FEDERAL TECH PODCAST

Ep. 57 Dual Use Technology & the World of Operational Technology

00:04
Welcome to the federal tech podcast where industry leaders share insights on innovation for the focus on reducing cost and improving security for federal technology. If you liked the federal tech podcast, please support us by giving us a rating and review on Apple podcast.

00:28
Welcome to the Philips tech podcast. My name is John Gilroy and I will be your moderator. Our guest today is Mike Wagan. He is the CEO and co founder of a company called shift five now because I'm obsessive compulsive and spent decades on the radio, I'll spell it out for it's the word shift Shi ft than the numeral five and.io. And you can go the website and you can see all kinds of different things to do. There's all kinds of videos about trains, about planes, and about the military. And that's the topic of conversation today. We've talked about trains and planes and militaries and security. But before we begin, I'm gonna have Mike maybe the thumbnail sketch of the company and how they can help their federal audience here. Got it. It's great to be here on the fedtech podcast. So you know, shift five is a fleet data company and we are also a dual US company. We were founded originally to solve cybersecurity problems on weapon systems, commercial airliners and railroad locomotives. But in the course of solving that problem, we built a solution that now helps democratize data and solve a variety of maintenance, operational readiness, operational sustainment and cybersecurity problems focusing on what we call operational technology, the really unique and what I think is really cool data bus technologies that allow all these onboard computers to talk to one another that make these exquisitely complex aircraft and ground vehicles and maritime assets work and, and be as effective as they are. Well, Shakespeare used to talk about things trippingly on the tongue, and then use that word, dual use that phrase dual use very trippingly. And there are some people who are listening to this that know exactly what it is. And some people that don't, I'm gonna try to give you my kind of layman's interpretation of what it is I always thought dual use was like a Swiss army knife or something. But I think in this context, what dual use means is technology that is used in the commercial world that also can be applied to the military world. Is that a working definition? We can start with? John Absolutely. You nailed it on the head. You know, we're we're very fortunate to be able to serve both federal and defense customers, and also the commercial sector and some of the most what I view as, you know, important, critical infrastructure verticals, right transportation, you know, chief among them, and in both the airline and in real red space. Well, let's get down to the nitty gritty. Let's go on to the, the bedrock here. So So what exactly is it? So how does your technology allow military folks to pay? You know, how to protect warfighters? And how do they maintain a competitive edge anyway, so John, when we look at a modern weapon system, think of a fighter jet, you know, in advanced, you know, tanks or a maritime vessel, what makes all of these things operate today, really is a bunch of embedded computers that all need to talk to one another and coordinate their actions. It's critical for mobility, for communications, you know, for for sensing for weapons delivery, and targeting. It is these embedded computers and electronics that, you know, candidly make our system so effective and provide the deterrent value, you know, that they afford

our nation. However, when we look at it from a cyber perspective, this is a type of cyber key terrain. At the end of the day, they're computers, and they're talking to one another. And they're using a very reliable and robust technologies. But in many cases, these systems were designed decades ago before an era, you know, what we now consider a contested cyber, you know, so there's a lot of opportunity for us to, you know, add censoring to this key cyber terrain, so that we can detect anomalies and faults and help protect, you know, onboard systems from, you know, would be malicious actors. When we do that. And we add in sensors to monitor for any type of nefarious activity in this cyber terrain, you know, under the skin and armor of these assets. We also get access to some of the most important and key data on the plot on these platforms, getting that data off the platforms and democratizing it enables us to solve a variety of maintenance and operations issues, that in the past, just were inaccessible to us because we didn't have the infrastructure, the hardware, the software, and the concepts and procedures to collect an aggregate and translate this data and then make use of it with modern algorithms and techniques. So shift five does all of that and it's a really exciting space. We're privileged to work on some of the most incredible engineering marvels for some of the most demanding customers in in some of them.

05:00
exciting mission spaces, I think anywhere in the world, your website talks about an onboard data company. And if you do research on that phrase, you find out that it's used by marketing companies as well. It's used for a lot of different purposes. And, and this is a unique purpose we're talking about here. If you go into the world of digital marketing, they talk about transferring data offline to online. And so what we're trying to do here in your case, is take data that's generated by multiple points all, possibly across the world, and bring it all together in one place and make sense of it. I mean, what are you gonna do for breakfast net, that's a pretty challenging job, isn't it, it's an incredibly challenging job. So, you know, when you think of some of the requirements and the operating environments, that the systems that we, you know, help tap and democratize data off of, they're operating in some of the most hostile

05:53
environments known to mankind, the environmental conditions, and testing is really challenging the data volumes, and the specific and very unique and,

06:02
you know, complicated protocols that are used on some of these mission critical applications, you know, force in approach that, you know, candidly, is unique, and the area of of cybersecurity. And so it's, it's, it's real exciting every day we come in, and we have to solve new engineering and data challenges. And we get to bridge this, this gulf between, you know, complicated system design and in architecture, and, you know, the world of operations research, cybersecurity, and, you know, prognostic conditions based on predictive maintenance. You know, data science. Last week, I was having a conversation with Colonel Eileen from the Space Systems Command, and she is tasked with, with buying equipment for state of the art activities and satellites and space. And what she told me, she said, Why in the heck would she design something and build it herself, when she gets something that's custom off the shelf or something right off the shelf, it saves money. Now, that sounds real good. If you're running Michaels donuts, or John's transmission shop, but you're not I mean, you're in a position where it may be cheaper for you to go with a commercial product than a dedicated

military product. So So where do you draw the line between public private partnership, especially with some of the secure information you're handling? Absolutely, well, I think some of the advantages of being a dual US company is that, you know, the commercial operators, you know, they optimize for slightly different use cases, then the defense, you know, market does as well. And, you know, each is unique focus actually complements the others operations. So what we try to do is bring this middleware infrastructure of hardware and software that can be easily plugged and played into existing systems or new systems that are being built to very efficiently solve specific requirements around, you know, data collection, edge computing, you know, maintenance, Operation sustainment and, and obviously, cyber protection of the digital architecture and terrain on these on these platforms, the more systems that we get on and in different domains, air, land, sea space, and subsea, you know, candidly the more efficient that we can offer this family of solutions to our customers. So, especially in the defense market, our capabilities always have to be tailored, because every satellite as a specific example is unique. But many satellites use common data bus technologies, and they try to use the same, you know, rad hard, you know, processors and architectures that have been battle proven, if you will, on prior constellations. And so, you know, it's just good business and sense to, I think, to the maximum extent feasible, leverage commercial off the shelf solutions that can be quickly and easily tailored, you know, to government applications. And candidly, you know, the commercial market likes to do that as well, for their applications and rail. And in an aviation, I'm like, I love talking about the Space Force. I love talking about laser communication feeds satellites, but let's put our feet in the ground here. I mean, literally on the ground here. I think everyone who's listening, this knows there was a little incident in Ohio, with a little train. And there's a problem there. And people are figuring out that there were sensors, that's gonna pick up your sensors on the tracks there. So maybe you can give us a maybe a view from your office window there the problem and, and and how it's been addressed, and how you can maybe step in and help the situation. Yeah, so John, my understanding was that, you know, we had a cards of ailment, and unfortunately, it was carrying hazardous cargo and, you know, pretty, pretty awful environmental situation, but a car derailment from a mechanical breakdown. One, one that, you know, candidly is probably impossible to completely reduce the likelihood of ever happening. You know, when there's a failure associated with the bearings around the wheels and the truck or of a car and you know that

10:00

Um, that cars moving down the line, it's going to create friction, friction creates heat, eventually, you know, you're going to have, you know, metal is going to melt, things are going to come off the rails, and you're going to have a problem. So, you know, how the freight industry monitors and attempts to address this risk is by having these Wayside detectors, you know, every generally 20 miles or so they're gonna have a detector that will look for any kind of equipment that's being dragged by the cars, like a brake hose or something else like that, you know, maybe at the, you know, at the end of the line, is also going to have some sensors to try and detect if there are hotspots associated with those wheels and the trucks. And so in this case, everything actually worked according to plan, as I understand, the detector detected that there was a hot wheel condition and alarm was set up and in the crew reacted appropriately. Unfortunately, just timing of the incident, you know, the derailment was, it was probably going to happen one way or the other. There are technology solutions to address this. That's not the the industry and the business that I'm in

11:11

what I you know, want to make sure that the freight railroad stays ahead of is making sure that the electronics on the locomotives, you know, stay secure, that they have good clean software and firmware, controlling the engine controlling the traction motors, that's literally what converts the electricity and makes them makes them go, I want to make sure that the operators, right, the that engineer and the conductor are getting good indications from their computer screens in the cab, and that nothing is being manipulated by an adversary. Just like, you know how we, we have computers in our office, those guys have computers that they use to, you know, control most of those high power locomotives on Main Line operations. So what shift five offers to the freight, you know, to the freight railroad market, and also to the passenger market is, you know, hardware and software solutions to monitor for any kind of tamper or cyber intrusion or malware on those onboard computers, and give confidence to, you know, the railroad and its employees that they have, you know, good trustworthy software and hardware that they're using to, you know, to haul cargo. You know, Michael, there's a podcast in town called Feds at the edge.

12:30

I think that should be your motto for your company there. But you're at the edge of it comes to railroads, when it comes to planes when it comes to satellites, when it comes to so many different areas. And I just think it's it's fascinating. Let's talk about airlines, my neighbor last over the weekend, he has an old Subaru and he changed out the Oh, two sensor in it, man, no big deal, you know, long as you don't strip it, you're fine. Pretty easy to do. Now, if you get a 737. And there's a sensor problem, maybe a more difficult to, and I don't think people realize the expense that it takes to maintain like these large 747. So these mid costs, the maintenance can cost millions of dollars to do that. And I think what a lot of time for the sensors can do is it can inform people and say, hey, look, XY and Z is happening here. You may want to do this because of that. And it sounds just so simple. It sounds like oh, it's just a little command that might go no, no, this could save hundreds of 1000s dollars, just one small component again. So when you don't can't disregard the value these sensors can you know, John, you can't. So the world of avionics, and you know, the computers on board, the our modern airliners that make them operate so efficiently and reliable, is fascinating technology that's been honed over decades. And actually a lot of Defense Innovation has enabled, you know, the modern conveniences and efficiency that we take advantage of, you know, when we fly with the airlines. So what, you know, shift five aims to do to help that market has made sure that we are collecting all of the data between onboard, you know, key computers and avionics onboard these aircraft. Now, today, a lot of advanced systems like airliners, they report out maintenance faults, they automatically consents, certain, you know, fault conditions and they can send alerts and indications some of that actually sent over the air while a plane is flying so that maintenance crews on the ground know, you know that hey, we might have a plane coming in that needs quite literally, you know, an oil change out of schedule, or it's going to need somebody to go check in and look at something. However, there are all of these types of unique issues that can come up that are called No Fault found maintenance conditions or other types of events where you know, there isn't a fault, but it's causing secondary systems to fail and an investigation needs to happen. A fault code at the end of the day required some engineer to think about a failure case in advance and write some computer code to look for that specific indication or signature and then

15:00

provide an alert indication, right? So what we provide is the ability to collect all of this other data and make it accessible to the community of interest, right? The integrator OEM, the avionics manufacturer and the operator, so that we can reduce those no fault found instances so that we can get to root cause analysis of, you know, maintenance failures and other issues faster. And ultimately keep planes in the air flying, where they're helping generate revenue and provide customer service at a higher rate. So that's, that's at a very high level, what we do there, but again, the technology, the problems, you know, the regulatory space around that is really fascinating. It's complex. And it's, it's bullet proof Tech, we want to make sure that everything stays reliable and safe as we enter, you know, the later half of the century. Yeah, the phrase predictive analytics comes to mind here, we're taking many different data sources and trying to make a conclusion from it, at your website is a phrase used called future proofing. So is that is that essentially what you can do with many different types of equipment through use of sensors and advanced diagnostics? We think so. So just by recording the existing data between these different computers, talking on a plane or a train or a tank, we think that by collecting 100% of that data on the edge, and being able to get that data off the platform, you know, whenever and wherever possible, centralizing, it enables folks to solve problems that we can't envision today, but that might happen down the line. That's what we mean by future proofing. In our case, we aren't actually adding new individual sensors to platforms, we're using the existing communications.

16:47

And in viewing the system as its own set of sensors in a way that hasn't traditionally been appreciated by, by the industry. You know, when we put an advanced aircraft through flight qualification, we have all of these orange boxes and orange wire, you know, data collectors and data historians and monitors when it's going through flight test. And then we take all of that stuff off. When it gets qualified, and you start mass producing something and it gets into production, effectively, what we think is, hey, let's let's build a very size, weight and power efficient system, tap all of that and collect all of the data because candidly, data storage is inexpensive these days. And there's tremendous, underappreciated value in collecting all of that operational fleet data that will allow us to solve problems that we really just haven't envisioned and appreciated moving forward. So that's some of the core thesis and what we mean by by future proofing. And so if you are looking to the future and try to, I mean, who could have predicted what happened, Ohio, no one could have predicted that, but you're in so many key points that you've seen. So where do you see this whole technology evolving in the next few years? Well, in the next couple of years, you know, we, we aim to, you know, continue to identify new use cases and uncovered new ROI using this data for our commercial and our federal customers. You know, again, we started doing kind of, you know, cybersecurity baselining systems, looking for anomalies and making sure that good clean software and firmware was running on all the embedded computers. And that's important for safety. And in the survivability of our weapons systems in a contested environment. However, we now appreciate that there's tremendous value in improving maintenance processes, and increasing the uptime and availability of these incredibly expensive, you know, fleet assets, locomotives, air, you know, commercial aircraft, military vehicles.

18:45

And as we move to the future, I think that we're going to uncover that the data can also be useful to inform operations, and to help make business decisions faster. This data incorporated with all of the other advanced, you know, kind of business logic that's already put into place in these various industries, it's going to be

complementary to the existing data transformation initiatives that we see, you know, the railroads, the airlines in the military, you know, continuing to to advance across their organizational interests. So sometimes companies just the right place at the right time. And what I see now is this whole move to the edge and, and you obviously have the qualifications for that, in fact, is a brand new acronym that people in the federal government and the commercial will start to use is called Secure Access Service edge. SAIC, and different people have different conversations about it. Some people say, at what point do the compute at the edge at what point to intermediating? What point to the data center, and how is that distributed? When it comes to satellite information? There's laser communication satellites, and at what point do you make the connection to the ground station? I mean, so this whole idea of at the edge, I think in the next few

20:00
yours, the real question is going to be well, what do we compute? I mean, isn't it is that question is brought up even now, but the way that we think about it is, you know, getting all of the data off these assets when they are in a place where they can communicate and send that high volume data, that's really helpful to solve all the problems that we just discussed around future proofing, and, you know, operations, insights, etc. But there are a lot of cases where you don't have connectivity, or it's not reliable, or you want to provide some type of indication and prompt some type of crew action without having, you know, a live data link.

20:36
So we think that folks need to think very, very carefully about that. And we have in our product architecture, right, we support disconnected operations, where the operators of a specific vehicle gets certain indications, from certain types of,

20:53
you know, anomaly detection, or other logic. You know, typically, those alert indications that, you know, those crew have already been trained to take certain actions, when they get it, hey, I see this happen, I don't need a data connection, I know what I need to do to, you know, continue to affect my mission. But where we can have, and when we can have real time data lakes, getting that data off, and up to, you know, higher headquarters in the military or, you know, to an Operations Center in, in an airline or in a railroad, you know, enables a level of planning that's helpful to keep things just moving. So we think very consciously about that, how much processing and what kind of processing and data store needs to happen at the edge, how the connectivity model works, again, across very austere and, you know, in some cases, contested communication environments, and then how to get all of that data centralized, translated, and then reviewed, so that you can you can find inferences across a fleet of assets, and identify things that are odd or off in the in the ones and twos, you know, find those needles in the haystack. That's also tremendously important. But all of that has to happen again, you know, Back Office in the cloud. So it's a really complicated, I think, conversation and one that is unique to each market. And in many cases, to each individual customer, it's my job to read the executive orders that come out and the last to mandated that every 15 minutes, I have to say the word cybersecurity, man, I have no choice. And you haven't said the word. So Michael, you're gonna have to do some push ups now or something because this hasn't come up in this conversation. I think I talked about, you know, going to Joe's doughnuts, I talked about cybersecurity or something. So this has got to be baked into everything we spoke about. So isn't it. So John, we, you know, we have really strong conviction that the more automation, the

more compute the more autonomy that get baked into all of these expensive fleet assets, the more important the cybersecurity, of these embedded computers in the, in the networks that they use to communicate with one another is going to be I think it's actually that simple. You know, when we think of the proliferation of unmanned aerial assets and their application in defense, and we think of what that could look like in the commercial market, I think everybody agrees that having some type of cybersecurity solution, you know, on a, a device that's operating in the physical world, where software is controlling this physical outcomes, that's just common sense. So we're positioning ourselves to offer solutions to those, you know, OEMs as integrators and the specific sub subsystems are avionics manufacturers that are supporting, you know, this, this new wave in aviation. So Michael, final question here. I made a silly reference to Feds at the edge. But increasingly feds are more and more at the edge where they can be working at home, whether they're in a satellite, whether they're at the edge of a battlefield somewhere. So in the next five years, where do you see your company growing is going more and more into the commercial area more into military or kind of a blender? Where do you see your company heading in the next four or five years? Well, John, we are unabashedly defense first, one in five, shift five employees as a veteran and and we're really motivated and focused on the national security mission, but we see the commercial

24:22
potential for our company as it's going to be a really exciting proposition in the in the coming years, again, as more automation, you know, finds its way into the railroads and into, you know, increasingly sophisticated glass cockpit systems and fly by wire aircraft come out from our aircraft OEMs we see, you know, an increasing need and opportunity on that data exploitation side for operations and other, you know, enhancements, you know, kind of growing in the commercial market. So I think in the next couple of years, we'll see the commercial business kind of catch up to what we're doing in federal and

25:00
In the future, certainly it's going to it's going to surpass because it's just a much larger market, in general and globally. Well, I think you've given our listeners a better idea of what onboard data is all about, and maybe some earmarks would look more into the future. You've been listening to the federal tech podcast with John Gilroy, like thank my guest, Mike wagon Cgo and co founder of shift five. Thanks, have a great day.

25:26
Thanks for listening to the federal tech podcast. If you liked the federal tech podcast, please support us by giving us a rating and review on Apple podcast.