's implementations—one of which is made public and the other of which is kept private. Without delving into math equations, suffice to say that the RSA algorithm includes the multiplication of two very large prime numbers, and its security relies on the extreme difficulty of reversing that process, i.e. factoring the product of those numbers back to find its original two primes. The ability to do so would enable an attacker to calculate the RSA private key for a given public key. With that private key, the attacker could decrypt data encrypted with the corresponding public key, as well as encrypt data such that a recipient would falsely believe the identity of the entity that encrypted it. Existing trust in RSA encryption would be gone.

The process of factoring such RSA numbers is computationally infeasible with conventional binary computing technology, at least for the foreseeable future. However, mathematicians and computer scientists have known that a sufficiently powerful quantum computer could potentially break such encryption using Shor's algorithm to factor the product of the primes. (Much has been written about quantum computing, so we won't attempt to describe it here.) The number of qubits in quantum computers has been slowly and steadily growing but is still orders of magnitude fewer than expected to be able to crack 2048-bit RSA encryption in a reasonable timeframe, at least without also requiring some breakthrough in factoring algorithms. Nevertheless, everyone who has been paying attention to the issue knows that eventually such a crack will happen. It's not a question of if, it's a question of when. Thus, the impetus to implement encryption algorithms that are inherently resistant to cracking by quantum computing, so-called post-quantum cryptography (PQC).

Back in 2016, the US National Institute of Standards and Technology (NIST) began a project to solicit, select, and ultimately standardize one or more post-quantum encryption algorithms. In 2021 NIST narrowed the list to 26 candidates, and in 2022 it further narrowed the list to four finalists, as well as four additional potential future candidates. NIST expects to standardize one or more of these algorithms in 2024, and VDC anticipates that will kickstart a wave of activities this year necessary to put them into use.

To back up for a moment, if quantum computing won't be able to crack 2048-bit RSA for a number of years, why worry about it now? First, transitioning the large and intricately entrenched web of RSA public-key cryptography and infrastructure from its many and varied use cases today to post-quantum solutions will take years to implement. Second, and perhaps more concerning, is that nefarious entities—including nation-states, organized criminal hacking groups, and the like—are already grabbing and storing large amounts of encrypted data, waiting for the day that quantum computing can crack RSA, at which point they could go back and decrypt vast troves of stored sensitive data, including financial information, health/medical records, government secrets, etc.

Although this issue has been known about for years, VDC expects that with the release of a NIST standard, 2024 will be the year that OEMs, cloud service providers, web developers, and other interested parties take the matter seriously and begin to shift their offerings to post-quantum cryptographic solutions.

OTA STANDARDIZATION EFFORTS CREEP OUT OF AUTOMOTIVE

Automotive OEMs have wholeheartedly accepted the over-the-air (OTA) update as the go-to method of fixing, maintaining, and upgrading the software in their fleets. Despite over a decade of use, standardization bodies, regulatory authorities, and industry groups are just now working on and finalizing the relevant guidelines that will dictate proper usage of OTA updates within the automotive market. With the emergence of the AUTOSAR Adaptive Platform, eSync Alliance, Uptane Framework, and ISO 24089 all lending credibility and integrity to the use of OTA updates, similar efforts are expected to arise elsewhere within the IoT. The software update management system (SUMS) model set forth by United Nations (UN) Regulation No. 156 (R156) can serve as a universal model for safely and securely deploying OTA updates to connected assets in adjacent safety-critical markets such as Aerospace & Defense (A&D) and Industrial Automation, as well as elsewhere within the IoT.

Already, regulatory entities are beginning to narrow the broad guidelines they had previously set forth regarding minimum security capabilities required within connected devices. Agencies and bodies across regions are explicitly focusing on OTA updates as one such way of achieving compliance. While the White House has made consumer IoT device security a priority in recent years, the introduction of the Cyber Trust Mark in July 2023 marks the first direct mention of requiring manufacturers to deliver secure software updates to their devices in the field. Similarly, the EU's Cyber Resilience Act (CRA) introduces the requirement for automatic deployment of critical security updates to devices in the field. While these two examples maintain a degree of vagueness and agnosticism in their applications, they point towards a regulatory shift trending towards the use of OTA updates. These efforts by regulatory bodies are likely to result in the emergence of standards similar to ISO 24089 for other IoT industries.

For more information on VDC's planned reports covering the markets behind these emerging trends, see **VDC's 2024 IoT & Embedded Technology research agenda**.

ABOUT THE AUTHORS

Chris Rommel

Chris leads VDC's syndicated research programs and consulting engagements focused on development and deployment solutions for intelligent systems. He has helped a wide variety of clients respond to and capitalize on the leading trends impacting next-generation industrial and device markets, such as security, the IoT, and engineering lifecycle management solutions. Chris has also led a range of proprietary consulting projects, including competitive analyses, strategic marketing initiative support, ecosystem development strategies, and vertical market opportunity assessments. Chris holds a B.A. in Business Economics and a B.A. in Public and Private Sector Organization from Brown University.

Email Chris at **crommel@vdcresearch.com**

Steve Hoffenberg

Steve is a leading industry analyst and market research professional for Internet of Things technology. He has more than two decades of experience in market research and product management for technology products and services. Prior to joining VDC, he spent 10 years as Director of Consumer Imaging and Consumer Electronics Research at the firm Lyra Research, where he led industry advisory services providing extensive market research on consumer technology trends, user adoption, market sizing, marketing strategy, and competitive analysis for major consumer electronics manufacturers. Previously, he worked in product management for electronic design companies that developed and licensed embedded digital imaging and audio products. Steve holds an M.S. degree from the Rochester Institute of Technology and a B.A. degree from the University of Vermont. He is also a Certified Information Systems Security Professional (CISSP).

Email Steve at **shoffenberg@vdcresearch.com**

Dan Mandell

Dan supports a variety of syndicated market research programs and custom consulting engagements in the IoT and Embedded Technology practice. He leads VDC's annual research services for embedded processors, boards, integrated systems, edge gateways, and other computing hardware. Dan's insights help leading technology providers align their go-to-market planning and competitive strategies with the dynamic embedded landscape and its constantly evolving buyer behaviors, technology adoption, and application requirements. His working relationship with VDC dates back to 2005 and includes time supporting Business Development as well as the AutoID practice. Dan holds a B.S. in Information Systems Management from Bridgewater State University.

Email Dan at **dmandell@vdcresearch.com**

Jared Weiner

Jared leads the Industrial Automation and Sensors practice's major research programs and custom research and consulting engagements. His major areas of coverage include sensors for process and automation control, industrial cybersecurity, data acquisition, and other topics related to IIoT. Jared was previously a member of VDC's IoT & Embedded Technology team, where his coverage areas included embedded operating systems and embedded systems security, among others. Prior to rejoining VDC, Jared managed market research at Trillium Software, a supplier of enterprise data quality solutions. Jared received an MBA from Babson College and graduated from Bentley College with a B.S. in information design and corporate communication.

Email Jared at **jweiner@vdcresearch.com**

Brendan Bradley

Brendan supports a variety of syndicated market research programs and consulting engagements within VDC's IoT & Embedded Technology practice. Prior to joining VDC, Brendan gained experience at WinnCompanies. Brendan holds a B.A. in Economics with a Concentration in Financial Markets from Colby College.

Email Brendan at **bbradley@vdcresearch.com**

Joe Abajian

Joe is an analyst supporting topics within VDC's IoT and Embedded Technology practice. Joe supports several of VDC's syndicated and custom research projects investigating trends related to connectivity, cybersecurity, and embedded software development. Before joining VDC, Joe gained experience as a consultant with Oracle. He worked with healthcare providers to optimize healthcare workflows and improve patient care through data analysis and Oracle software implementation. Joe holds a B.A. in Economics from Boise State University.

Email Joe at **jabajian@vdcresearch.com**

ABOUT VDC RESEARCH

VDC Research
Insights for the Connected World

Founded in 1971, VDC Research provides in-depth insights to technology vendors, end users, and investors across the globe. As a market research and consulting firm, VDC's coverage of AutoID, enterprise mobility, industrial automation, and IoT and embedded technologies is among the most advanced in the industry, helping our clients make critical decisions with confidence. Offering syndicated reports and custom consultation, our methodologies consistently provide accurate forecasts and unmatched thought leadership for deeply technical markets. Located in Southborough, Massachusetts, VDC prides itself on its close personal relationships with clients, delivering an attention to detail and a unique perspective that is second to none.