Safety Doesn't Happen by Accident: System Safety Comes of Age
Part 2: System Safety as a Value-Added Business Driver

RAILWAY AGE – PODCAST

Bot, Sonia D., Tony Zenga, William C. Vantuono (editor). 2020. Safety Doesn't Happen by Accident: System Safety Comes of Age, PART 2: System Safety as a Value-Added Business Driver. *Rail Group On Air (Railway Age; Rail, Tracks, and Structures; International Railway Journal)*. Podcast. November 2020. https://www.railwayage.com/podcasts/safety-doesnt-happen-by-accident-part-2-rail-group-on-air-podcast/

TRANSCRIPT

QUESTIONS

1. You point out that "implementing a comprehensive safety program that meets the new demands of autonomous systems can be perceived as a daunting and risky proposition, especially when breaking new ground." How can such a perception be overcome?

2. Explain and provide examples of the five guiding principles of implementing a system safety program—rewarding an entrepreneurial culture, exercising business rigor and relevancy, forging productive partnerships, safeguarding end-to-end flow, and fostering a learning organization.

3. You note that "in some cases, safety failures are socially accepted within the walls of an industry." Why is that, and how can this be overcome?

4. What are "Big Bang delivery" and "isolated brute force"? You propose an alternative, "Entrepreneurial Time-to-Market." Describe that.

5. Why is it so important for safety to evolve from a cost center to a value-added business driver?

6. Final words, wrapping up the podcast

RA INTRODUCTION

Welcome to this edition of rail group on air the podcast series presented by Railway Age, Railway Track and Structures, and International Railway Journal. This is railway editor and chief - Williams C. Vantuono.

We are continuing our series on System Safety with Sonia Bot and Tony Zenga. This is part two of our Safety Doesn't Happen by Accident: System Safety Comes of Age series… and Part 2. We are going to look at System Safety as a value-added business driver. Sonia and Tony, welcome… this podcast series as well as the articles that are published in Railway Age Part 2 will be in the November issue part one is in the October issue part three of three will be in the December issue.

I understand that this has been very well received topic as it should be.

Sonia Bot – Yes it has, were are quite excited at all the feedback we've been getting and folks reaching out and stating how well this has been communicated how well it's hitting the points that we really need today in terms of system safety and there is quite some excitement out there.

RA QUESTION 1: You point out that "implementing a comprehensive safety program that meets the new demands of autonomous systems can be perceived as a daunting and risky proposition, especially when breaking new ground." How can such a perception be overcome?

RESPONSE – Sonia Bot

When I work together with leaders, organizations, and teams, I often come across, what I call, "the problem of the heap"… Imagine a heap, a disorderly collection of objects placed haphazardly on-top of each other… imagine a pile of blankets, bicycles, bottled water, shovels, flashlights, toilet paper, matches, hoola-hoops, you name it… and they are all entangled and locked into each other… there is no organization, no structure, it's a real mess to pull something out… and why are all these things in the same heap? Is there something missing from the heap? Are there things that don't belong in the heap? What is this heap all about?

This example heap is meant to be an emergency car kit. It is missing booster cables, flares, and first aid supplies. It's a stretch to see where hoola-hoops belong, and we can argue at length about the bicycles.

In business - and inside our minds - we also have heaps… for example, we are bombarded with safety heaps in our organizations and teams… more so these days with the onset of Industry 4.0, digitization and automation, where system safety is also now piled on… it's pretty difficult to find where and how you fit, how you align with others, and how you navigate through it… and where there are gaps and what things don't fit.

So the immediate perception, for many people, is that it's daunting, intimidating, and risky.

So, what we first need to do is to unravel the heap…. And in this case, we have a heap of safety, and now, with system safety piled into it too!

We start by defining a framework that connects all the parts, in the context of safety… In the framework we have components such as business objectives, safety objectives, a safety management system, system safety engineering, and so forth. With this we can see where various pieces fit in the greater connected whole… where people themselves fit in the big picture… And by having greater clarity, there is a better sense of direction and ability to work more effectively and safely.

From there we then systematically prioritize, plan, and work through the various items… And build out functionality in value-based increments… we deliver value at each step of the way… And we also systematically build up capability maturity of processes and skillsets as we go along.

RESPONSE – Tony Zenga

In reference to the problem of the "heap" and the framework as Sonia pointed out … I am going to talk specifically how that applies, when it comes a project.

From a System safety perspective there is a lot of confusion at the start of a project … even if it is an existing product which was previously fielded.

This could be for several reasons for confusion… New client, having different specifications, citing different Safety Standards and different deliverables than the previous project or… The system operational concept could be different from the previous project… There could be new key internal or external stakeholders on the project… There may be new suppliers with different system boundaries… We cannot assume that a subsystem will be completely supplied by the same vendor…

for example: A passenger train door system could be supplied by the door manufacturer excluding the mechanical doors (i.e., the door leaves) which could be supplied by a different vendor or the vehicle integrator).   This sort of thing results in a lot of finger pointing if an incident arise.

To unravel the heap therefore organizations should make use of experienced system safety professional to help them navigate through the program requirements complexities and respective engineering processes … much like a cruise ship captain who is responsible for the ship and its passengers that hands the ship control to the "Pilots" …. who's primary role is to advise the ship's officers regarding conditions in the port – … tides, … the location of sand bars, and changes in the ship channel.

I just gave a quick example of when a project is launched. There is an encompassing framework, and there are many examples through the program lifecycle… whether it is during the development, testing or field operations.

RA QUESTION 2: Explain and provide examples of the five guiding principles of implementing a system safety program—rewarding an entrepreneurial culture, exercising business rigor and relevancy, forging productive partnerships, safeguarding end-to-end flow, and fostering a learning organization.

RESPONSE – Sonia Bot

Thanks Bill… what you've just identified are the five guiding principles… which we can apply to implementing a system safety program.

I'd like to start by providing a little bit of background on these guiding principles, so that you can better appreciate them… so that they mean something to you… At their core, these guiding principles are based on innovation and sound business practices… and even more they address the global shift that has taken shape. In the past, businesses placed heavy emphasis on operationally improving. But now… businesses these days are not just about improving… they are also placing emphasis on differentiating and innovating.

So, let's dive into these guiding principles… I'll talk about the first two, and how about you, Tony, talk about the remaining three?   <TONY> Sure Sonia, sounds good! OK!

Let's start with the first guiding principle… which is "*Rewarding an entrepreneurial culture".* So, you are probably wondering what on earth does this mean to reward an entrepreneurial culture when we are talking about system safety? I don't want you to get the impression that this is an undisciplined free-for-all. What I'm really trying to say is that *Rewarding an entrepreneurial culture* means promoting the participation of all stakeholders …and creating the space to identify and act on emerging safety-driven opportunities.

Here is how this would play out in the context of system safety…

Let's start with entrepreneurial traits like creativity and controlled risk-taking… These are important traits for safety program managers, and need to be cultivated. However, these entrepreneurial safety program managers have different qualities than safety field personnel where they must adhere to strict safety procedures… Both must co-exist… Effectively, I'm saying that we must strike a balance between creative risk taking and adhering to strict safety protocols…

Next… managers now become more like orchestrators where they encourage cross-collaboration among functional teams and stakeholders… instead of just focusing on the administration of their own function. This cross-fertilization sparks ingenuity for mitigating safety related risks in order to determine optimum mitigation strategies, that is, better safety-driven solutions. It's a multi-function team effort, with multi-function accountabilities to a shared goal.

Next… in order for staff to participate and contribute their input to strategic level initiatives… It is necessary to have an environment where everyone feels safe to contribute on an equal playing field… with responsive feedback loops.

In addition… Safety organizations should consider reassessing their operating concepts to ensure they are adaptive to the ever-increasing complexity of systems and their environment.

Organizations also need to constantly re-examine decisions (for example, policy, financial, strategic) and then pivot… This is because organizations need to keep a tight focus on reducing risks in delivery and performance… and concentrate on doing the right thing.

All of this is done systematically and with discipline…

<Bill> So what you are saying, Sonia, is than an entrepreneurship mindset demands rigor and continuous delivery of value, and nothing less.

That's right!

Now, let's take a look at the second guiding principle… *Exercise business rigor and relevancy.*

Safety is a non-negotiable requirement for a railroad to meet its business objectives, obligations, and product / service offerings. When precisely fitting services to markets, or automating processes and solutions, the system safety planning and approach must be tailored for the application upfront in the early concept stage. Starting anytime later in the cycle adds risks to cost, quality of the solution, maintainability, and reliability.

The safety business case must include a multi-dimensional business assessment with clear definitions of strengths, weaknesses, threats, and opportunities.

As the system safety capability matures, safety can be positioned as a value-added business driver… and become less of a business cost center. And… on the commercial side, safety features, or their derivatives, can become revenue generating product and service offerings for customers.

So… these are the first two guiding principles… rewarding an entrepreneurial culture… and… exercising business rigor and relevancy…

Tony, I'll pass the baton to you to cover the remaining three guiding principles…

RESPONSE – Tony Zenga

Forge productive partnerships: Because of the complexities and scalability introduced in the digital world of system of systems or system integration, no one person or group or company can attack system safety alone.

Within a corporation, this is a multi-disciplinary effort across the corporation end-to-end, requiring productive partnerships to be established.

Highly specialized talent, not necessarily part of the current talent pool is required, for both the initial stages and the longer term.

In the short term, the surest, fastest, and most sustainable approach is to bring in a small tiger-team of elite professionals to assess, architect, setup, and assist in implementing system safety best practices … to establish work instructions and solutions to problems. In the process, employees learn and mature their capabilities through expert example. Furthermore, more emphasis can be placed on developing more productive and collaborative partnerships with the players in the transportation ecosystem (…such players would be, other railroads, air, ports, trucking, pipeline, subsystem suppliers, including customers) to pursue creative approaches to system safety challenges and also act as force multiplier for governmental agencies that do not have the resources to investigate every potential system safety issue.

(The 4th guiding principle is …)
Safeguard end-to-end flow: By its very nature, system safety requires an end-to-end system view, where the system can comprise of technology components, processes and people, and scale within and across organizations, companies, ecosystems, and supply chains. Typical areas of safety vulnerabilities include integration points of technology components and interfaces, handoffs between parties, and balancing supply chain implications at first- and last-mile terminals. One needs to follow and address (potential) hazards step-by-step from its point of origin and through the cascading web within which it impacts.

(The 5th guiding principle is …. to)
Foster a learning organization: As system safety is being embedded into the organization, company, and ecosystem, it is important to develop learning mechanisms that allow the adoption and execution of safety best practices. A continuous mastery and improvement mindset is required system wide; along with supporting tools and structures. Learning elements come from all areas (for

example, crisis, disruption, success) are augmented with leadership rotations through and within the ecosystem (for example, inter-disciplinary people exchange, skills investment, enterprise-wide mobilization to engage and build the leadership cohort). This requires fully committed, aligned, disciplined, transformational, and experienced leadership.

To reiterate the guiding principles, Sonia covered the first 2 Guiding principles which are: Rewarding an entrepreneurial culture… Exercising business rigor and relevancy… and I just spoke about the remaining 3 guiding principles which are: Forging productive partnerships, Safeguarding end-to-end flow, and Fostering a learning organization.

RA QUESTION 3: You note that "in some cases, safety failures are socially accepted within the walls of an industry." Why is that, and how can this be overcome?

RESPONSE – Tony Zenga

In some industries it is simpler to pay the costs associated with an incident or accident.

I'd like to remind the listeners .. that .. the roles of the system safety professionals is to perform hazard analysis and work with the organization to eliminate or control the safety related risks.

System safety professionals do not assign blame, this is the job of the courts.

Let me share 2 very high-profile cases…

The first case involves the Ford Pinto (the millenniums may never have heard of this ... but some of us probably remember the Ford Pinto)…

During the 1970s, the explosion of Ford Pinto's was due to a defective fuel system design … that was centered around the use by Ford of a cost-benefit analysis, … and the ethics surrounding its decision not to upgrade the fuel system was based on this analysis. Although Ford had access to a new design which would decrease the possibility of the Pinto from exploding, …the company chose not to implement the design, which would have cost $11 per car. Based on Ford's analysis, the cost to mitigate the safety risk would have been $137 million versus the $49.5 million price tag put on the fatalities, injuries, and car damages, and thus the company felt justified not implementing the design change.

… So here is what happened...

In 1972, a mother and son traveling in their Pinto was struck by another car traveling at approximately thirty miles per hour. The impact ignited a fire in the Pinto which killed one parent and left the boy with devastating injuries. A judgment was rendered against Ford and the jury awarded the family $560,000 as well as $2.5 million dollars in compensatory damages. The surprise came when the jury awarded $125 million in punitive damages on top of that.

(Source: https://users.wfu.edu/palmitar/Law&Valuation/Papers/1999/Leggett-pinto.html#Text)

… now fast forward to 2018 and the aviation industry…

The Boeing B737 MAX incorporated a number of design changes which included LEAP-1B Series turbofan engines, and made structural changes to accommodate the new engines, and other improvements as well as a Maneuvering Characteristics Augmentation System known as (MCAS) function.

Collectively, the changes incorporated into the B737 MAX design resulted in increased fuel efficiency, increased range, and a reduced noise profile compared to its predecessor, the B737 NG. As for MCAS … it is used to adjust the horizontal stabilizer trim to push the nose down when the aircraft is operating in manual flight, with flaps up, at an elevated angle of attack, so the pilot will not inadvertently pull the airplane up too steeply, potentially causing a stall.

Without analyzing this in too much detail, the MCAS became notorious for its role which led to the worldwide grounding of the aircraft and, in August 2020, the FAA issued a Preliminary Summary of the FAA's Review of the Boeing 737 MAX

(Source: https://www.faa.gov/news/media/attachments/737-MAX-RTS-Preliminary-Summary-v-1.pdf)

In the review… there are 12 global recommendations, one of which is: The FAA should take the necessary steps to ensure a total system approach to safety, linking all safety requirements from type certification to pilot training, and operational performance of the product.

From the two examples we note that companies and regulators are overwhelmed with the preparation and review of safety artifact.

Passenger rail is further ahead than freight by doing a voluntary self-assessment for safety. But the situation is improving given that In Feb 18th 2020 the FRA issued the Federal Register / Vol. 85, No. 32 / Rules and Regulations to require a Risk Reduction Program to be implemented by the rail industry.

RESPONSE – Sonia Bot

Bill, this is one of the most loaded question when it comes to safety… anywhere! This is a very complex area…

Tony spoke about a tactical business case perspective, which is high risk and by no means strategic nor sustainable, amongst other things… and this occurs across many industries, including our own in rail… whether in high-profile cases, similar to what Tony mentioned, or in lesser profile ones that have been perpetuating for the longest time and still are unresolved (think: derailments and collisions related to engineering infrastructure, mechanics of rolling stock, and human factors).

I'll take a step outward, and talk about the cultural maturity perspective…

First, we have psychological factors that can spread throughout an organization and an entire industry.

One factor is… Learned helplessness. For example: When you hear statements along the lines of… *“Things will never change, no matter what you do”…* it’s a sign of learned helplessness. People come to believe that they are unable to control or change the situation, so they do not try — even when opportunities for change become available.

Another psychological factor is Cognitive dissonance. For example: When you present a well-proven safety solution, you immediately hear push-back statements like…_*“This will take too long”… “Why do we need this now”… “This will add too much work”… “Another example of safety slowing things down and causing problems”… t*hese push-backs are signs of cognitive dissonance.

The two examples that Tony provided both show evidence of cognitive dissonance, and when digging behind the scenes, we also find signs of learned helplessness by the staff.

Second… safety laws can be complex… and so can operator-regulator relationships and dynamics. Safety laws and regulations are continually evolving to create safer environments, but it’s an ongoing challenge to keep abreast of these changes. Not only must you understand and adapt to these changes, you must also communicate them to your employees and ensure they can act on them appropriately.

The only way to move forward is to know where you are at… This is done by benchmarking the maturity of your safety culture. We can use the DuPont Bradley Curve as a tool to do this. It classifies four stages… from the least mature to the most mature…

1-Reactive: Individuals don’t take responsibility and believe accidents will happen. Safety is delegated to a lone safety manager.

2-Dependent: Individuals view safety as following rules and procedures. Accident rates start to decrease.

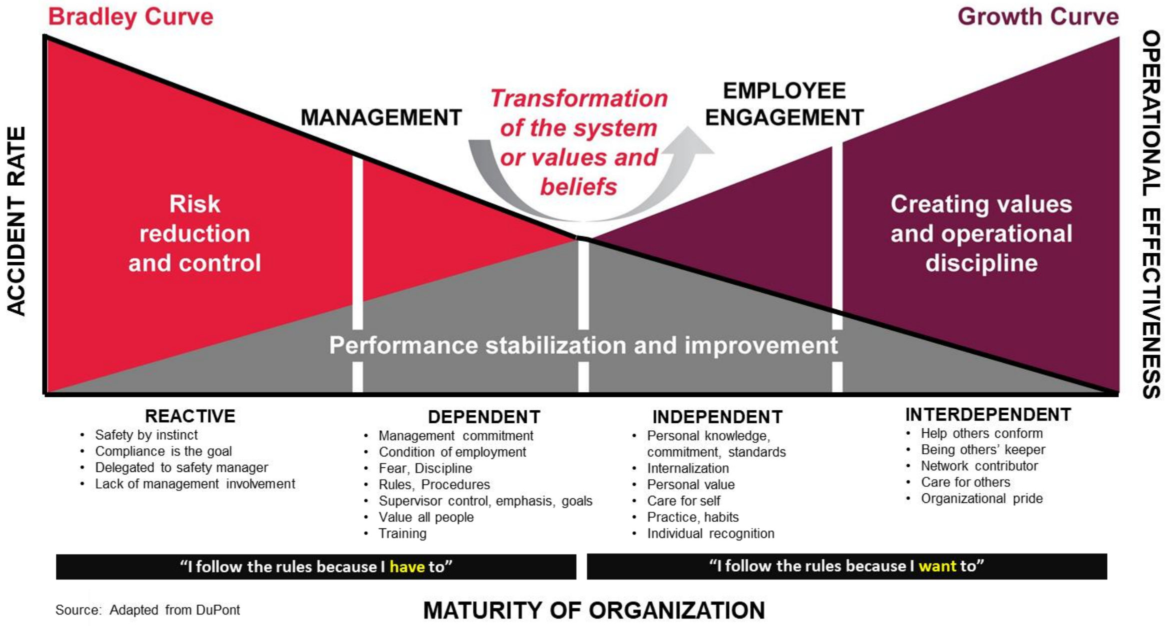
3-Independent: Individuals take responsibility and believe they can make a difference with actions. Accidents reduce further.

4-Interdependent: The shift moves from individuals to teams that own the safety culture. “Zero accidents” is an achievable goal. In rail, according to AREMA (American Railway Engineering and Maintenance-of-Way Association), the recommendation is to design safety solutions that have less than 1 catastrophic event per million operating hours.

So in the end… as the culture matures through the progression from the reactive stage (the least mature) through to the interdependent stage (the most mature), operational effectiveness improves, and that gives more room for pursuing profitable opportunities, while being safe and growing the enterprise.

I'd like to point out that organizations can move forward or backward in their cultural maturity. For example, Boeing was very mature in its safety culture at one point in time, with all of its processes, best practices, tools, and infrastructures in place… and everyone following them. However, there came a point with the 737 MAX where this eroded… where these processes and best practices were not followed or short-cut… and we are seeing the consequences. Executives can state to the investigators, the media, and the courts that they have good safety processes or best practices, however, if they are not followed, they are not being useful. So, you need to always be vigilant where you are at on the safety culture capability maturity curve.

In the long run, by having the awareness of knowing where you are at, you can then move forward with real action.



Source: Adapted from DuPont

RA FOLLOW-ON QUESTION: I just want to expand on this briefly. I've been following the space program since I was a child in the 1960s growing up with the Apollo program. The two space shuttle disasters; the Challenger where the solid rocket booster burned through and caused the external fuel tank to explode and the Columbia where several heat shield tiles had fallen off during launch where they were struck by pieces of the insulation on the external fuel tank that caused the shuttle to break up during re-entry. Those seem to me as though they are similar type of what you were just describing, would you agree?

RESPONSE – Tony Zenga

Having worked on space programs, I worked both on the robotic arm for Canadian Space Agency as well as several satellites. Yes! those were issues which were flagged; at least the first one that did not get the required support from the organization. Whereas the second accident was an unknown. Nobody thought that a foam could have done that kind of damage and therefore the mitigation to that accident was the addition of a robotic arm under the space shuttle to visually check that everything was fine before re-entering the atmosphere. So accidents do happen! the goal of system safety is to either minimize them or prevent them entirely.

When I worked for the space agency, I was reminded that although organizations such as NASA that have billion-dollar budgets, bad things can still happen. Therefore, everybody needs to work diligently when working on Safety System programs.

RA QUESTION 4: What are "Big Bang delivery" and "isolated brute force"? You propose an alternative, "Entrepreneurial Time-to-Market." Describe that.

RESPONSE – Sonia Bot

I'll talk about "Big Bang" and "Entrepreneurial Time-to-Market… and Tony, how about you cover "isolated brute force"… <Tony> OK, Will do!

"Big Bang development and delivery" is loosely based on the cosmological "Big Bang" theory… The notion is that beginning with nothing, you feverishly work at developing the finished product, which you produce in a mere instant (relatively speaking).

"Big Bang" delivery is fundamentally about simply starting the project right now, at this instant, with no formal development structure or organization... There is virtually no planning, organization, best practices, or typical procedures… A one-time, typically large, funding investment is made at the early beginning… There is a lot of experimenting, lots of trial and error improvements; which boils down to sweat equity until you get it right... It's full of high-profile heroics and firefighting… and it does not endure the rotation of leadership… Etc. Etc. Etc.

The "Big Bang" approach becomes increasingly risky, because success or failure is evaluated at the end of a long and expensive implementation cycle… The bottom line, is that "Big Bang" – or any of its derivatives – is too linear and simple for complex and safety critical systems… and the current business climate… This is why an Entrepreneurial Time-to-Market approach is much better.

The Entrepreneurial Time-to-Market approach…is low risk, nimble, and scalable… and aligns with modern approaches used by new entrant competitors… Capital and effort are allocated in stages… Tangible value is delivered in progressive increments… The system safety value propositions and methodology are embedded into the delivery framework, the systems engineering lifecycle… It is structured to be more inclusive of all stakeholders… And… it calculates and manages risk tightly… incrementally delivering value, earlier… and there is no waiting until the end of a long program cycle to determine success or failure.

So, we need to shift from “Big Bang” delivery approach (or its derivatives… depending where you are on the continuum) to rapid value-added delivery cycles as in the Entrepreneurial Time-to-Market approach.

Tony… over to you to talk about shifting focus from an “isolated brute force” approach to a more mature systems engineering approach.

RESPONSE – Tony Zenga

From isolated brute force to progressively interconnected system maturation focus… Railroads must still resolve longstanding human factors safety issues such as lack of adherence to policies and rules. Our system safety methodology is very systematic and relentless with its approach to cultural and capability development across organizations and across the ecosystem.

System safety is all about the performance of hazard analysis, their elimination and or control. System safety professionals have proven system safety processes and methodologies and hands on experience to evaluate systems and ensure that adverse conditions are considered, mitigated and verified. We make it a point to practically understand current maturity levels and progressively build up to its target levels. We utilize the Pareto principle as a starting point, recognizing that 80% of problems arise from 20% of their causes (unless there is solid data indicating otherwise), and applies business precision methods for prioritization.

With traditional approaches, focus is typically on individual departments or organizations within a railroad, and in several cases unnecessary large-scale “rip and replace” strategies are used; plus there is no consideration for the rest of the transportation ecosystem.

RA QUESTION 5: Why is it so important for safety to evolve from a cost center to a value-added business driver?

RESPONSE – Sonia Bot

The traditional approaches view safety as a business cost center. It costs money to clean up accidents or close calls… and it impacts your reputation.

I believe that we can do much better than that with our system safety approach… Rather than investing heavily on processes and systems to clean up mishaps and accidents, or gaming the system let’s shift focus in proactively building systems, solutions, products and services with value-added safety and reliability features upfront, where they can even generate new revenue streams. We can even consider system safety as a vehicle for adjacent segment strategies for growing the business.

With safer operations, the need for investing in processes and systems for cleaning-up decreases, and with the time and resources that are freed up they can be productively channeled for innovative and entrepreneurial endeavors.

From a commercial perspective, innovative safety-based solutions… for example, conflict avoidance algorithms, safety-specific test procedures for a given system… can be patented, where the patents can be monetized… for example, generating revenue streams from licensing, sale, or litigation. This is a potentially lucrative business model… as proven over the past decade in many industries that have taken advantage of technology-based innovation.

Also, in my experience, process waste is reduced by 20% to 80%. And this is proven through statistically correlated data of our results… I do not spew out these statistics lightly. The amount of improvement depends on where the organization starts from on the maturity curve.

With safety at the core and heart of railroading since the 1800's, this is one area where railroads have the potential to maintain competitive advantage!

RA QUESTION 6: Final words, wrapping up the podcast

RESPONSE – Tony Zenga

A very basic summary as a value added business driver: there is a need to move toward the guiding principles. Industry 4.0 demands a shift in traditional paradigms for safety in railroading. System safety engineering is at the core. When driven by the proven guiding principles, a railroad, including its partners, can effectively launch and progressively mature its system safety practice. As an added bonus, system safety becomes a mechanism for creating new revenue streams.

I would like to thank you Bill for giving us the opportunity to introduce the listeners to the system safety engineering discipline and look forward to constructive comments from your listeners.

Safety is everyone's business!

RESPONSE – Sonia Bot

It's great that in the rail industry we are focusing on using new technology for improving safe operations… However, we must keep in mind that the digital and automation world continuously demands integration of systems and solutions… yet it is unforgiving to any short-comings in their integration… this is where system safety plays a crucial role… and the good news is that the methods are proven!

What's more, we can leverage the full potential of what system safety can bring to a railroad, beyond operating safely… it can be a lever for growing the business… and this requires a paradigm shift in how we are operating today.

In closing… we invite the listeners of this series to reach out to us with your thoughts… We'd love to hear from you as we evolve through system safety… and … the next generation of railroading together…

And I'll continue to say… These are really exciting times to be a railroader!

Contact

Sonia Bot**,** sdbot@botgroupinc.com or www.botgroupinc.com
Tony Zenga, tzenga@cmtigroup.com or www.cmtigroup.com