Safety Doesn't Happen by Accident: System Safety Comes of Age
Part 3: Identifying Overlooked Practices

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 3: Identifying Overlooked Practices. *Rail Group On Air (Railway Age; Rail, Tracks, and Structures; International Railway Journal)*. Podcast. December 2020. https://www.railwayage.com/podcasts/safety-doesnt-happen-by-accident-part-3-rail-group-on-air-podcast/

TRANSCRIPT

QUESTIONS

1. What are the three often neglected or not fully understood aspects of system safety practices?
2. What is System Safety Engineering?
3. Describe the seven components of developing a System Safety Program Plan

4. You talk about “Safety By Design.” How can safety be “designed.” Can you provide some examples?

5. What is a KPI? How is it applied?

6. Getting back to “Industry 4.0,” why does it require system safety?

7. 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 3. We are going to look at identifying overlooked practices. Sonia and Tony, welcome… this podcast series as well as the articles that are published in Railway Age Part 3 will be in the December issue, part one is in the October issue, part two is in the November issue.

RA QUESTION 1: What are the three often neglected or not fully understood aspects of system safety practices?

RESPONSE – Tony Zenga

Well Bill, … from our experience, the three often neglected aspects of system safety practices as a minimum are:

1. The integration (OR lack of) system safety in the systems engineering lifecycle,
2. designing for safety, and
3. process-based safety performance management.

By having these technical aspects in place, a system safety practice can effectively achieve its potential.
For example… The use of analysis modeling techniques such as Quantitative Risk Assessment, Fault Tree analysis or Bowtie models only! … used to justify safety to stakeholders … could bring a false sense of security, unless all interfaces are evaluated and engineered mitigations are validated and verified.

To add … Just like in a workshop … every tool has its special application, therefore each analysis technique … when correctly applied brings value to the overall system safety lifecycle. But you cannot ONLY rely on one analysis technique to claim the absence of safety related risks.

And in addition … there are other common system safety myths such as; The idea that a certified system is a "safe system"! When in Fact!.. Certification deals with the system behavior as specified … Safety however, deals with the system behavior under unsafe conditions. …. (As in our last podcast we gave the example of the Boeing 737 MAX – which was a certified product).

Another myth is … that "Operator error is the main cause of accidents" … This could be avoided … if the system is designed with safety in mind … which mitigates human machine interface weaknesses.

OR … Compliance to safety legislation or industry standards which may result in safe systems. … Unfortunately standards or legislation do not cover safety related mitigation in their entirety; especially with dealing with new technology.

And the last myth... IS the idea that … "The system is tested and therefore it is safe" – BUT that's not realistic! … Since you cannot test for the absence of safety related risks;

That is … "you don't know what you don't know" so how can you test for the absence of safety requirements ?

RESPONSE – Sonia Bot

Let's take a look at how this plays out…

It's well established that finding safety-related design flaws late in a lifecycle are very expensive to fix. When design flaws are found, we often see arguments arising… arguments on the validity of the design flaws… or… arguments trying to convince that they don't need fixing… or… arguments to put in a quick fix. However, the problem doesn't go away, and you see it repeating over and over… Arguing only causes delay… And then when a fix is put in, it is typically more like a stop-gap patch, than what a real design solution should be in the first place.

This can be avoided… by using practices that kick-in at the early stages and live throughout the systems engineering lifecycle… By #1 integrating system safety practices into the systems engineering lifecycle,
by #2 designing for safety, and by #3 using process-based safety performance management.

By addressing these three practices… costs of engineering for safety are considerably reduced, while increasing safety effectiveness and outcomes. Naturally, re-work (which is a form of waste) is decreased, which in turn compresses project schedules, lowers costs, and lowers risks on the project side… and improves performance and responsiveness on the operational side.

RA QUESTION 2: What is System Safety Engineering?

RESPONSE – Tony Zenga

By definition… System Safety Engineering is a design philosophy … and methodology used to prevent accidents by identifying and eliminating or controlling hazards. Hazards are system states or conditions that, together with a particular set of worst-case environment conditions… will lead to unsafe circumstances; Incidents or accidents.

System Safety Engineering is tightly connected to the Systems Engineering Lifecycle… Systems Engineering is an interdisciplinary field of engineering and engineering management that focuses on how to design, integrate, and manage complex systems over their life cycles.

When system safety is not connected or is in isolation from the systems engineering lifecycle… Safety ends up being handled as postmortem or backward-looking assurance activity. Then the domino effect kicks-in… and organizations get trapped into a vicious cycle of trying to manage the hazard.

RESPONSE – Sonia Bot

To emphasize what Tony said… The premise of system safety is one of synergy… a whole is more than the sum of its parts. System safety requires a risk-based strategy that is centered on identifying and analyzing hazards, and applying remedies using a systems-based approach.

This differs from traditional safety strategies that rely on the results of accident investigations or epidemiological analysis, such as the tracking of patterns.

The systems-based approach to safety requires the application of scientific, technical, and managerial skills to hazard identification, hazard analysis, …and the elimination, control, or management of hazards throughout the lifecycle of the system.

The good news is that system safety engineering is a well-established discipline that continuously evolves its methods and tools. System safety has been around since the 1940s era… when it became evident that once both aircraft and weapon systems became more technologically advanced and more money was put into them, their accidents became less acceptable.

Today, system safety is evolving to integrate Artificial Intelligence, AI… where the inherent stochastic and system design-based approaches allow us to address far more risks and manage uncertainty to much higher levels than the traditional deterministic and non-systems based approaches… This is more good news, as we can utilize, and benefit, from the power of system safety as it is today… plus system safety is the foundation for how safety evolves in the future with the use of AI.

RA QUESTION 3: Describe the components of developing a System Safety Program Plan

RESPONSE – Tony Zenga

To begin .. When rail systems are created,… modified or expanded, … Stakeholders (such as: suppliers, integrators and Operators)… need to deal with both ….the system being developed (*the product system*) and the system that does the developing (*the producing system*).

The Product system …. Is the Product itself … AND … the producing system is the system that produces the system.

For example: The product is a Train … and the Producing system … are structures that describe the product system … such as; The train requirements tree, … the train system architecture, drawings, schematics, databases and program plans.

For Safety, …. This is referred to as a System Safety Program Plan which…. is the rule book that describes to all stakeholders…. how the Safety Program will be conducted …. from a managerial and technical perspective.

To build on that … The System Safety Program Plan is done at the start of a program and it defines:

- The project scope,…. the organizational responsibilities,….
- The depth of the system safety hazard analysis (including software Level of Rigor), ….. AND resources.
- It describes … the system safety organization integration …. with other program engineering and managerial activities… *A side note here - It has been my experience …. that you can find vast opportunities to improve the program … simply by reviewing the System Safety Program Plan at the onset of a project)*.
- The System Safety Program plan … also needs to describe the System Safety Validation definition & Verification program activities… the Milestones and deliverables (that's the …What , When, and How many).,
- The plan …. Needs to describe: ...Tools such as the Hazard Tracking System to document incidents, hazards, respective mitigations, …. and the system safety integration with the hardware…, software … and Verification program activities … and results…. All of these elements constitute hazard log!.
- One more extremely important element which forms part of the System Safety Program Plan … is the definition of the program level safety related risks …. and their thresholds levels. There are at least … 3 or more risk threshold categories .. they are: (Acceptable, Unacceptable and Undesirable), … for simplicity we will only discuss two risk categories … which are: Acceptable risk …. which is the part of identified risk ….allowed to persist without further engineering or management action … and… Unacceptable risk. …This Is the risk which cannot be tolerated by the managing activity. Unacceptable risk need to

be either eliminated or controlled. However, … Making the "Unacceptable Risk" decision is very delicate and difficult …. yet A necessary responsibility of the managing activity. Also the decision is made with full knowledge … that it is the user who is exposed to this risk. Sonia and I are available to the listeners if they would like to discuss this very important point.

Source: [FAA System Safety Handbook, Dec 2000] --Unmanned Systems Safety Guide for DOD Acquisition, 27 June 2007

Bill, …. I spoke about the System Safety Program Plan key structures … and now I would like to discuss the seven components or tasks that should be undertaken … for an effective system safety engineering program.

The first step is to: identify safety constraints requirements… using a Process Model diagrams … consisting of Human, Controller and Hardware interface …. Safety feedback loop analysis.

Followed by: A Safety assessment of the system Operations and Maintenance… Also known as the Operating and Support Hazard Analysis (the activity is started after the approval of the System safety Program plan … and continues through-out the program): It is applied to identify hazards …. that may arise during operations of a system … And …. to recommend risk reduction alternatives or constraints applied … during the operations to ensure safety related risks are controlled or eliminated.

The next step is the Subsystem Hazard analysis: (which is started during the Definition, design & Build program phases)… This activity is used to identify hazards in subsystems …. of a larger major system. The activity evaluates functional failures …. or hazardous functions .. of the subsystem that may result in accidental loss.

At the integration level is the System Hazard Analysis **…. (**which is started as soon as the preliminary subsystem hazards results become available). This activity **….** examines the entire system for its state of safety. It integrates …. the essential output of the subsystem hazard analysis to identify safety weaknesses …. in the total system design by: analyzing the system interfaces …. including safety critical human errors activities … or omissions.

Similarly, the system of systems hazard analysis examines the entire ….. system of systems … for its state of safety.

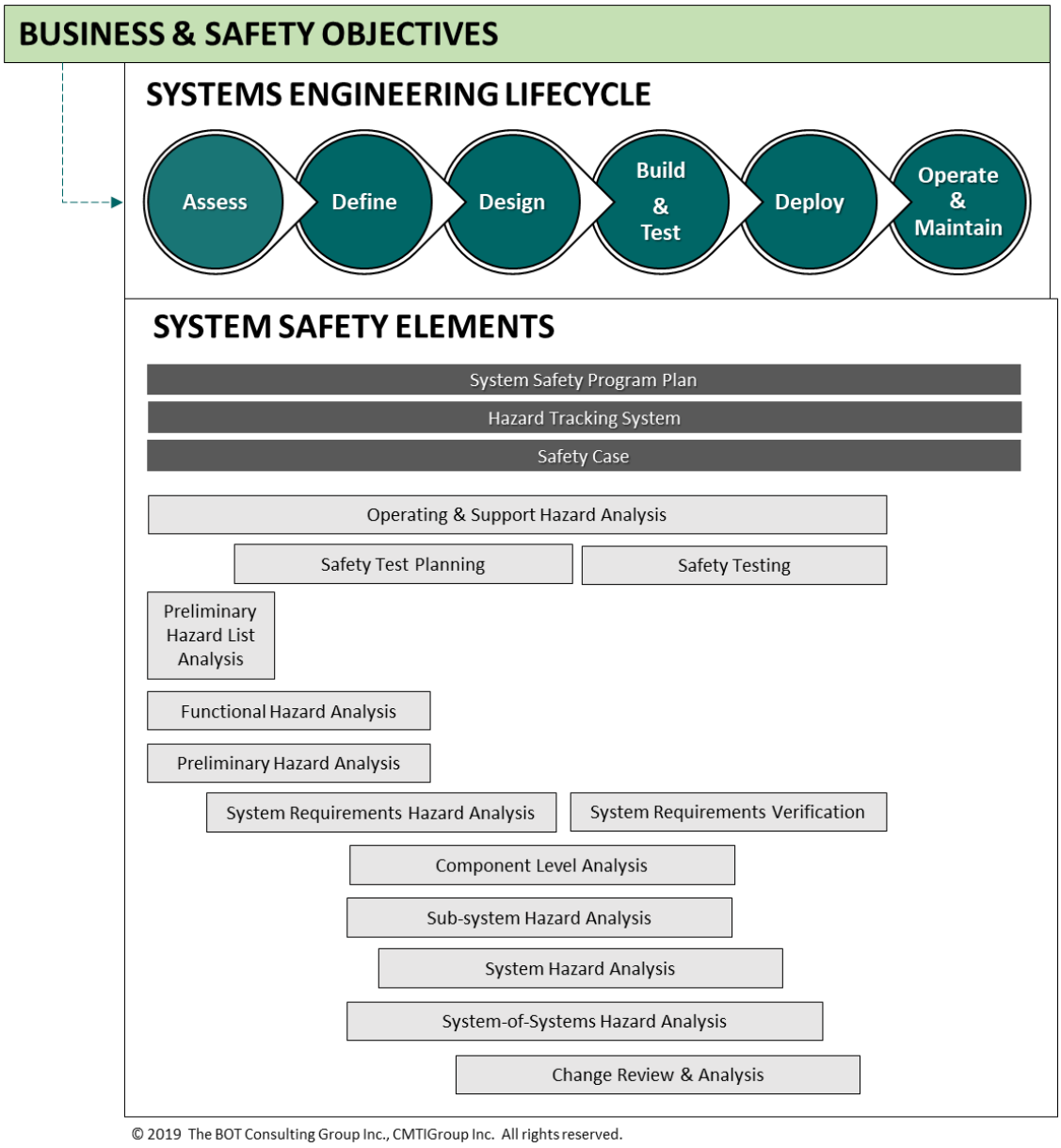
Going further in the design …. is the: Component Level Analysis …. which provide a systematic evaluation of the components based on their failure mode and effects …. that they have at the subsystem, or system level (for example, a door controller failure at the Door system level… and its effect on the integrated train). Each failure mode is categorized in terms of safety or service affecting severity criticality on the system (for example the train).

Another essential task is the: Functional Hazard Analysis which examines the system functions …. to identify: potential functional failures or …. functional behavior … and classifies the hazards associated with specific functional outcomes …. of failure or anomalous conditions. An example is the landing gear on an aircraft… this task assesses if the landing gear is commanded to deploy:…. - too early,… or too late,… or fails to deploy entirely…. when the aircraft is required to land. And …. what the end effects are from the safety perspective. Of course the output from the Functional Hazard Analysis are …. Safety requirements … which will form part of the system when designed and assembled … that prevent any bad outcomes from happening.

The Sixth Step is the … Safety Verification (which is done during the program testing phase). This task provides the necessary evidence through inspection, demonstration, and test results …. that the system comprising of its hardware, software, and human interaction complies to the system safety requirements … performed under special safety testing.

And the last step in the safety process is the Safety Case …. which is a documented demonstration and due diligence …. provided by an organization, to demonstrate … that the completed system can operate within the risk safety margins … defined in the System Safety Program Plan.

Bill, One more very important NOTE to the listeners: Although the safety engineers would have done all of the work I described; … Managing changes in the hardware… , software.. , or Operational procedures … need to be assessed by Safety before the system is allowed to operate. The changes could happen immediately after the system is delivered to the end user …. or after several months of its deployment. System safety must remain an integral part of the system.



System safety is present at every stage of the systems engineering lifecycle

RA QUESTION 4: You talk about "Safety by Design." How can safety be "designed."

RESPONSE – Sonia Bot

It is during the time when new technologies, or when solutions and features get added that you consider designing-in safety. This is done up-front within the early design phases rather than the more common re-design work that's done well after the testing stage. We are preventing hazards by designing them out in the first place. This is what I mean by "Safety by Design".

Now we will use a tool called the Design Order of Precedence. It is a framework with five levels… and specifically for safety. The five levels deal with hazard control measures… and range from the least effective to the most effective.

Now… let's look at each of the five levels…

At the very bottom… Level 1 is the least effective hazard control. Essentially it is a problem for people to deal with… And it makes it so by incorporating signs, procedures, training, and personal protective equipment (PPE). Unfortunately, this is often considered the first line of defense, when really it should be the last resort.

Level 2 is about adding technology that provides warning mechanisms… such as alarms and flashing lights.

Level 3 is about adding a protective barrier between people and the hazard…A simple example would be the protective shield over a table saw blade.

Level 4 is about replacing a serious hazard with a lesser one. A simple example is using a transformer to reduce a fatal high voltage to a low voltage that is not fatal.

At the very top… Level 5 is eliminating the hazard completely. One example that comes to mind is replacing toxic cleaning solutions with environmentally friendly ones… another example is replacing high volatile explosive fuels, such as hydrogen, with battery power… it doesn't change the operation.

RA QUESTION 4b: Can you provide some examples?

Sure Bill… I'll provide you some real life examples where we apply the Design Order of Precedence…

As our first example, let's look at the hazard of train over-speed derailment.

The very lowest level of protection is… giving the train crew speed-related bulletins, operating procedures, and posting signs on the tracks. The crew ends up being responsible for themselves and therefore prone to human error.

The introduction of PTC (Positive Train Control) raises the safety protection by providing speed warnings and other engineered features such as stopping the train if the speed warnings are not properly addressed. These would be Levels 2,3, and 4 design controls. As much as PTC reduces the overspeed risk, it does not fully eliminate the overspeed derailment hazard.

Imagine the full elimination of this hazard, with a solution that prevents trains from over-speeding in the first place; trains are programmed to process events in real time to travel at safe speeds based on conditions of the track, weather, geography, and consist, amongst others.

In reality, this is an example of how safety has been approached by multiple generations of solutions dealing with trains over-speeding. The industry paces through each level based on financial investment and technological support. Over time, the highest level of safety would be achieved.

As our second example… Let's consider electric trains docked at their maintenance shop, and powered through a 750 volts DC facility connector. The hazard is that the train can move unintentionally. One consequence is that it collides with personnel, causing bodily harm or death.

Once again, at the lowest level… providing signs, floor markings, and training the personnel to stay out of the way, makes it their responsibility to be safe.

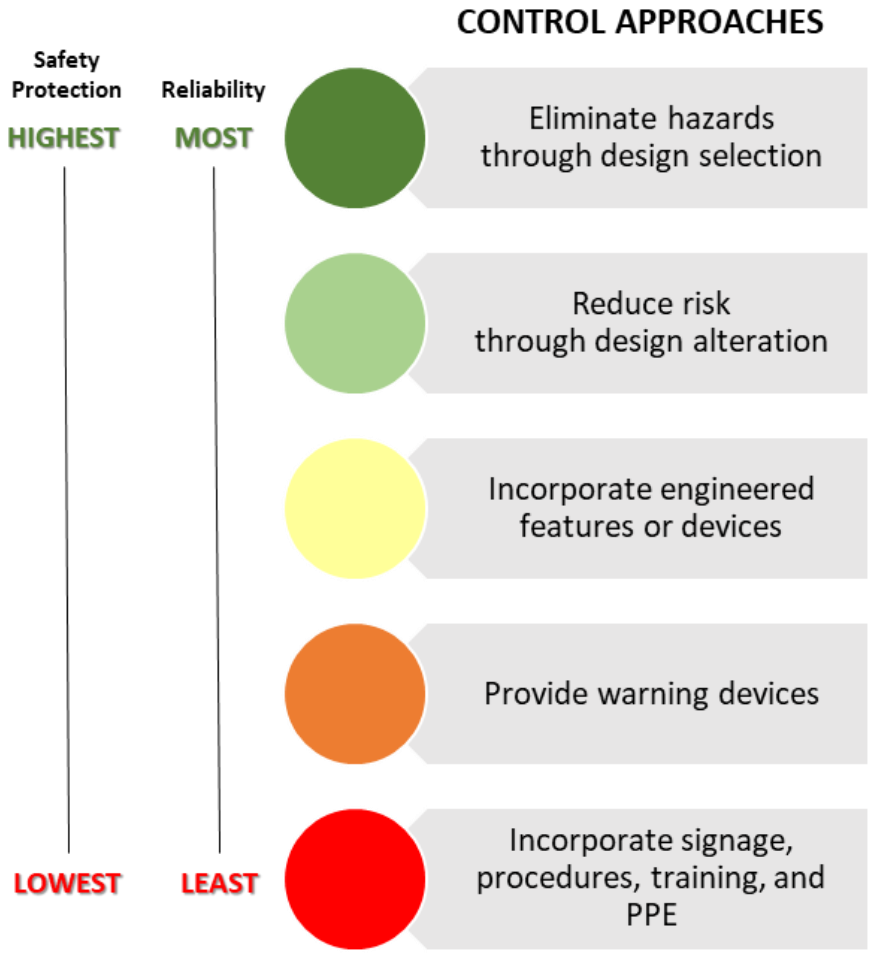
The next level of protection would include adding motion sensors or laser trip sensors that trigger visual-auditory warnings whenever personnel enter hazardous areas.

Higher levels of protection address the hazard at the source, such as tethering the train to prevent it from moving or reducing the power through electromechanical interlocks to disable train propulsion.

In this example, we see that the most effective hazard control adds no cost to a program when it is designed-in upfront during the assessment and definition stages however, it becomes very costly when addressed later in the systems engineering lifecycle such as during testing or field operations.

So… While the best approach to every hazard is to eliminate it completely, this may not always be possible or even easy to do. Tradeoffs may be necessary. Regardless… The levels of hazard controls identify where you are at in your safety solution.

Essentially… Safety by Design is all about preventing hazards by designing them out in the first place.



Reference: MIL-STD-882E DoD Standard Practice – System Safety

System Safety Design Order of Precedence

RA QUESTION 5: What is a KPI? How is it applied?

RESPONSE – Sonia Bot

A KPI is a Key Performance Indicator. KPIs measure a company's success versus a set of targets, objectives, and industry peers. KPIs are typically financial, customer, and safety related. After all, a company must be good at making money top-line and bottom-line (financial KPI), attracting and retaining customers (customer KPI), and operating safely (safety KPI).

KPIs are meant to be simple… and just the vital few… they are simply indicators that are specifically designed to flag performance issues so that direct action can be taken.

This means that KPIs must be defined top-down, with traceability from one process level to the next through a KPI tree. The top level KPIs are tied to the top-level processes of the company. And then you work downward through the sub-process levels. If you have more than a handful of KPIs for a process area or level, then it's time to simplify… focus on the vital few, and not on the trivial many.

It's really important that the KPIs must be explicitly attached to a process step, at its respective process level, where it is clear-cut for "where and when" to take measurements and providing a clear starting point for working through investigations and interventions.

This means that… If a KPI is not explicitly tied to a process step, then by definition it is not a KPI. This is a common mistake that organizations that make with KPIs. The consequence is that more than necessary effort is spent investigating and addressing issues… otherwise known as "waste" in the Lean world..... additional consequences include risks of making mistakes with understanding the messages in the data, gaming the system for vanity, and ultimately misleading the business… more forms of "waste"… and… exposure to safety.

To define and effectively use KPIs, a process architecture must be in place. Often, process architecture is missing. This results in processes that are misaligned and poorly adaptable. Which means their safety is in question… not to mention the amount of "waste" they perpetuate…And… Digitizing processes that are not properly architected is an exercise in futility.

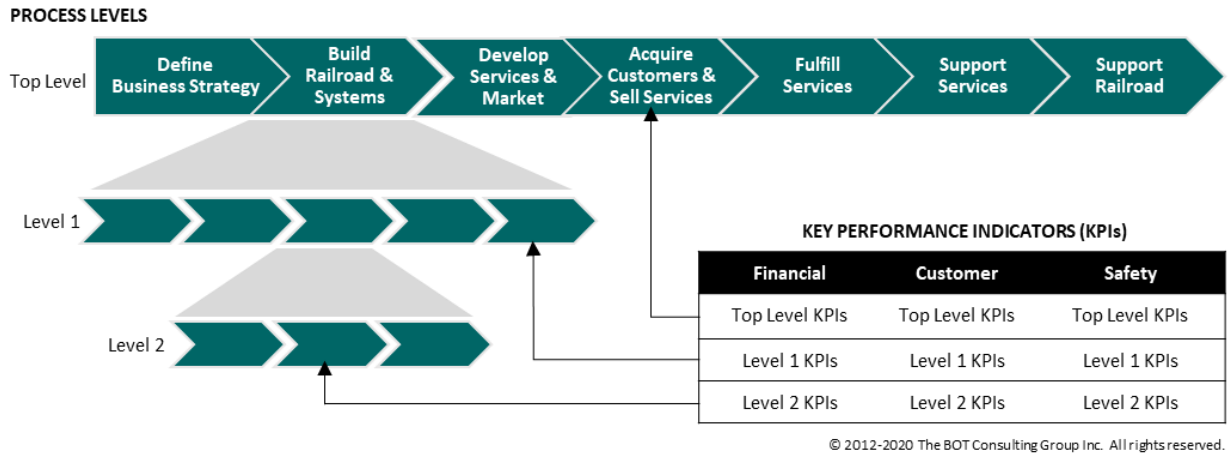
Instead, you must have process areas, processes, sub processes, and detailed process flows all tied together in a process hierarchy. From there, the traceable KPI tree can be readily put in place from the top level through to the lower levels of the company. And… any supporting technology solution and system must also be systematically tied into the process, as well as the data flow.

What I've just talked about is the direct link between KPIs and processes. Next I'll talk about how to be proactive using KPIs…

In today's reality…Many organizations only define outcome KPIs, where one needs to wait for the unfavorable outcome to occur before taking corrective action, thereby making the response a reactive one.

The proactive and more effective and lower risk approach is to couple the outcome indicators (outcome KPIs) with predictive ones (predictive KPIs), so that any corrective action can take place well in advance and thwart the occurrence of the unfavorable outcome. And, keep in mind, both the predictive and outcome KPIs are tied to process steps… and we focus on the vital few.

So, when it comes to safety, using predictive KPIs tailored for safety can go a long way in addressing hazards without waiting for the hazards to occur.



Relationship between Process Levels and Key Performance Indicators (KPIs)

RA QUESTION 6: Getting back to "Industry 4.0." why does it require system safety?

RESPONSE – Sonia Bot

Industry 4.0 takes automation and computerization into the future. Industry 4.0 promises to completely revolutionize how work is done… not just improving productivity and efficiency by a little bit.

Safety is embedded in every aspect and function of the railroad. For several decades, railroading has been filled with advances in mechanical, civil, chemical, and electrical engineering. Industry 4.0, which is in its early stages, introduces a greater need for advances in computer science and AI.

Because of this, in the Industry 4.0 world, we need to ask questions such as

- How do we know that these solutions and systems are safe - and that there are no lurking issues?
- How do we know that the integration of multiple components from vendors, partners, and even from within meet safety objectives?
- How do we know if safety integrity is preserved after a change is made?
- How do we shift the paradigm where safety moves from a cost center to a value-added business driver?

…and, of course, design and implement safe solutions in this new world.

System safety is the mechanism to answer these questions.

The bottom line… is… system safety is no longer an option, especially when it comes to Industry 4.0.

RESPONSE – Tony Zenga

System safety is required because of the multiple challenges ahead of us. The world of yesterday's problems have not gone away but continue to exist in contrasting and new context.

As Sonia pointed out - Industry 4.0 offers entirely new challenges through increased complexity of daily operations. Smart technology embedded in systems has started to push the envelope between efficiency and safety. System safety therefore needs to be an integral part of the solution and a recognized necessity for the industry.

RA Final words, wrapping up this podcast

RESPONSE – Tony Zenga

By embracing a holistic system safety program, railroads can shift safety from a business cost center to a value-added business driver. A place to start is by focusing on often overlooked or poorly understood key practices such as integration into the systems engineering lifecycle, designing for safety, and process-based safety performance management.

Starting the system safety activity with a Robust System Safety Program Plan… and Key performance indicators in place is a good practice.

You never want to be compared unfavorably to your competition when it comes to safety.

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

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 as I always 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