



Rocket Wagon Venture Studios

# Illuminating Paths to Success in the Connected World

*A Framework From Concept to Commercialization in 2020*



**A Rocket Wagon Venture Studios White Paper**

*Christopher Bonanti, Vice President and General Manager, Strategic Advisory Services*

# Introduction

While it is impossible to pinpoint the year the terminology “Internet of Things” (IoT) was coined, the idea of system bridging physical and digital worlds was part of the vision of Internet pioneers as early as 1982, when a soda vending machine at Carnegie Mellon University was connected to the Internet, generating data showing inventory and temperature of recently loaded beverage cans.

Great milestones were achieved in the 1990s, including the publication of Mark Weiser's famous 1991 paper on ubiquitous computing, “The Computer of the 21st Century,” and again in the early 2000s, when tech giants, including Microsoft and Cisco, and consumer packaged goods companies, like Proctor & Gamble, began work on scalable connected products as the Internet “bubble” exploded. Arguably, the term “Internet of Things” was initiated by Kevin Ashton, co-founder of the Auto-ID Center at MIT and a pioneer in RFID technologies.

By 2010, the advent of smart phones and the massive growth of cellular and other wireless networks changed everything. Tens of thousands of consumer products were now connected and in the marketplace. Industrial deployments of machine-to-machine (M2M) grew in size, scope and value and the inevitability of a world of computing devices, given unique identifiers (UIDs) and able to transfer data automatically, without human intervention, became the new reality.

In this white paper, we will address opportunities ahead in 2020, after four decades of accelerating progress has been realized in the IoT and Industrial IoT worlds. We will explore the value being created in the context of highly fragmented ecosystems, where industry consolidation is certain, and where enterprises who do not leverage connected systems will lose relevance and risk their futures when they fail to participate, or do not participate strategically. We will discuss serious concerns about privacy, security, data integrity, safety and ethics and consequently industry and governmental standards and regulations being put in place to address future challenges.



# Innovation and the Internet of Things

The Internet of Things is an umbrella term describing the instrumentation of our increasingly cyber-physical world. At its most basic level, it is using sensors to detect the state of a wide variety of objects. This can be the temperature in a room, the pressure in a tire, the vibration on a factory machine, the precipitation on a floor, the blood glucose level on a human being, and on and on. As the moniker suggests, it uses the Internet to transport the sensor messages from their creation to where that information is used. By instrumenting so many “things” we begin to get a more granular understanding of the world around us. As a result, we can act in ways that are more efficient and effective, saving time, money, and achieving better outcomes across all walks of life.

The challenge is that companies must adapt at an increasingly rapid pace and in a profound way. There are widespread structural changes to almost all industries. The pace of change is increasing, and companies that do not adapt successfully will struggle or even fail to survive. As a result, we see a dramatic increase in corporate spending on innovation. Companies know they have to keep pace. According to available data, the average tenure of companies in the S&P 500 has gone from 33 years in 1965 to a projected 14 years by 2026. Corporate CEOs know they must innovate to remain relevant. Innovating internally, however, is almost always in conflict with the core and traditional business models of most companies.



The fourth industrial revolution can be described as the advent of “cyber-physical systems” involving entirely new capabilities for people and machines. While these capabilities are reliant on the technologies and infrastructure of the third industrial revolution, the fourth industrial revolution represents entirely new ways in which technology becomes a critical element of societies and even our human bodies. Examples include genome editing, new forms of machine intelligence, breakthrough materials, and approaches to governance that rely on cryptographic methods such as the blockchain.

The implications are far-reaching. For instance, by instrumenting physical assets to better understand the state of each asset, or groups of assets, what we can “know” and act upon is far more granular and informative than before. Second, the ability to aggregate and contextualize this information provides even further (in fact, much, much further) insight than that of a simple understanding of the state of an asset in isolation. This is augmented by contextualization with enterprise systems and other information to add further understanding that was not possible before. Moreover, that understanding provides the opportunity for actions that increase productivity and create all kinds of new opportunities.

# What's Different in 2020?

We are reaching a critical point in the evolution of this cyber-physical progression. IoT is no longer a “nice to have.” Industries are now changing on a grand scale, and the necessity to adapt is clear. As a result, the somewhat ordinary rendering of IoT in the past, most notably in the form of point to point silo solutions, are giving way to more thoughtful, holistic approaches to deploying this technology.

Most companies seem to recognize and agree that adapting to changes in the world, especially seen in the emerging cyber-physical world, is not a move that is “nice to have,” but is an absolute requirement. This recognition, in turn, signals a need for these companies to better understand the value proposition provided by integrating IoT into their corporate business model moving into 2020. This is a vital step in the right direction and will pay significant dividends in the years to come.



# Measurement, Management & Mastery

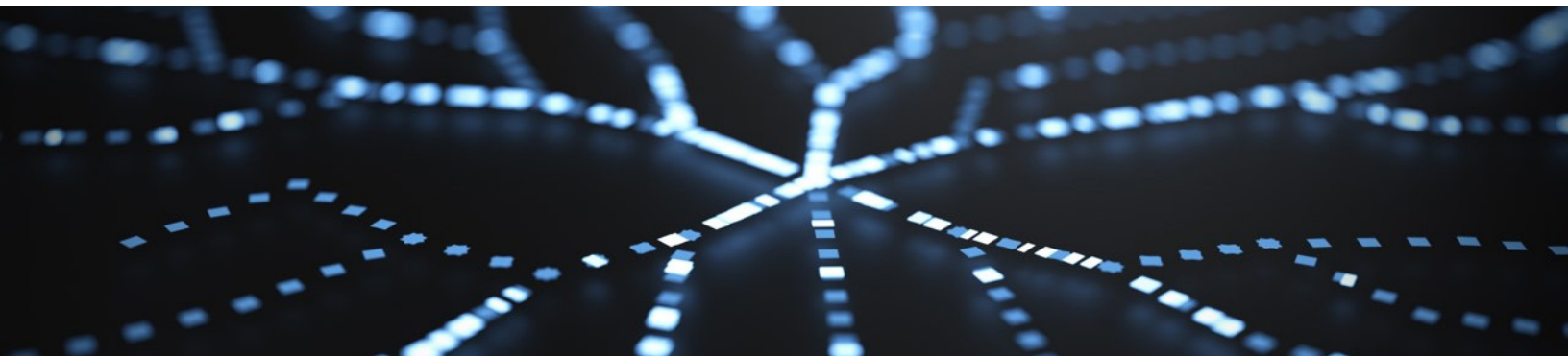
It is critical that enterprises begin to approach IoT from a holistic standpoint. This starts with “measuring” their state of assets. It also means that organizations must pay close attention to foundational elements associated with creation of the data.



The “management” comes in the form of data architecture and especially data governance. Decisions as to who owns the data, who can be stewards of the data, who should be able to see and use the data, all contribute towards achieving robust and useful datasets.



The “mastery” comes in the form of analytics. This can be operational analytics (what is happening?), investigative analytics (why is it happening?), and predictive analytics (what will be happening?). Beyond this, lies artificial intelligence (machines executing tasks that mimic the human brain) and the closely related concept of machine learning (applying AI in a way where we can give machines data and they can learn for themselves). This begins to pave the way for the agile systems of the future.



The measurement, management and mastery of the IoT space are all critical elements that enable companies to thrive and innovate. Each of these concepts are intertwined throughout this whitepaper and are essential to fully understanding the value proposition that IoT plays in a corporation’s future success.

# Why Build IoT Into Products & Services For Customers?

Vendors who see and appreciate the shift towards true enterprise IoT architectures will make strides to accommodate it, and in doing so, create their own competitive advantage, as their products will be much more attractive to customers buying them. This means viewing their solutions from the eyes of their customers, then making their offering as attractive and useful and accessible as possible.

Specifically, this means product providers pay close attention to data ownership, privacy, governance, security, and communications. Ideally, they not only have a strong grasp of what is needed to address these elements but offer them in a way that allows for accommodation into any given enterprise IoT architecture as easily and seamlessly as possible.

The integration of IoT into the business model enables a company's products and services to be competitive. If a company fails to take advantage of "connected products" their competition most certainly will. Examples of how companies have already integrated IoT into their consumer products include: 1) energy efficient products (e.g. water heaters and furnaces) sold to homeowners, 2) household appliances (e.g. washer and dryers, refrigerators and ovens), and 3) automobiles where manufacturers utilize downloadable software updates to fix glitches in vehicle operating systems. In addition, vehicle manufacturers have utilized data to better understand customer habits and their movements which has enabled them to monetize GPS data and such for marketing purposes.

When IoT integration is considered in an industrial business process model, there are several examples that can be provided. For instance, 1) the operation and maintenance of manufacturing equipment, 2) the integration of factory lighting, which is one of the largest energy uses for a factory next to the actual manufacturing equipment, and 3) the use and operation of assets within a management system. In each of these examples, the use and integration of IoT to a system has the potential to save significant capital resources on sunk costs and substantially increase the profits of a company.



The opportunities for application and integration of IoT into the commercial transportation and military sectors is endless. Within the transportation sector, for instance, commercial vehicle operators currently integrate with IoT to meet regulatory requirements of the U.S. Department of Transportation. Although commercial vehicles and operators must use the Internet to transfer operational data for hours of service, some of the operators have decided not to enhance their business operations by fully taking advantage of IoT software and data available. This has placed them at a significant competitive disadvantage to the rest of the industry.

Other examples of how IoT has the capability of enhancing competitiveness in the transportation sector include aviation, as well as, the passenger and freight railroad industries. The aviation industry has an untold amount of opportunity for IoT integration, which the industry has moved forward with, but has not fully developed into a streamlined competitive advantage for one company over another. A few ways the aviation industry currently uses IoT is interacting with passengers and tracking baggage, as well as, offering entertainment systems while airborne.

The railroad industry also has significant potential to become a more competitive industry with the integration of advancements of IoT into their business practices and models. The industry currently uses IoT for passenger interaction, such as ticketing and marketing, and Wi-Fi on operating passenger railcars. There are two additional and important areas within the safety operations of the railroads where IoT can benefit operational competitiveness. First, is the expansion of the use of IoT in Positive Train Control (PTC) implementation, which is required by Congress, as well as other safety initiatives. Second, is the acquisition and the transference of data in real time while physically or digitally inspecting rail, ties, and securement systems for anomalies and potential defects.

The application and use of IoT in the armed forces has significant benefit in saving lives while our soldiers, airman, sailors and marines are in theater. Although IoT integration has been utilized in securing communications, intelligence and reconnaissance, which are all essential to the war fighter's mission, the use of IoT in medical fields, human capital, logistics and other support roles makes the mission run more effectively and efficiently. These systems increase operational efficiencies and allow military leaders to focus on decision making instead of supply and support activities.





## Aligning IoT & Business Strategy

What is your business strategy? Are you an automaker? Are you an insurance company? Are you a consumer products company? Every company has a business strategy. But we are at a point in time where strategies are changing at an increasing pace.

The landscape for the automobile manufacturer looks entirely different today than it did 15 years ago and will likely look entirely different 15 years from now. It goes without saying that the landscape for the insurance industry will continue to change as well. The same can be said for healthcare, manufacturing, and most every other industry.

In many respects, there is very little difference between aligning your IoT strategy and your business with aligning your information technology strategy, your operational strategy, or any other element of your business with your overall organizational strategy. IoT is one of many enabling pieces of the overall puzzle, and yet, the nature of IoT is inextricably tied to the very transformative factors that are changing so many of the businesses and so many of the industries we see.

Those companies who deploy an IoT strategy without fully understanding the relationship between the IoT strategy and their business strategy are making a mistake. The business strategy should come first. While there are numerous factors that should be considered within a carefully constructed IoT architecture, the decisions that are made regarding IoT should be in the context of achieving the strategy and goals of innovating the company to outpace its competition. While this is a painfully obvious statement, it is not universally practiced.



# Creating an IoT Roadmap for the Future:

1

**Architecture.** Start with architecture. The importance of this cannot be overstated. Key to this is separating the creation of data from the consumption of data which is effective for leveraging the utility value of that data. This way, the underlying data assets can be exposed for greatest leverage. Pre-processing the data makes sense to filter out inconsequential data from the master store. Last, the overall design should contemplate the fundamental organizational objectives. But “keeping everything” is a bad idea. First, while the price of computing and storage continues to drop, in most cases the data is growing at a faster rate than the corresponding costs of computational accommodation are dropping. That said, there is certainly a role for the visionary who understands the various component technologies and that the volume of data kept will likely grow but craft their architecture with a deliberate eye on the value of the data to the organization. It is critically important to understand the inter-relationships between the elements of the architecture, as a decision relative to element A may have knock-on effects on elements B, C, and D. While it is extremely difficult to find system architects that truly have a holistic understanding of the entire ecosystem, such understanding remains critical, nonetheless.

3

**Power Supplies.** Power supplies. Depending on the use case, devices may or may not have a direct power supply. More and more devices are battery powered. The earlier days of IoT saw many small, battery-powered devices with lackluster life. The power source is a great illustration of the inter-relationships amid the architecture. Decisions regarding security and communications will have a significant impact on the life of a battery. Battery technology is improving, and small battery powered devices are proliferating. Regardless, a careful consideration of power supply should be applied in the context of the rest of the architecture.

2

**Chipsets.** Not all chips and sensors are equal. The speed and capacity of the sensors, the materials and characteristics of the sensors, and the cost and practicality of sensors will differ from use case to use case. How a sensor is selected for a factory or an asset tracker or an invasive medical use will all bring a host of different requirements. On a broad scale, though, the cost of sensors is dropping, the size is shrinking, and the practicality of instrumenting more and more is growing. Sensor selection is generally a function of the device providers and not the enterprise. The key with respect to the sensors is understanding the data capabilities, the power requirements, and the addressability. Also, more and more we will see encryption built into the sensors themselves as security continues to be a critical issue.

4

**Communications.** The communication options are also increasingly strong. They are also widely varied. While some believe 5G is the Holy Grail, it is clear that LPWA (Low Power, Wide Area) options like NB-IoT, LoRa, and Cat-M1, as well as SigFox are good options for certain use cases with smaller, more limited transmissions like asset tracking and agricultural monitoring. And choices for closer proximity connections like Wi-Fi, Bluetooth, and RFID are still broadly in production, as is traditional cellular and LTE. The important consideration is to match the communication choice with the use case considering performance, volume, scale, security, chip capabilities, and power sources.

## 20 Factors to Consider in 2020

5

**Security.** It is hard to overstate the importance of security. While some people believe “data is the new oil,” the more accurate portrayal should be “trusted data is the new oxygen.” You cannot live more than minutes without oxygen. If you cannot trust the data from the wide proliferation of cyber-physical systems, then everything in world becomes undermined. But security is not easy. The ongoing innovation is compelling, but equally compelling, if not frightening, is the ongoing innovation in cyber-crime. Best practices would suggest a layered security model. Just like a building would have motion sensors and hardware locks and security cameras for multiple layers of protection, so should cyber- physical systems. Considerations should include symmetric key encryption, multi-factor authentication and biometric authentication, intrusion detection, malware and virus protection and more.

7

**Data Ownership & Governance.** Enterprises should want to own and control their IoT data in most instances. That is not to say you don't want the vendor to get it, because you do. The vendors can do a lot with it, and they will service you better as a result. You just don't want them to have it at your expense. That really means you want to be able to also create and use that data in the context of other IoT data from other smart products you are using, along with data from your enterprise resource planning (ERP) or other enterprise systems, including external data you might be pulling together, cleansing and enriching, then publishing to a variety of consuming applications at your region or corporate headquarters, as well as, providing subsets of that information to supply chain partners or regulators as appropriate. The overwhelming value of IoT will come from the data. Your company will benefit most if they can leverage the utility value of that data. Some will figure that out sooner than others, but you should be asking about this now. Considerations should include symmetric key encryption, multi-factor authentication and biometric authentication, intrusion detection, malware and virus protection and more.

6

**Privacy.** This will become the elephant in the room and should absolutely be considered in the context of any IoT architecture. At any given lunch meeting or even standing around with drinks at a cocktail party, it is not uncommon to hear people talking about the Equifax breach, or the looming concerns about what Facebook or Google is “doing with my data.” In the European Union, the move towards regulation has been solidifying for some time, resulting in the General Data Protection Regulation (GDPR), which went into effect in May of 2018. These regulations are seen as the first and perhaps most comprehensive approach to ensuring personal information is protected. It is largely viewed as a clarion call for organizations to anonymize data or face astoundingly large fines. In fact, the fines can be 4% of the company's annual revenue. There are a variety of approaches to addressing privacy. Some are better than others. Many organizations will spend a great deal of time and money on implementing IoT in their enterprise without carefully considering the role privacy could play going forward. That is a mistake. Considerations should include symmetric key encryption, multi-factor authentication and biometric authentication, intrusion detection, malware and virus protection and more.

8

**Scale.** This is absolutely an architectural consideration, but includes contemplation of volume, capacity, message velocity, and the nature of the use cases as well as the capabilities of the various processing, communication, and storage elements. Scale in technology has often been addressed by simply deploying bigger, better, faster, but when that has not been enough, the industry has shown an ability to accommodate. A good example of this would be eventual consistency. The notion that file systems would deliberately allow for the data to be out of sync for some time before “catching up” was heresy to some at the point it was first introduced. But the acceptance in the market was strong as people began to realize that not every application really needs to have instantaneous synchronization, and the result in making this accommodation was dramatic increases in scalability for the underlying systems themselves. This is absolutely application dependent. There will continue to be meaningful adaptation in IoT systems based on scale and use case dependencies.

9

**The Basic Analytic Stack.** IoT systems will make heavy use of operational, investigative, and predictive analytics. These are the traditional business intelligence tools like early players IBI, Crystal Decisions, Cognos, and Hyperion, as well as tools like column store databases used for dicing and slicing data for forensic analysis. That level of investigative analytics feeds into the creation of models for predictive analytics, which have come in the form of packaged solutions. One of the early successes in predictive analytics using sensor technology was provided by Smart Signal for doing predictive models for capital intensive assets like turbines and jet engines.

**Advanced Analytics.** AI and Machine Learning, Artificial Intelligence, and the more specific rendering of AI as Machine Learning are the critical elements of delivering truly adaptive systems. The net effect is to create what is essentially a “living organism” capable of adapting to changing conditions without intervention. Some instances of this are crystal clear, like the adaptive nature required in autonomous vehicles. Other examples might be more subtle, like the way your music stream adapts to your choices. But as data is more carefully curated, and more thoughtfully enriched, the capabilities of these systems will continue to increase, with huge implications and benefits.

10

**AR/VR.** Augmented Reality and Virtual Reality will play an increasing role in IoT, as more and more sensors feed the AR systems in areas like construction safety, asset maintenance and servicing, self-servicing, and even surgical procedures. Virtual Reality is a strong candidate for doing real time simulation for situational awareness, such as a model of where a crowd of people and vehicles would disperse during an emergency incident based on the vast amount of sensor data collected and modeled based in historical data, then used by first responders for determining and deploying access strategies.

**Digital Twins.** These are becoming increasingly important as virtual digital representations of their “twin” physical assets. This could be a car, a factory machine, or even an organ. Digital twins rely heavily on well-constructed architecture, where the connectivity and processing capabilities are capable of leveraging the most complete set of data to create the most accurate virtual representation possible. Digital Twins allow for advanced modeling of an asset without impacting the actual asset itself, and subsequently incorporating changes modeled against the digital version to be reflected back into the physical asset.

12

11

**Drones.** One of the other key technologies we can expect to proliferate within IoT is drones. These are getting more and more sophisticated. They are also one more example of the importance of architecture. The drone itself has power, payload, sensing and communication considerations. We are seeing advances such as swarm drones, where multiple drones will interoperate as a consolidated unit for a specific purpose. These are emerging in transportation use cases like rail inspection, in industrial use cases like off-shore oil rig inspection, and for a multitude of infrastructure and government use cases, especially for police and fire protection. We should consider drones in a growing number of use cases and within the context of the overall architecture.

13

14

**People & Training.** Organizations need to pay close attention to upgrading their human capital with respect to cyber-physical transformation. When planning, implementing, and subsequently operating these systems, there needs to be considerable attention given to the knowledge base of the teams responsible for all aspects of the systems. And because IoT spans the IT organization and many, if not most of the operations of a given enterprise, a single person overseeing the IoT initiative would ideally understand technology and architecture very well. This means, hardware, networking and communications, sensor technologies, data and analytics, user interfaces, and more. The CIO and the CTO are both fairly far reaching jobs already. A comprehensive grasp of technology doesn't come easy, and requires ongoing study and interaction to remain current, and thus, effective. But if a single person has responsibility and accountability for the IoT systems, a very real understanding of the information technology elements as well as the departmental operations, may be problematic. It's one thing to appreciate a publish-subscribe architecture or the possibilities of machine learning. It's another to appreciate the requirements of street lighting, or the imperatives and considerations in running the police department. One person cannot know everything.

15

**Organizational Structure.** Because IoT crosses operational and information technology spheres, logical organization structures must be examined. For instance, how are funding decisions made? Who "owns and maintains" these systems? Some organizations have put in place Chief IoT Officers or Chief Data Officers. Both are similar in nature. Consider the Chief IoT Officer. This person would not be expected to understand as much as the Chief of Police about police safety, or as much as the Plant Manager about the manufacturing system. But the Chief IoT Officer will need to have a working knowledge of these, along with an appreciation for the potential dependencies and inter-workings of various elements in a given organization. That's a tough call. Organizational adaptation requires a structure to accommodate the changing business processes. They also require new leadership. Those leaders must increasingly be some form of technologist and constant learner with broad comprehension about a variety of subjects, as well as, the ability to distill this information into a coherent strategy, communicate that strategy to a team, then execute that strategy.

16

**Leadership.** This is not an impossible task, but it is a challenging one. For starters, you have to have the experience of an elder statesman, but the drive to learn new things like a newly minted MBA. You need the negotiation skills of a diplomat in order to reach across multiple departments and organizations to be effective. This is not a job for the faint of heart, but it will become more and more a reality. Because it has such broad and deep demands, this is a role where many will fail. But there will be a few driven, smart, talented renaissance-like leaders who will rise to this challenge. But it is going to truly require renaissance-like qualities to make that work. That won't be easy.

17

**Financial Implications.** The idea that companies will invest in their IoT infrastructure only works if there is a clear economic payback to the company doing the investing. The idea that governments will invest assumes that the people are willing to support politicians that will spend tax dollars on long term, costly systems that will pay dividends, but perhaps not for a while. Some use cases are more obvious than others and some have quicker paybacks with smaller initial investments. That is where the progress will happen. In that progress comes awareness of the potential.

18

**Business Models.** Perhaps this topic gets too much ink, but it is absolutely clear that the pace of innovation and transformation is only increasing. The increase in digital assets is driving the evolving landscape of business models, and almost no industry is untouched. In healthcare, we are seeing everything from telehealth services to massive implications of wearable technology changing the requirements of in-hospital observation, with similar implications relative to aging in place. Ride share models are transforming the automobile and taxi industries, in part driving down car ownership. Autonomous vehicles will further turn the industry upside down. Assets will increasingly be provided as a service. Analysis of IoT within an enterprise should also incorporate analysis of the disruptive and the irreversible trends in their market. A potential example of this is when you consider that a company may well be in businesses tomorrow that was not even contemplated today.

19

**Ecosystems.** Jim Heppelmann and Michael Porter highlighted the progression of IoT in their paper in the Harvard Business Review in late 2014, showing products becoming smart products, becoming smart connected products, becoming product systems, and becoming system of systems. It is fair to say we are straddling the smart connected products and product systems at this point. As we progress, organizations will increasingly need to consider, and often cooperate with other organizations, in their ecosystem. This is not a new phenomenon in and of itself. In Japan, organizations have operated in Keiretsus since before WWII. However, in a cyber-physical world, these linkages and the associated data become especially important. Such relationships will also potentially align in the context of innovation. As we progress to a truly heterogeneous world, the idea that devices will interact autonomously with one another makes the ecosystem consideration all the more important. Organizations will need to thoughtfully deploy instrumentation with an eye on how such interactions will occur and what data can be given and received.

**Existential Considerations.** The key considerations and corresponding plans that are critical for every board of directors will be the need to identify and evaluate what cyber and climate risks are today and over the next five years. The importance of both cannot be overstated. These areas are essential for organizations to proceed into the cyber-physical world. This will have an impact on access to capital. This will have an impact on access to risk products. This will play a key role in any organizations quest for resiliency. Organizations need stability. Organizations need security. They need agility. They need scalability. They need profitability. They need sustainability. And they need equitability. These are the critical elements of resiliency and all are highly linked to a thoughtful and effective progression into the cyber-physical world. No organization will exist in a bubble.

20



# De-risking Innovation

The progression to the cyber-physical world is creating an imperative for all companies to innovate and adapt. Those who do this well will be highly rewarded, and those who don't will fail. The problem is commercializing meaningful innovation.

There have been a number of approaches to stimulating innovation for organizations. These include in-house innovation organizations, participation in external startup incubators, and participation in external startup accelerators. These all have positive aspects but have largely failed to deliver the overall desired results.

Internal innovation organizations remain common, but also tend to struggle. These are usually staffed by internal people, not experienced entrepreneurs, and remain a part of a larger, often bureaucratic organization. They generally have the prized ingredients needed for startups, including working capital and distribution structure for going to market. And yet, the speed, agility, and objectivity of the team are seldom that of an external startup. They take too long to incubate, and worse, they take too long and cost too much to fail. There are prominent examples of such failed efforts in every industry, from automotive to retail, manufacturing and more.

External incubators are essentially shared working spaces for startups. Over time, they have evolved with Entrepreneurs-in-Residence for mentorship, and some offer startup-focused programs, and most try to create the “vibe” for startups. For new entrepreneurs, this is better than simply operating as two guys and a dog in a garage, but the success rate remains extremely low.

Startup Accelerators are a more evolved rendering of incubators and show more success. These are organizations like TechStars and Y-Combinator that offer co-working space for a defined period of time (generally 3 - 6 months) and include more formalized mentoring and workshops focused on teaching young entrepreneurs how to raise capital. They run these periods as cohorts of around 10, to as many as 90 entrepreneurs, and often include a small amount of capital investment as well. Once they finish the program, they find their own space and go forward as a company, ostensibly first focused on raising capital then pushing forward. There are certainly a number of “graduates” of accelerators that have been enormously successful, yet the overall success rate, while higher than startups not participating in accelerators, still remains low.

More recently, we have seen growing momentum around an approach called venture studios. A venture studio is a company made of generally 10 - 12 people, who themselves are all experienced entrepreneurs. This would include a CEO or Managing Director, a key product person, financial person, engineering person, and a team of engineers, developers, and go to market people who all have successful startup experience. The new, inexperienced entrepreneurs with their idea for a company would submit to become accepted into a venture studio. Once entering the studio, the studio team essentially becomes a working extension of the entrepreneur. This serves two purposes, speed to commercialization and augmentation of the team.

# The Appeal of Venture Studios

The studio has all of the infrastructure in place. This includes systems like code management, payroll and accounting, help desk, etc., and includes relationships like legal, banking, accounting, and more. The studio team works with the new entrepreneur on the further vetting and development of the product. They operate side by side, there to help them make the right moves and avoid the myriad of mistakes that often kill small emerging companies. As a result, they evolve faster and with a higher probability of success.

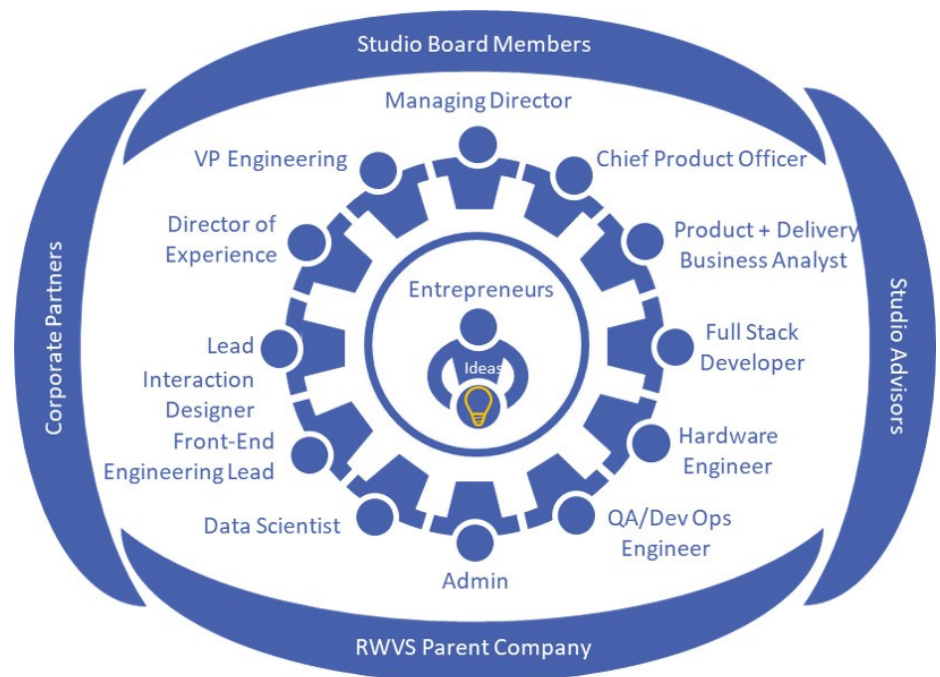
The studio team also is continually assessing the entrepreneur(s), making objective note of strengths and weaknesses and mentoring them on the job. This not only allows the studio team to guide entrepreneurs into the roles that suit them best as they move forward, but also highlight gaps in the management team and help recruit key people needed to augment the company before reaching the studio exit, which is a funding event or sale.

By taking a comprehensive approach to IoT initiatives, the venture studio model reduces risk for organizations who have tremendous upside opportunities, but lack experience and skills specific to IoT. Rather than experiment, entrepreneurs, enterprises, manufacturers, governments, and others can adopt proven methodologies and the best available technologies to increase their chances of success, avoiding costly programs that ultimately lead nowhere.

## About Rocket Wagon Venture Studios' Strategic Advisory Services

As a team of experienced entrepreneurs focused on the Internet of Things, we knew adding additional expertise would make the formula even better. In early 2019, we created an IoT-focused venture studio, pulling together a team with decades of IoT experience and successful track-records.

We then created a family of vertically aligned IoT Studios. Our commitment is to ensure that all solutions created in any Rocket Wagon Venture Studio emerge as architecturally sound, forward-looking and competitive solutions. Our Strategic Advisory Services team contributes to Rocket Wagon Venture Studios' vision to be the gold standard of creating companies for the cyber-physical world.



Learn more @ [RWVStudios.com/strategic-advisory](https://RWVStudios.com/strategic-advisory) or contact the author directly at [chris@rwwstudios.com](mailto:chris@rwwstudios.com).