IoT Standards

IoT Standards will look at different segments of the IoT market as it relates to implementation and use of standards. Each column will select a particular vertical, and lay out the relevant standards and technologies that affect the evolving IoT hyperspace. The pace of the columns will start broadly with the vision of narrowing the subject of subsequent articles toward more specific applications of standards, whether in the development, application, test, or commissioning of IoT technologies.

Introduction

In the last two and a half centuries, the transformation in the industrial domains has been anything but ordinary, and has further accelerated in the last couple of decades. But with the availability of massive computing power, innovations in data processing technology, and the advent of IoT, big data, and machine learning algorithms in the last decade, the industrial environment has undergone a phenomenal transformation in every aspect. However, the focus until now has been on productivity, processes, and cost efficiencies resulting in drastic increase in GHG emissions amounting to a quarter of total GHG emissions from Earth. This column takes a holistic view of the Industrial IoT paradigm including but not limited to machine learning, providing strategic insights to develop a digital circular economy strategy framework for the sustainable digital transformation of the industrial sector.

Mentor's Musings on Disruptive Technologies and Standards Interplay in Industrial Transformation

by N. Kishor Narang
Technology Philanthropist, Innovation & Standardization Evangelist

The Industrial Revolution brought about sweeping changes in economic and social organization. These changes included a wider distribution of wealth and increased international trade. Managerial hierarchies also developed to oversee the division of labor. The Industrial Revolution brought rapid urbanization (i.e., the movement of people to cities). Changes in farming, soaring population growth, and an ever ncreasing demand for workers led masses of people to migrate from farms to cities. Almost overnight, small towns around coal or iron mines mushroomed into cities. The Industrial Revolution had many positive effects. Among those was an increase in wealth, the production of goods, and the standard of living. People had access to healthier diets, better housing, and cheaper goods. In addition, education increased during the Industrial Revolution.

The Fourth Industrial Revolution (4IR) represents a fundamental change in the way we live, work, and relate to one another. It is a new chapter in human development, enabled by extraordinary technology advances commensurate with those of the first, second, and third industrial revolutions. The 4IR is a fusion of advances in artificial intelligence (AI), robotics, the Internet of Things (IoT), genetic engineering, quantum computing, and more.

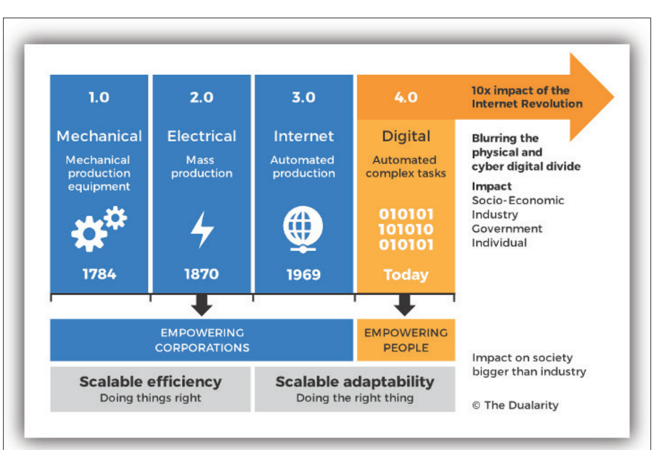
With the 4IR already well underway across the globe, the attention is now shifting to the 5th Industrial Revolution (5IR). Across the globe, conversations are shifting from the technology that encompasses the 4IR to the human interaction with technology in the 5IR. While, Industry 4.0 offers mass production with little or no human involvement, Industry 5.0 brings personalization and the human touch back to manufacturing. Collaborative robots are well positioned to become Industry 5.0 tools, helping humans create the personalized products demanded by consumers. The 5IR is dawning upon the world in unforeseeable ways as we increasingly rely on Industry 4.0 technologies including AI, big data, IoT, digital platforms, augmented and virtual reality, and 3D printing.

With people at the center of processes, Industry 5.0 focuses on three increasingly important aspects: quality of life, inclusion, and sustainability. Industry 5.0 aims to make workers' lives safer and more comfortable, while ensuring access to technologies that enable automation and increase productivity.

Evolution of the Automation Paradigm

Automation has been at the core of Industrial Revolutions from the beginning. However automation itself has been undergoing metamorphosis continuously to enable the unprecedented advancements in the industrialization across domains. Starting with mechanical, followed by electrical and electronic (analog and digital), and now leveraging computer, software, and communication/network technologies, automation has been evolving through one avatar after the other and is still undergoing much accelerated transformation using disruptive but profound technologies including IoT, AI, robotics, 3D printing, digital twin, augmented reality and so on. It has moved from being classified as fixed, programmable, flexible, or integrated automation to a new paradigm in automation — software and remote controlled with embedded AI.

Humans power industries of all kinds, bringing irreplaceable skills like judgment, reasoning, and imagination to the table.



With intuitive, agnostic, and end-to-end software on their side, there is no limit to what industrial workers can achieve.

M2M >> IoT >> IoE >> AIoT >> IoMT >> IIoT

With the evolution of communication and compute technologies, this new wave has quite rapidly evolved from machine-to-machine (M2M) to IoT and its multiple variant like the Internet of Everything (IoE), Artificial Intelligence of Things (AIoT),Internet of Medical Things (IoMT), and Industrial IoT (IIoT).

IoT adoption has increased significantly in the last five years due to the availability of massive computing power, innovations in data processing technology, and the advent of machine learning and natural-language processing algorithms. IoT has opened an entirely new arena for customers to address their long-standing issue of connecting devices and using the resulting data to positively influence decision making processes. IoT also opens an entirely new spectrum of use cases where customers can operationalize actions on the IoT devices in real time—something that was not possible a few years ago.

IIoT refers to the combination of IoT technology and data with manufacturing and other industrial processes, often with the goal of increasing automation, efficiency, and productivity. This is where IoT gets applied in practice in various industries, such as:

- Factory equipment, machines, and devices used in manufacturing
- Health monitoring devices in healthcare
- Sensors and supervisory control and data acquisition (SCADA) systems in oil and gas production
- Telemetry data from autonomous vehicles

IIoT helps organizations leverage the power of data that their machines created over several years and use that for real-time analytics to drive faster, more accurate business decisions.

Looking from a slightly different perspective, IIoT refers to interconnected sensors, instruments, and other devices networked together with computers' industrial applications, including manufacturing and energy management. This connectivity allows for data collection, exchange, and analysis, potentially facilitating improvements in productivity and efficiency as well as other economic benefits. The IIoT is an evolution of a distributed control system (DCS) that allows for a higher degree of automation by using cloud computing to refine and optimize the process controls. It is also about connecting devices and making them more available and intelligent, but on a much bigger scale.

IIoT connects people, products, and processes to power digital transformation. Using industrial IoT platforms, companies connect, monitor, analyze, and act on data in new ways. Companies use IoT and IIoT for innovative management and for monitoring widely dispersed processes. IIoT today drives how to design, manufacture, and service products, to how to create value and engage with customers.

IIoT is a vital element of Industry 4.0. IIoT harnesses the power of smart machines and real-time analysis to make better use of the data that industrial machines have been churning out for years. The principal driver of IIoT is smart machines, for two reasons. The first is that smart machines capture and analyze data in real time, which humans cannot. The second is that smart machines communicate their findings in a manner that is simple and fast, enabling faster and more accurate business decisions.

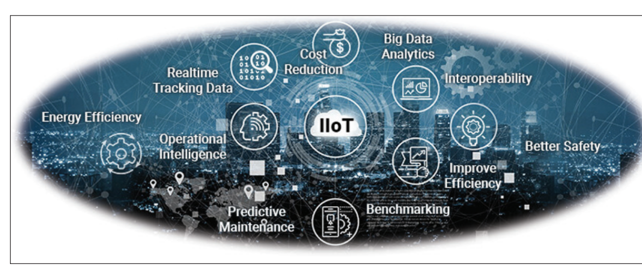
IIoT empowers manufacturers to digitize nearly every part of their business. By reducing manual processes and entries, manufacturers are able to reduce the biggest risk associated with manual labor: human error. This goes beyond just operational and manufacturing errors.

Digital Transformation

In the wake of technological advancements, especially in the field of ICT , all ecosystems including smart factories now find themselves making three classes of transformations — improvement of infrastructure — to make it resilient and sustainable; addition of the digital layer — which is the essence of the smart paradigm; and business process transformation — necessary to capitalize on the investments in smart technologies.

In the genesis of digital transformation in any paradigm, domain, or ecosystem, sustainability is the true destination, resilience is the core characteristic, smart is merely the accelerator, and standards are the chromosomes of digital infrastructure. And it is not only about the integration of information technologies (IT) and operational technologies (OT), as the network technologies have evolved to a level of complexity and advancements (5G and software defined networking) that play a crucial role in the digital transformation. Last but not least, the new kids on the block, IoT and AI, have become so pervasive and ubiquitous that they enhance the value proposition of digital transformation comprehensively in any ecosystem.

Digital transformation is NOT a technology; it is a complex paradigm with domain-specific implications as we are living in an ephemeral world, and AI and machine learning (ML) are powering the digital transformations happening in every industry around the world.



Industry 4.0 takes the emphasis on digital technology from recent decades to a whole new level with the help of interconnectivity through IoT, access to real-time data, and the introduction of cyber-physical systems. The digital transformation offered by Industry 4.0 has allowed manufacturers to create digital twins, which are virtual replicas of processes, production lines, factories, and supply chains. A digital twin is created by pulling data from IoT sensors, devices, PLCs, and other objects connected to the Internet. Digital twin technologies enable combining powerful simulations and analytics in a virtual, software-led environment that brings to life data for better performance, promising significant business benefits.

Digital transformation helps create the Industries of the Future by making manufacturing and process industries smarter, sustainable, more agile, and resilient through open, intuitive, agnostic, and end-to-end software-centric automation. IIoT and data analytics expertise can help bring unprecedented flexibility and automation to each level of an industrial enterprise. This can be achieved through connected products, edge control, and digital solutions that improve energy efficiency and lower carbon footprint.

The industries of the Future are leading unprecedented digitaliszation of industrial automation applications which rely on new business models that combine smart control, a digitally connected workforce, and optimized assets to drive operational profitability safely.

Accelerating digital transformation takes more than just the right IIoT platform. You also need pragmatic applications of technology that will make an impact on your business.

Shifting Perspectives in the IIoT Paradigm

Real-time IoT data holds the insights needed by digital transformation initiatives to succeed. However, legacy technical architectures and platforms limit IoT data's value by not scaling to support AI and ML modelling environments, workloads, and applications at scale. As a result, organizations accumulating massive amounts of IoT data, especially manufacturers, need an IoT platform purpose-built to support new digital business models.

Machine Learning and IoT: Game Changer?

Machine learning strives to minimize human intervention in tasks that can be automated—and it is fully applicable to IoT. It opens many opportunities to automate and optimize the world of IoT. Using ML algorithms, organizations can use IoT data to discover patterns and build models that can then be scored in real time on the IoT data to operationalize the models. Common use cases with ML algorithms in IoT are:

- Smart traffic prediction using classification, anomaly detection, and clustering techniques
- Energy usage prediction using linear regression, classification, and regression trees
- Food safety prediction using a naive Bayes algorithm.
- Smart city and smart citizen initiatives with *K*-means clustering

ML strives to minimize human intervention in tasks that can be automated, and it is fully applicable to IoT. ML opens many opportunities to automate and optimize the world of IoT. Using ML algorithms, organizations can use IoT data to discover patterns and build models that can then be scored in real time on the IoT data to operationalize the models.

ML can have a greater impact on people's lives when applied to IIoT than in consumer applications. When applied to IIoT, ML can enable organizations to identify when an object should be replaced before it fails, or in the case of healthcare, help clinicians make sense of massive amounts of data in computer-assisted diagnosis.

For example, a single jet engine creates/produces about a terabyte of data in five hours. That is an unfathomable amount of data coming from just one engine, and with 50,000 flights a day, this is an example of the scale of the data we are starting to deal with.

In highlighting the impact of the successes and failures of industrial ML models, a true positive could mean identifying a cancerous tumor before it is too late. And if you have a false negative, it means you have a crack in a pipe that your system missed. Organizations must also get comfortable with having more false positives. If you can live in a world with lots of false positives, you will do better than if you had no ML at all, which will ensure an "abundance of caution" built into ML models used in industrial applications.

Unlike data-driven models that may contain biases, industrial ML is grounded in the laws of physics. You can build physical models to capture the understanding of devices and simulate things that have not happened yet in the real world. However, there are some drawbacks to industrial ML. For one, physical models do not easily learn from new data, and not all physical laws have been built into large complex systems. That means we have an imperfect model, and we just hope that the imperfections are not fatal. Refinements to industrial ML models are not easy to make either, since experts with doctoral degrees are often needed in specialized fields relevant to specific use cases and applications.

A data-driven model, however, does not require explicit understanding of the physical world. You just throw in lots of data and optimize the model based on metrics that you have set up. It will naturally improve as you throw more data at it, and it is extensible to more data sources. That said, there is uncertainty over whether data-driven models can be generalized to other similar systems. It is also difficult to derive real physical intuition for those models.

Work is underway to combine physical and data-driven ML models in its systems, and to ensure that the information generated from those models is trusted and understood by users. Even if the models are correct, if people do not trust and accept them, they are not going to wind up being used. In the end, we need to create not just better algorithms, but also make ML suggestions understood to people with domain expertise. We also need to build systems that take in feedback, and are cognizant of the end user and the effects of a good and bad answer.

The key to getting more value from IIoT and IoT platforms is getting AI and ML workloads right. Despite the massive amount of IoT data captured, organizations are falling short of their enterprise performance management goals because AI and ML are not scaling for the real-time challenges organizations face. If you solve the challenge of AI and ML workload scaling right from the start, IIoT and IoT platforms can deliver on the promise of improving operational performance.

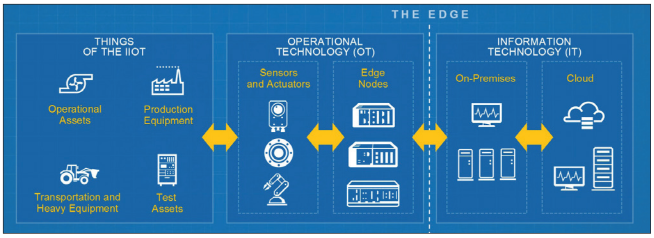
More organizations are pursuing edge AI-based initiatives to turn IoT's real-time production and process monitoring data into results faster. Enterprises adopting IIoT and IoT are dealing with the challenges of moving the massive amount of integrated data to a data center or centralized cloud platform for analysis and derive recommendations using AI and ML models. The combination of higher costs for expanded data center or cloud storage, bandwidth limitations, and increased privacy requirements are making edge AI-based implementations one of the most common strategies for overcoming IoT's growth challenges.

IIoT/IoT platforms with a unique, differentiated market focus are gaining adoption the quickest. For a given IIoT/IoT platform to gain scale, each needs to specialize in a given vertical market and provide the applications and tools to measure, analyze, and run complex operations. An overhang of horizontally focused IoT platform providers rely on partners for the depth vertical markets required when the future of IIoT/IoT growth meets the nuanced needs of a specific market. It is a challenge for most IoT platform providers to accomplish greater market verticalization, as their platforms are built for broad, horizontal market needs.

In order to use IIoT and IoT to improve operational performance, enterprises must face the following challenges:

- **IIoT and IoT endpoint devices need to progress beyond real-time monitoring to provide contextual intelligence as part of a network.** The bottom line is that edge AI-based IIoT/IoT networks will be the de facto standard in industries that rely on supply chain visibility, velocity, and inventory turns within three years or less. Edge AI is the cornerstone of the IoT and IIoT deployment plans. Enterprise IT and operations teams want more contextually intelligent endpoints to improve end-to-end visibility across real-time IoT sensor-based networks. Build-out plans include having edge AI-based systems provide performance improvement recommendations in real time based on ML model outcomes.

- **AI and ML modeling must be core to an IIoT/IoT architecture, not an add-on.** Attempting to bolt-on AI and ML modeling to any IIoT or IoT network delivers marginal results compared to when it is designed into the core of the architecture. The goal is to support model processing in multiple stages of an IIoT/IoT architecture while reducing networking throughput and latency. Organizations that have accomplished this in their IIoT/IoT architectures say their endpoints are most secure. They can take a least-privileged access approach that is part of their zero trust security framework.



- **IIoT/IoT devices need to be adaptive enough in design to support algorithm upgrades.** Propagating algorithms across an IIoT/IoT network to the device level is essential for an entire network to achieve and keep real-time synchronization. However, updating IIoT/IoT devices with algorithms is problematic, especially for legacy devices and the networks supporting them. It is essential to overcome this challenge in any IIoT/IoT network because algorithms are core to AI edge succeeding as a strategy. Across e-logic controllers (PLCs) in use, supporting control algorithms and ladder logic. Statistical process control (SPC) logic embedded in IIoT devices provides real-time process and product data integral to quality management success. IIoT is actively being adopted for machine maintenance and monitoring, given how accurate sensors are at detecting sounds, variations, and any variation in process performance of a given machine. Ultimately, the goal is to predict machine downtimes better and prolong the life of an asset.

Some further insights:

- Business cases that include revenue gains and cost reductions win most often.
- Design IIoT/IoT architectures today for AI edge device expansion in the future.
- Plan now for AI and ML models that can scale to accounting and finance from operations.
- Design in support of training ML models at the device algorithm level from the start.

Security Considerations and Challenges When Adopting IIoT

The adoption of IIoT can revolutionize industries, but this increased connectivity can create additional security issues. Companies that work with OT understand the importance of worker safety and product quality. But with the integration of operations, the Internet, automation, and smart machines, several challenges arise with availability, scalability, and security.

Most industries are well versed in managing availability and scalability since they are crucial to functioning and can easily be integrated in an IIoT system. Security is where most organizations tend to falter. Many businesses still utilize legacy systems and processes, and new technologies can complicate integration and end-to-end security.

The increase in smart devices, particularly employee devices used for work, give rise to a plethora of security vulnerabilities. Organizations are responsible for the secure implementation and setup for any connected devices. But device manufacturers also have to prove they can keep devices safe, which is not often the case.

Cyber-security issues are rising. Successful hackers can crack connected systems and potentially shut down operations. To handle these security issues, manufacturing companies need to approach IIoT like any IT company would: with a focus on the security of physical and digital components.

Another challenge with IIoT adoption is securely integrating industrial operations with IT. User data has to be in sync with global privacy regulations. Gathering data is essential to generating essential insights for a company, but personal information needs to be separated and stored in encrypted databases. Storing personal data with business data can lead to serious risks of exposure.

Several other security problems are associated with IIoT. These could be exposed ports, a lack of sufficient authentication practices, or even the use of obsolete applications. All these small problems, in addition to having an Internet network, can be dangerous for companies. Unsecured IIoT systems can result in operational disruption and financial losses.

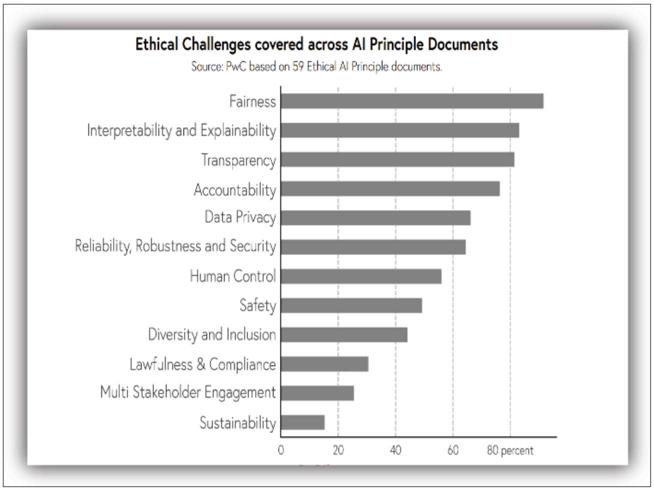
The more connected an environment is, the higher the security risks:

- Software vulnerabilities are easy prey for hackers to attack.
- Devices and systems connected to the Internet are publicly searchable.
- Hacking attempts increase, leading to targeted attacks and data loss.
- Operations are disrupted from system manipulation or sabotage attempts.
- System malfunction results in device damage, or worse still, physical damage to employees.
- Extortion attempts result from compromised operational technologies.
- Increased fines may be incurred if private information is made public against regulations.

The last concern is that IoT and IIoT suffer from technology fragmentation, which can lead to inoperable systems if processes are not handled correctly or efficiently. Adoption of IoT technologies has increased exponentially in the past five years — but successful implementation still eludes some.

The Imperative for Ethical Guardrails in ML and AI

Generally, the use of ML and AI is synonymous with good innovation and positive applications of this technology. The emergence of these technologies has already begun to profoundly reshape our lives, our interactions, and our lived environments. AI itself will also become smarter with each passing year. It will not only become more productive, but will also develop intelligence that humans do not yet have, accelerating human learning and innovation. As we look forward to the gains, efficiencies, and new solutions that AI creates for nations, businesses, and everyday life, we must also think about how to maximize gains for society and our environment. The fact that AI will have a major impact on society is no longer in question. Current debate turns instead on how far this impact will be positive or negative, for whom, in which ways, in which places, and on what timescale. It would be interesting to undertake a meta-analysis of the ethical challenges presented by emerging technologies collectively referred to as ML and AI.



Transparent, Interpretable, and Unbiased AI

Artificial intelligence use cases are proliferating, from many business applications to more and more facets of day-to-day living. And as awareness of AI becomes more prominent, justifiable concerns about the fairness and power of ML algorithms, and the effects of AI on privacy, speech, and autonomy are growing. In the private sector, businesses must grapple with how to develop and deploy ethical AI, while in the public sphere, government policy is being crafted to ensure safe and fair AI use.

What does responsible and ethical AI look like? "Ethical" is a subjective term, while responsibility, or being accountable for your choices, is essentially doing the right thing when it comes to implementing software.

It is less about what you perceive as right or wrong, and more about how you are going to be held accountable for the outcomes of the things you build. I feel like every company can move in that direction, regardless of where they are on the spectrum of ethical-ness in their AI.

Being accountable for the outcomes is important; however, it is not about whether the system is biased or fair, but rather whether it does what is claimed. The importance of transparency in datasets and testing evaluation canno't be overstated. As part of that, the focus is often on the human factors, such as participatory design techniques, multi-state coding approaches, and human-in-the-loop test methods, rather than the bigger picture.

None of these really are a panacea against the bias, which is part of a broader socio-technical perspective that connects these AI systems to societal values. And I think this is where experts in the area of responsible AI really want to focus to successfully manage the risks of AI bias so that we create a system that is not only doing something that is claimed, but doing something in the context of a broader perspective that recognizes societal norms and morals.

We need to understand the broad consequences of failing to have the necessary guardrails, even if unintended. It could decide where we go to school, who we might marry, if we can get jobs, where we will live, what healthcare we get, what access to food we will have, and what access to capital we wi'll have. The risks are high, and they require a serious evaluation of the way that we implement them.

Unfortunately, many of the data scientists and business unit experts who are in the position to design, build, and implement ML models or algorithms are not ethicists by trade. They generally did not study ethics in school or have the opportunity to learn about the concept of questioning in product design. They do not know what questions to ask, or cannot identify what they can be held accountable for in terms of the performance or intention of their models and the data being used to train them. Employees lower in the business hierarchy tend to assume that these ethics questions are above their pay grade.

With every line of business now leveraging AI, we need to each take responsibility for understanding and finding a defense for why we are using this technology, what the scope of that use is, and how we are collecting the data that creates those predictions.

All humans have developed their own idea of what is ethical or non-ethical. And if they are building AI systems, they are imbuing their own view of ethics and ethical behavior into the system — which may or may not have an alignment with societal practices or societal values that we want to propagate.

It is critical to start pulling in more people from the social sciences and that data scientists start thinking about the human dynamic in the relationship with AI so that we do not end up building something that hurts a person.

That is ultimately the biggest failure: building an AI that infringes on someone's rights, hurting someone's ability to do something that they would have had a right to do, but the AI models inadvertently decide against it. This is something most companies are battling with: how to do that well.

Implementing Responsible and Ethical AI

To start on the path to ethical AI, an organization needs an AI manifesto. Leaders need to understand what it means to be a data-driven business, and then set an intention that they are going to build it responsibly. When you build an AI solution, it needs to include transparency, and interpretability of the models such that someone who is not necessarily a data scientist can understand how the models operate.

A focus on privacy is also essential, especially when building the right datasets. It is expensive to do that responsibly, and it is expensive to make sure that every constituency is represented, or at least empathically noted, in your training data. It is where a lot of organizations struggle — but it is worth it, as it ensures that the software is fair and equitable and avoids potential setbacks or even company catastrophes. Ethical AI also requires a feedback loop so that anyone working on the models can raise their hand to flag any issues or concerns.

There is also the need to expand beyond the ML and technical capabilities of transparency and responsibility to remove bias, and drill down to how the systems are being created, and what impact they are going to have on society, even when on the surface they are good at what they do. For instance, using algorithms for crime prevention and prediction has been relatively successful in helping law enforcement; at the same time, they have had a disproportionately negative impact on some communities in society because of the way that those algorithms are implemented.

While most of the data scientists are quite bullish on AI and the prospects of using it for good, the fact is that because it is so focused and capable of rippling through our broader society, when it does not work the way we want it to, the scale of the damage and the speed at which it can be perpetuated across the entire society are very vast and very impactful.

Is AI the New Plastic?

As adoption of AI/ML technologies becomes widespread, they are likely to play a substantial independent role in society's energy consumption and environmental impact. In this section, we argue that AI poses collective challenges like the widespread introduction of plastics half a century ago — providing cheap and/or seemingly efficient solutions to a wide range of contemporary problems while creating (and displacing) new aggregate costs that will impact all of society. It is well understood and acknowledged that AI leverages predictive models to help scientists understand how climatic shifts might manifest across the world in the coming decades. But as exciting as it may be to contemplate a world where AI helps tackle the climate crisis, there is no escaping the bitter irony that AI itself comes with a significant carbon footprint.

How does AI work like plastic? It promises to be a cheaper and more effective alternative to business procedures that are commonly in place. But it has the potential to displace explicitly evident costs (fewer staff, more productive machinery, and procedures) into costs that are harder to perceive (massive energy costs generated at computational facilities). Also, will its implementation change the structure of our economy in ways that facilitate downstream burdens on the environment that are currently hindered by the limitations of our economy?

The planetary scale of our knowledge and technologies is revealing new interdependencies and feedback loops between environmental and engineered systems. This renewed understanding requires an updated ethical, ontological, and practical discourse—one that is not reductionist, but rather makes the moral responsibility for planetary custodianship even more urgent. Accordingly, the consideration of environmental impacts and the responsibility to care for our planet should be reflected in our technical infrastructure, our ways of working, and our practices and policies for fair, accountable, transparent, and ethical AI systems. AI will not be a substitute for more integrative ways of knowing or even degrowthist political agendas — but rather, when used responsibly, can be an enabler that helps us move faster to a safe and just post carbon world.

A holistic ethical and policy approach needs to be taken toward the design and deployment of AI technologies. It is imperative to embed an awareness of key ethical and policy goals throughout the ecosystem and value chain — from researchers to engineers to corporations to global policymakers — to better generate and distribute metrics that can inform policies oriented towards ethical and sustainable practices.

RED AI vs. GREEN AI

Artificial intelligence promises both to combat the ill effects of climate change and to make the emergency worse with excessive energy use. How can AI be made greener?

Implementation of an AI solution is often preceded by multiple iterations of refinement by tuning hyperparameters. Needless to say, this can incur a large computational cost, and consequently a large environmental cost. Creating efficiency in AI research will decrease its carbon footprint and increase its inclusivity as deep learning study should not require the deepest pockets.

The term "green AI" refers to AI research that yields novel results while considering the computational cost, encouraging a reduction in resources spent. Whereas red AI (AI development that is oblivious to its environmental impact) has resulted in rapidly escalating computational (and thus carbon) costs, green AI promotes approaches that have favorable performance/efficiency trade-offs.

Green AI.

Some researchers feel that the efficiency of red AI solutions can be improved as follow-up work, and this can be achieved by training on a smaller dataset. The computational cost of recent work, they feel, pays off in downstream performance. However, this rate of return is declining with time.

They advocate for a green AI approach where both training and inference aspects of running ML algorithms are optimized for computational efficiency. This is necessary because models used in production incur higher computational costs during inference, whereas in research training is done much more frequently.

Today, a few organizations are offering sets of metrics for benchmarking the efficiency of AI systems. The proposal considers efficiency across four categories: training time; training cost (measured in U.S. dollars); inference latency; and inference cost (measured in U.S. dollars).

Circular Economy and Industry 5.0

Today, the world is only 8.6 percent circular. Not only is it clear that this is not sustainable, but the urgency also to step away from a take — make — waste economic model is growing. If this wasteful trend continues, we will need the natural resources of two Earths by 2030, making achieving the sustainable development goals (SDGs) and Paris Agreement virtually impossible. Also, there are no signs that circularity gap is closing. Material use and carbon emissions continue on an upward trend.

The latest Intergovernmental Panel on Climate Change (IPCC) report released recently emphasized that the next few years are critical — limiting warming to around 1.5°C (2.7°F) requires global greenhouse gas emissions to peak before 2025 at the latest, and be reduced by 43 percent by 2030. It is now or never if we want to limit global warming to 1.5°C (2.7°F). Without immediate and deep emission reductions across all sectors, it will be impossible. We have options in all sectors to at least halve emissions by 2030.

Reducing emissions in industry will involve using materials more efficiently, reusing and recycling products, and minimizing waste. For basic materials, including steel, building materials, and chemicals, low- to zero greenhouse gas production processes are at their pilot to near-commercial stage. This sector accounts for about a quarter of global emissions. Achieving net zero will be challenging and will require new production processes, low and zero emissions electricity, hydrogen, and, where necessary, carbon capture and storage.

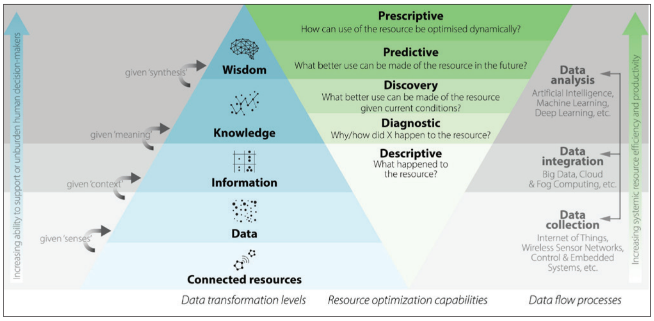
Circular economy is about transformation. The circular economy is not just about recycling — it is about a transformation of the entire value creation system by decoupling growth from finite resources. Transitioning to a circular economy is about much more than just reducing the waste inherent in the linear economy. It is about sustainable growth that creates economic opportunities, and environmental and social benefits, and increases business resilience. This transition requires a systemic shift that closes, optimizes, and values resource loops across the value chain which makes collaboration across organizations pivotal.

While the focus of Industry 4.0 is mass production, Industry 5.0 focuses on sustainability. Furthermore, we emphasize that regardless of its version, the next industrial revolution should be fueled by both the information technology and the concerns for environmental sustainability. The priority of Industry 5.0 is to utilize efficiently workforce of machines and people, in synergy with the environment. The theme of this vision is industrial upcycling. This vision focuses on waste prevention. Industry 5.0 includes 6R (recognize, reconsider, realize, reduce, reuse, and recycle) methodology and logistics efficiency design (L.E.D.) principles.

6R methodology actually defines a business improvement model. Depending on the specific case, it can be considered as a business process improvement or a business process innovation. Therefore, the 6R methodology is subject to the rules, assumptions, and dynamics of process improvement efforts. L.E.D. is designed for global supply chain efficiency improvements. Its goal is to eliminate the waste created by the current modern standard buyer-supplier business relations. L.E.D is the concurrent application of transparency, profit sharing, and efficiency in the supply chain.

Role of Industrial IoT in Achieving Sustainability and Net Zero Targets

Technology is an enabler; how we use it is entirely up to us. Leveraging IoT, ML, AI, and big data to make the industrial designs, processes, and logistics more circular and carbon neutral should be the real driver of digital transformation of the industry ecosystem. We need to develop a holistic strategy framework to embed sustainability, circularity, and ethics in the industrial transformation in the next few decades.



Digital circular economy strategy.

Standardization Conundrum

Innovation and technology development are accelerating. Strategic plans and roadmaps are needed to help ensure that the market is suitably served with best practices, which is pertinent to the goals and context of this very large market.

Standards support our need to balance agility, openness, and security in a fast-moving environment. Standards provide us with a reliable platform from which we are able to innovate, differentiate and scale up our technology development. They help us control essential security and integrate the right level of interoperability. Standards help ensure cyber security in ICT and IoT/IIoT systems.

The Question Most People Would Ask Is: What Do Standards Have to Do with All This?

Although most people do not realize it, standards and the methods used to assess conformity to standards are absolutely critical. They are essential components of any nation's technology infrastructure — vital to industry and commerce, crucial to the health and safety of citizens, and basic to any nation's economic performance. About 80 percent of global merchandise trade is affected by standards and by regulations that embody standards.

Given the scale, moving forward cannot be successfully, efficiently, and swiftly accomplished without standards. The role of standards in helping to steer and shape this journey is vital. Standards provide a foundation to support innovation. Standards capture tacit best practices, and set regulatory compliance requirements.

Standards Enable Us to Pre-Solve Complex Problems

The extensive work done by various global SDOs has very comprehensively defined the frameworks and roadmap for future information and communications technology (ICT) infrastructure. However, the new paradigm of smart grid, smart home, smart building, smart manufacturing, and smart city, already complicated by IoT and the Internet of Everything and made further complex by AI, ML, big data, and quantum computing, has given rise to new aspects of the way humans, machines, and things are going to communicate with each other in the very near future. The heterogeneity of the IoT paradigm and challenges for different aspects of security, privacy, and trustworthiness have made it imperative to take a fresh look at the prevalent architectures and frameworks of the ICT infrastructure being deployed or developed. The recent evolution of disruptive technologies and digitalization compounded by COVID-19, changing geopolitical situations, and increasing cyber-attacks from not-so-friendly nations have made all the stakeholders sit up and take note of this imminent danger to the sovereignty of nations and safety of their citizens.

The irony is that standards and even SDOs are not at the forefront of solution designers', developers', providers', deployers', or users' minds. There are misconceptions on what standards are for, and the case for the use of standards has not been made. Most researchers, design engineers and even startups argue that standards block innovation. In fact, standardization brings innovation and spreads knowledge. Standardization helps define the contours of structured innovation, first because it provides structured methods and reliable data that save time in the innovation process, and second because it makes it easier to disseminate ground-breaking ideas and knowledge about leading edge techniques. Liberalization and markets have a lot of great virtues, but they cannot create their own conditions of existence; they must be designed! Truly speaking, a consumer focus is also missing in the global standardization movement. It is important to remember that standardization is a tool and not an end in itself.

The IIoT value chain is perhaps the most diverse and complicated value chain of any industry or consortium that exists in the world. In fact, the gold rush to drones and the Internet of Drones (IoD) is so pervasive that if you combine much of the value chains of most industry trade associations, standards bodies, the ecosystem partners of trade associations and standards bodies, and then add in the different technology providers feeding those industries, you get close to understanding the scope of the task. In this absolutely heterogeneous scenario, coming up with common harmonized standards is a major hurdle.

The multiplicity of technologies and their convergence in many new and emerging markets, however, particularly those involving large-scale infrastructure, demand a top-down approach to standardization starting at the system or system architecture rather than at the product level. Therefore, the systemic approach in standardization work can define and strengthen the systems approach throughout the technical community to ensure that highly complex market sectors can be properly addressed and supported. It promotes increased cooperation with many other SDOs and relevant non-standards bodies needed on an international level. Further, standardization needs to be inclusive, top down and bottom up; a new hybrid model with a comprehensive approach is needed.

Industrial IoT standards encompass all the standards relevant to wide spectrum of industries and technologies ecosystems. The recent leveraging of disruptive technologies like AI, ML, and big data in industries has further expanded the standards landscape for IIoT into new arena. All the global SDOs — IEC, ISO, ITU, and IEEE — have enhanced focus on these critical and emerging technologies.

In ISO/IEC JTC1, there is a Subcommittee SC42 on "Artificial Intelligence & Data" that addresses standardization in AI, ML, data, and all related technologies and domains.

Standards by ISO/IEC JTC 1/SC 42: Artificial Intelligence

Published

- ISO/IEC 20546:2019: Information technology — Big data — Overview and vocabulary
- ISO/IEC TR 20547-1:2020: Information technology — Big data reference architecture — Part 1: Framework and application process
- ISO/IEC TR 20547-2:2018: Information technology — Big data reference architecture — Part 2: Use cases and derived requirements
- ISO/IEC 20547-3:2020: Information technology — Big data reference architecture — Part 3: Reference architecture
- ISO/IEC TR 20547-5:2018: Information technology — Big data reference architecture — Part 5: Standards roadmap
- ISO/IEC TR 24027:2021: Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making
- ISO/IEC TR 24028:2020: Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence
- ISO/IEC TR 24029-1:2021: Artificial Intelligence (AI) — Assessment of the robustness of neural networks — Part 1: Overview
- ISO/IEC TR 24030:2021: Information technology — Artificial intelligence (AI) — Use cases
- ISO/IEC TR 24372:2021: Information technology — Artificial intelligence (AI) — Overview of computational approaches for AI systems

Under Development

- ISO/IEC DTS 4213.2: Information technology — Artificial Intelligence — Assessment of machine learning (ML) classification performance
- ISO/IEC AWI 5259-1: Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 1: Overview, terminology, and examples
- ISO/IEC AWI 5259-2: Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 2: Data quality measures
- ISO/IEC AWI 5259-3: Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 3: Data quality management requirements and guidelines
- ISO/IEC AWI 5259-4: Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 4: Data quality process framework
- ISO/IEC AWI 5259-5: Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 5: Data quality governance
- ISO/IEC CD 5338: Information technology — Artificial intelligence — AI system life cycle processes
- ISO/IEC AWI 5339: Information Technology — Artificial Intelligence — Guidelines for AI applications
- ISO/IEC AWI 5392: Information technology — Artificial intelligence — Reference architecture of knowledge engineering
- ISO/IEC AWI TR 5469: Artificial intelligence — Functional safety and AI systems
- ISO/IEC AWI TS 5471: Artificial intelligence — Quality evaluation guidelines for AI systems
- ISO/IEC AWI TS 6254: Information technology — Artificial intelligence — Objectives and approaches for Explainability of ML models and AI systems
- ISO/IEC CD 8183: Information technology — Artificial intelligence — Data life cycle framework
- ISO/IEC AWI TS 8200: Information technology — Artificial intelligence — Controllability of automated artificial intelligence systems
- ISO/IEC AWI TS 12791: Information technology — Artificial intelligence — Treatment of unwanted bias in classification and regression machine learning tasks
- ISO/IEC AWI 12792: Information technology — Artificial intelligence — Transparency taxonomy of AI systems
- ISO/IEC FDIS 22989: Information technology — Artificial intelligence — Artificial intelligence concepts and terminology
- ISO/IEC FDIS 23053: Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)
- ISO/IEC DIS 23894: Information technology — Artificial intelligence — Risk management
- ISO/IEC CD 24029-2: Artificial intelligence (AI) — Assessment of the robustness of neural networks — Part 2: Methodology for the use of formal methods
- ISO/IEC AWI TR 24030: Information technology — Artificial intelligence (AI) — Use cases
- ISO/IEC DTR 24368: Information technology — Artificial intelligence — Overview of ethical and societal concerns
- ISO/IEC DIS 24668: Information technology — Artificial intelligence — Process management framework for big data analytics
- ISO/IEC CD 25059: Software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality model for AI systems
- ISO/IEC AWI TS 29119-11: Information technology — Artificial intelligence — Testing for AI systems — Part 11
- ISO/IEC 38507: Information technology — Governance of

IT — Governance implications of the use of artificial intelligence by organizations
- ISO/IEC CD 42001: Information Technology — Artificial intelligence — Management system

Standards by IEEE

- IEEE P2830™ — Standard for Technical Framework and Requirements of Shared Machine Learning
- IEEE P2841™ — Framework and Process for Deep Learning Evaluation
- IEEE P3333.1.3™ — Standard for the Deep Learning Based Assessment of Visual Experience Based on Human Factors
- IEEE P3652.1™ — Guide for Architectural Framework and Application of Federated Machine Learning

Since standardization is a collective churning, deliberation, and collaboration process, we need to moderate as well as expand our individual thoughts on any subject to make it acceptable globally.

Conclusion

Following the conclusion of the COP26 climate conference, private organizations and governments alike are stepping up their promises to combat climate change, bringing to bear a mix of public policy and innovative technologies to address one of our era's defining challenges.

AI systems, and their ability to control machines automatically and remotely, have caught the public's imagination. The opportunity for AI to be harnessed to benefit humankind and its environment is substantial. AI as a technology can help to mitigate climate change. This aspect should be further emphasized in terms of measuring the benefits of AI for the environment and climate. The intelligence and productivity gain that AI will deliver can unlock new solutions to society's most pressing environmental challenges: climate change, biodiversity, ocean health, water management, air pollution, and resilience, among others.

However, AI technology also has the potential to amplify and exacerbate many of the risks we face today. To be sure that AI is developed and governed wisely, government and industry leaders must ensure the sustainability (energy efficiency, circularity, and carbon footprint) along with the already accepted aspects like safety, explainability, transparency, and validity of AI applications. It is incumbent on authorities, AI researchers, technology pioneers, and AI adopters in industry alike to encourage deployments that earn trust and avoid abuse of the social contract.

Achieving this requires a collaborative effort to ensure that as AI progresses, its idea of a good future is aligned to human values and encapsulates a future that is safe for humanity in all respects — its people and their planet. It is imperative to consider sustainability as a moral framework based on social justice, which can be used to evaluate technological choices.

We have a unique opportunity to harness the ongoing disruptive technologies' revolution, and the societal shifts it triggers, to help address environmental issues and redesign how we manage our shared global environment. The disruption we are witnessing could, however, also exacerbate existing threats to environmental security or create entirely new risks that will need to be considered and managed.

Harnessing these opportunities and proactively managing these risks will require a transformation of the "enabling environment," namely the governance frameworks and policy protocols, investment and financing models, the prevailing incentives for technology development, and the nature of societal engagement. This transformation will not happen automatically. It will require proactive collaboration between policymakers, scientists, civil society, technology champions, and investors. If we get it right, it could create a sustainability revolution.

Give technology new roles to play. The next step is to reimagine the role of digital technology. Until now, it is largely used to boost efficiency, cut costs, and promote consumption.

Digital technologies, for example, have been used for tasks such as predictive maintenance and tightening up production processes, but sustainability and efficiency are closely linked — making better use of resources and materials makes your company more sustainable. By using digital technologies to track performance through the cycle, from carbon, water, and waste to plastics, packaging, and product, leaders can generate insight into how sustainable the supply chain really is and how it can be improved.

Sustainability must be at the center of a digital strategy, not a sideshow or an afterthought. The most important thing here is blending technologies, system design, and hardware to create a platform for ML and AI to help Industrial IoT unlock the value of the data.

They shall be at the core of innovation and technology that we leverage to steer our narratives and build bridges between the worlds we inhabit now and the ones we imagine for tomorrow.

Biography

N. Kishor Narang (kishor@narnix.com) is a technology consultant, mentor, and design architect in electrical, electronics, and ICT with over 40 years of professional experience in education, research, design, and consulting. He has over 30 years of hardcore research, design, and development experience in fields as diverse as industrial engineering, power and energy engineering, IT, telecommunications, medical devices, and environmental engineering. Professionally, he is an electronics design engineer practicing design and development across a wide spectrum of products, systems, and solutions through his own independent design house, NARNIX, since 1981. For the last 10 years, he has been deeply involved in standardization in the electrical, electronics, communications, and information technology domains with a focus on identifying gaps in standards to bring harmonization through standardized interfaces to ensure end-to-end Interoperability. He has been leading national standardization initiatives at BIS, the Indian national standards development organization, in smart cities, smart manufacturing, smart energy, and active assisted living as the Chairman of the Smart Infrastructure Sectional Committee LITD 28, along with contributing to multiple other SDOs and initiatives. Globally, he is Vice Chair-Strategy and Project Leader of two international standards in IEC SyC Smart Cities, a Co-Editor of the ISO/IEC JTC1/WG 11 Four Standards, and a member of the Steering Committee of OCEANIS, beyond proactive contributions in many committees in global SDOs.