System and Software Safety Challenges for Widespread Acceptance of Driverless Vehicles

Gregory R Turgeon.; GT Software Services, LLC; Decatur, Alabama, USA

Keywords: driverless vehicle, system safety, software safety, system of systems

Abstract

Widespread use of driverless automobiles has the potential to save tens of thousands of lives annually in the United States. While the technology for these vehicles exists today, there are unique system safety and software safety challenges that must be addressed to ensure this lifesaving potential can be realized. The primary system safety challenge is developing techniques to assess the complex system of systems that is composed of the vehicle safety equipment interacting with other vehicles and the constantly varying highway environment. The primary software safety challenges are to ensure rigorous software standards are enforced and to tightly control the configuration of the software in each vehicle. These new challenges will require development and update of safety standards, regulation and enforcement by government agencies, acceptance by automotive manufacturers and suppliers, and training of the professionals developing these systems. The paper describes a potential driverless vehicle transportation system, identifies the system and software safety challenges to assure safety of that system, and lists specific steps for system safety professionals to generate the foundation to fully realize the lifesaving potential of this new technology.

Introduction

Several companies have announced their intention to field driverless vehicles within the next few years. While these early vehicles are required to operate within the current highway transportation system, widespread use of driverless vehicles could radically change the operating rules of the road. While the goal of vehicle designers is to develop vehicles that will never crash, there will inevitably be accidents that could cause injuries and fatalities. The role of system safety engineers and software safety engineers must be to help shape regulations that will minimize the hazards and develop the guidance, standards, and tools to ensure safety of the complex future transportation system.

This paper provides a context for the system safety and software safety environment that must be developed for the widespread use of driverless vehicles. It provides a framework for future efforts and research to begin to solve the challenges required to fulfill the potential lifesaving use of driverless vehicle technology.

As Joseph B. White wrote in the Wall Street Journal on August 28, 2013, Nissan Motors plans to offer cars with self-driving technology by 2020. It may be another 10-15 years before self-driving vehicles become widespread, which means the time to address the associated safety challenges must begin soon.

System Description

Current thinking on driverless automobiles is focused on single driverless vehicles added to the existing population of vehicles with human drivers. While this presents a set of safety challenges, this paper focuses on the challenges to be addressed before driverless vehicles are the majority of automobiles on the roads.

From a vehicle perspective, the following scenario is one description of what a single trip in a driverless vehicle could be like when driverless vehicles are widespread. Assume that an elderly couple would like to pick up a prescription and going shopping at a local pharmacy. One of the passengers indicates they are ready to take a trip by requesting a vehicle and selecting the origin and destination with their cell phone or computer. This initiates the closest available vehicle to be automatically dispatched to their home from a holding area. The vehicle pulls up in their driveway and a notification on the passenger’s cell phone indicates the vehicle has arrived. As the passengers enter the vehicle, the vehicle display asks for confirmation of the destination. The passengers confirm the destination and the number of passengers. The vehicle detects that both passengers have entered the vehicle and have buckled their safety belts before starting to back out of the driveway. As the vehicle is backing out, it detects a pedestrian walking their dog behind the vehicle and temporarily halts. The vehicle waits until the driveway is clear before it resumes backing up and then starting the trip. As the vehicle approaches the first intersection, it slows down slightly. The vehicle communicates with the cross traffic. All the vehicles approaching the intersection communicate with each other and negotiate the timing of their trip through the intersection. The vehicles weave through each other like a marching band crossing in formation, barely slowing down as they pass in close proximity. As the vehicle continues, it approaches a cross walk with pedestrians waiting to cross. A signal indicates to the pedestrians that it is time to cross. The vehicles closest to the cross walk stop and all the following vehicles quickly line up behind the stopped vehicles. When the pedestrians have safely crossed, the lead vehicles quickly accelerate with all the following vehicles accelerating in unison, leaving a uniform 2 meter space between the vehicles. The vehicle with our passengers seamlessly merges onto a 4 lane highway with other vehicles slowing down and speeding up ever so slightly to allow the merging vehicle to enter. It is rush hour and the 4 lane highway is tightly packed with vehicles leaving the uniform 2 meter spacing. The major intersection in town is now constructed as a roundabout with two 4 lane highways intersecting. Our vehicle needs to turn left, so it weaves through other vehicles to the 2nd exit in the roundabout. As with other intersections, the vehicles around it all communicate with each other and move to a defined protocol to allow each vehicle to move to its destination. It is choreographed like a well-rehearsed dance. Our passengers arrive at the pharmacy by turning into the drive way. The vehicle approaches the front door and waits until the passengers have exited. The vehicle then parks in the exact size parking space it needs. It is soon blocked into the parking spot by other automatically parking vehicles.

When the couple is in the store checkout lane, they use their cell phone to summon the car from its parking spot. The summoned vehicle communicates with the other parked vehicles that are blocking it in to quickly and efficiently move all those vehicles and allow the summoned vehicle to proceed to the front door to pick up the waiting elderly couple. The couple decides they would like to stop for coffee before going home, so they request the new destination using a voice command after they enter the vehicle. The vehicle confirms the new destination, verifies the passengers are seated and buckled and then drives them to the coffee shop. At the coffee shop, the vehicle indicates that it is low on gas and is going to automatically refuel while the couple is in the coffee shop.

Looking at the changes from the highway transportation system perspective, gives another view on the complexity of the system. The system is able to operate both safely and efficiently because of the cooperation between the independent driverless vehicles. Each intersection requires communication and negotiation between all vehicles that are entering the intersection. The protocols for this must be well defined and need to be validated to ensure that no collisions will occur. The protocols must include fail-safe conditions to prevent collisions in the event of communication failures, mechanical failures, or external events. The protocol specifications must be rigorously reviewed and modeled to ensure they are safe under all conditions. The implementation of the protocols on each vehicle model must also be rigorously verified.

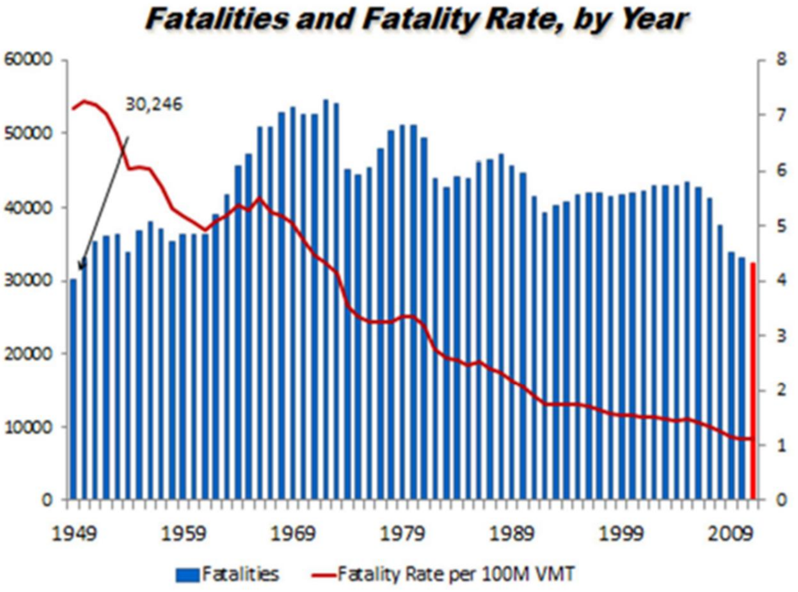
On the interstates and highways, the vehicles can be densely packed because driver reaction time is no longer a limitation. They can accelerate and decelerate as a single unit. The vehicles can also smoothly accommodate merging traffic by slightly slowing down or speeding up to make space for merging vehicles. Vehicles approaching a busy highway can also slow down to prevent overloading of a packed highway. This will alleviate the stop-and-go traffic seen on today's highways, which will reduce commute times, reduce fuel consumption, and reduce highway infrastructure costs.

In the city, the system will have to accommodate external factors such as pedestrians and bicyclist. City streets could be cleared up by automated parking, leaving street parking lanes available for either vehicles or pedestrian and bicycle usage.

System Effects and Benefits

Widespread use of driverless vehicles will result in many benefits to society. Among the benefits are lives saved, injuries prevented, reduced medical costs, increased productivity from reduced commuting time, infrastructure cost savings, and reduced emissions of CO_2 and other pollutants.

According to the United States National Highway Traffic Safety Administration, there were 32,367 fatalities from motor vehicle crashes in 2011 (ref. 1). This number has varied between approximately 30,000 to more than 50,000 fatalities per year since 1949 (Figure 1).



Fatalities and Fatality Rate, by Year

Figure 1. Fatalities and Fatality Rate per 100 Million Vehicle Miles Traveled Between 1949 and 2011.

Figure 1 – US Highway Traffic Fatalities

According to Sebastin Thrun, the lead developer of Google's driverless car, accidents can be reduced by 90% (ref 2.). Assuming that there is a corresponding reduction in fatalities, this could save more than 29,000 traffic fatalities in the United States alone.

Another 2.22 million people were injured in motor vehicle traffic crashes in 2011 (ref. 3). The use of driverless vehicles has the potential to significantly reduce these injuries and the corresponding medical costs. In 2010, 2.24 million people were injured in motor vehicle traffic crashes (ref. 4). The estimated cost of these injuries is estimated to be $99 billion in lifetime medical care and lost productivity (ref. 5).

While not nearly as significant as reduced fatalities and injuries, widespread use of driverless vehicles will more efficiently move traffic, especially during peak traffic times. This will reduce commuting time and pollutant emissions. One study estimated the delays caused by traffic congestion resulted in $121 billion in lost productivity and added fuel costs in the United States in 2011 (ref. 6). This is a combination of 5.5 billion extra hours and 2.9 billion gallons of fuel due to congestion delays. Google has stated their goal is to reduce traffic congestion by 90% (ref. 2). This would reduce traffic congestion costs by almost $109 billion in the US annually.

Amazingly, each gallon of gasoline burned by an automobile produces 19.6 pounds of CO_2 (ref. 9). Therefore reducing 90% of congestion delays could reduce CO_2 emissions from automobiles in the US by 51.2 billion pounds annually (90% of 2.9 billion gallons X 19.6 pounds per gallon).

Finally, cities and states can reduce infrastructure costs. The efficiencies of the driverless vehicle system will reduce the need to add lanes to existing roads and to build new roads that are currently needed to reduce traffic congestion. If done properly, this will contribute to a higher quality of life in addition to the cost savings.

System Safety Challenges

Driverless vehicles have great potential to save lives and reduce injuries. There are, however, significant system safety challenges to realize the greatest improvements. These challenges include the complexity and magnitude of the bold new highway transportation system of systems, the variability of the external environment, and developing methods to evaluate both the specification of the traffic protocols and the implementation in various vehicle model designs.

The main focus of current automotive system safety is in two arenas. First is the safety of each individual vehicle. The safety of the vehicle is considered including crashworthiness, active safety devices such as airbags, anti-lock brakes, and traction control, and the hazards caused by failure modes of critical components. There are significant developments recently in the area of crash avoidance systems. These include automatic braking, adaptive cruise control, lane departure warning systems, heads-up displays, and blind spot warning detection. The NHTSA is actively involved in research to validate the effectiveness of these systems on fleets of vehicles (ref. 1).

The second arena is a macro perspective of roadway safety. This is embodied as traffic engineers analyzing accident data to determine dangerous roads and intersections. This is also analyzed by NHTSA to provide feedback on safety equipment, speed limits, traffic laws, and factors such as distracted driving.

Widespread driverless vehicle use will create new system safety challenges. The aerospace and defense system safety communities have gained hard earned experience that will greatly benefit the safety challenges of this new environment. In particular, the system safety techniques used on complex systems such as the Federal Aviation Administration’s NextGen (ref. 7) and the Department of Defense Missile Defense System should be applied to this new complex system.

One new system safety challenge is to assure the safety of the driverless vehicle protocols. Assume that the vehicles automatically determine the flow of traffic at all intersections. Consider the case of two vehicles arriving at the intersection at about the same time. Also assume that the vehicles communicate with each other and use a predefined protocol to determine who will travel first through the intersection. Also assume that the protocol does not require any vehicles to stop, but only to slow down or speed up slightly to avoid a collision within some tolerance (for example 2 meters of clearance).

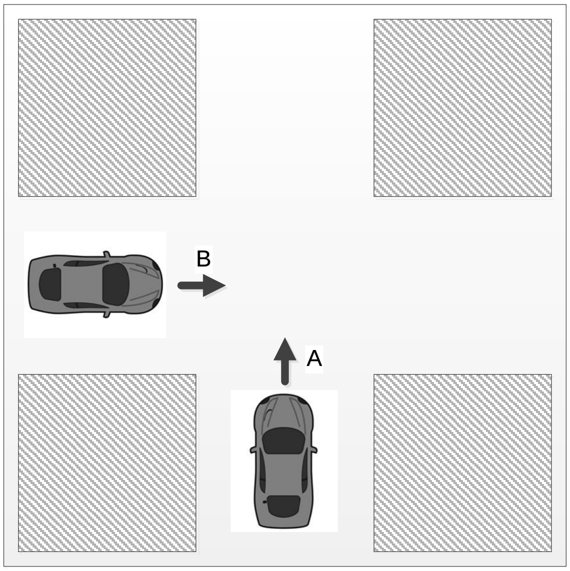


Figure 1 — Two Vehicle Intersection

One possible protocol for ensuring the vehicles proceed safely and efficiently through the intersection can be summarized as a decision table (Table 1).

Table 1 — Sample Two Vehicle Intersection Protocol Decision Table

Vehicle A Direction	**Vehicle B Direction**	**Vehicle B Relative Position**	**Vehicle A Fail Safe Mode**	**Resulting Action**
Straight	Straight	Left of A	No	Vehicle A through intersection ahead of Vehicle B
Right Turn	Straight	Left of A	No	Vehicle A enters traffic ahead of Vehicle B
Left Turn	Straight	Left of A	No	Vehicle A turns left behind Vehicle B
Straight	Right Turn	Left of A	No	No conflict
Right Turn	Right Turn	Left of A	No	No conflict
Left Turn	Right Turn	Left of A	No	Turns coordinated to prevent conflict
Straight	Left Turn	Left of A	No	Vehicle B turns left behind Vehicle A
Right Turn	Left Turn	Left of A	No	No conflict
Left Turn	Left Turn	Left of A	No	Vehicle A turns left behind Vehicle B
Any	Any	Any	Yes	Vehicle A pulls over and stops clear of intersection. Vehicle B pauses until Vehicle A pulled over.
(Partial Table- All Vehicle B Relative Positions Not Complete)				

System safety requires the protocol to be analyzed to ensure it is safe under all conditions. This example can be analyzed using manual techniques or using existing techniques such as formal methods. The protocol and the resulting system safety analysis become more complicated when other factors are included. For example, what is the protocol if 4 vehicles, one from each direction, arrive at the same time? What is the protocol when there is a line of traffic approaching from each of the four directions? Additional complexity is added when external factors such as road conditions, weather, pedestrians, bicycles, and animals are included in the system.

Development and safety analysis of the protocols developed may be done by industry standards organizations. System safety engineers will need advanced analysis techniques as part of these teams to approve the resulting protocols.

Verifying the correct implementation of these protocols in individual vehicle models will also require complex system safety techniques. Internal vehicle component and system failure responses will have to be identified, verified, and validated to ensure they meet the protocol under all conditions. A non-exhaustive list of factors that need to be included are vehicle maintenance, non-standard replacement parts, weather conditions, road conditions, exceeding specified load limits, and fuel quality. Unlike aircraft, the condition of an automotive vehicle has large variability over the fleet. Aircraft have stringent requirements for mechanics, replacement parts, mandatory inspection and replacement intervals, and extensive record keeping requirements. Automobile maintenance has none of these advantages, which requires a different set of assumptions in the safety analysis.

Finally, system safety must help define and specify safety solutions that provide independence from the components that provide navigation and steering. The assumption must be made that the vehicle software will never be proven safe under all possible conditions. Therefore, system architectures must be developed that will provide independent means to put the vehicle in a safe state when it is determined that the navigation and steering system is moving toward an unsafe condition. The independent system may include features such as crash detection and avoidance, moving to the side of the road, and broadcasting a warning to other nearby vehicles. Providing a safety mechanism that is independent of the primary software is a critical lesson that has been learned from previous accidents and must not be ignored when fielding future complex systems (ref. 8).

Software Safety Challenges

A critical component of driverless vehicles is the software. The complexity of this software and potential safety effects are significant. Unfortunately, based on empirical evidence, the ability of engineering organizations to develop and verify such complex and critical software is poor.

Considerations such as RTCA DO-178B largely rely on process assurance as the method to ensure the software meets the system requirements; including the system safety requirements. For complex safety-critical systems, process assurance will not be enough. In order to develop software that will meet the safety criticality required and to demonstrate the software is correct, the following criteria must be met:

1) The requirements must be specified in a notation that is unambiguous and can be proven to correctly meet the safety requirements.
2) The design of the software architecture must provide partitioning, be robustly fault tolerant, and provide a test interface that allows verification of both subsystems and modules.
3) The code must be written in a language or language subset that prevents common software errors. It must also be demonstrated to meet the software requirements specification. Also, static code analysis must be used to verify that common software errors are not present.
4) The software review processes must be thorough and efficient. The review processes must remove almost all software defects before the artifact is moved to the next software phase. Metrics must be used to track the efficacy of the review processes.
5) Software testing must be complete and thorough. It must verify both the integrated software and the software modules. The testing must verify each requirement, ensure that the code only implements the requirement (negative test cases), and that all code is completely tested.
6) The configuration management process must ensure that the correct data is used for each review and test. It must also ensure that the build process supports the complexity of the configuration combinations. CM must also ensure that each problem report correctly identifies each software issue and that each issue is correctly worked to completion.
7) The Software Quality Assurance organization must be domain knowledgeable and assure that each software process is performed correctly, that defective software products are identified and corrected, and that schedule or budget demands do not affect the safety of the software.
8) Independent oversight from knowledgeable regulators is required. Unfortunately, business considerations including budget, schedule, lack of training, and inexperienced staff do affect the safety of even the most critical systems. Independent oversight is required to educate new organizations and ensure that public interest and safety requirements are always met.

The aircraft industry is held to some of the highest software safety standards. A survey was conducted to determine how well the aircraft software industry would meet the criteria listed above. Based on the initial survey results for software on several aerospace systems, the capabilities of many software organizations would not be adequate to ensure the safety of complex driverless vehicle systems. This survey is based on 11 aircraft systems that were developed to RTCA DO-178B. The evaluation of these projects was to determine the capabilities of these organizations for the rigor and complexity that is required for driverless vehicles. Some of the key criteria evaluated were:

1) Formality and correctness of the software requirements description. In order to verify that the software specifications correctly specify the traffic protocols formal requirements specifications must be used. Almost all of the projects surveyed use natural language software requirements, which cannot be used to prove the correctness of the requirements.
2) Ability of the software architecture to ensure the stability of the executing software.
3) Ability of the test environment to verify both the software/system integration aspects and the low-level software robustness.
4) Capability of the Configuration Management (CM) and Problem Report (PR) systems to handle complex configurations and ensure consistency and completeness of all software artifacts.
5) Technical capabilities of the Software Quality Assurance (SQA) personnel and their ability to ensure quality.

The preliminary results of the survey are summarized below (Figure 2).

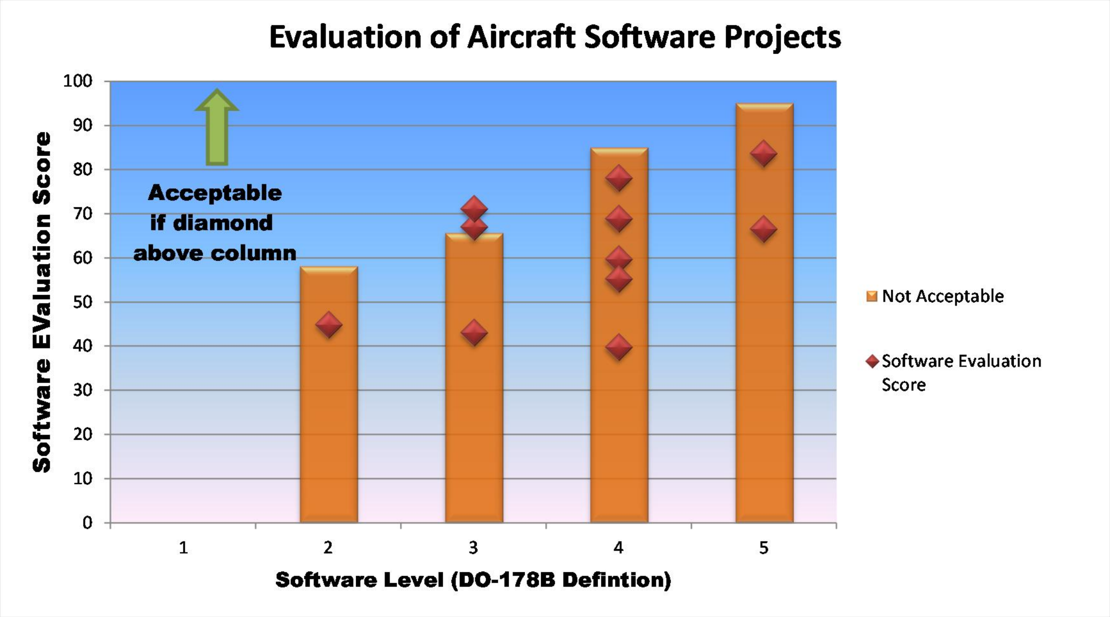


Figure 2 — Preliminary Software Capability Survey

Figure 2 key- Software Level on the x-axis: 1=Level E, 2=Level D, 3=Level C, 4=Level B, 5=Level A

An important note about this survey. This survey was looking for data that is different than the DO-178B and FAA criteria. For example, DO-178B ensures that requirements are developed, reviewed and tested. DO-178B does not specify that requirements be in a formal language or that natural language requirements are unacceptable. Therefore, these projects were found acceptable and were approved for their intended use in certified aircraft. The purpose of the survey was to determine if the techniques used for the aircraft projects would support the envisioned complexity and rigor required for driverless vehicles.

In summary, the survey demonstrates that even software organizations that are currently developing software for some of the most critical systems using the most rigorous standards are unlikely to meet the highest software standards that will be required for driverless vehicles. To remedy this, the following actions should be taken to ensure organizations are ready to develop this critical software:

1) Research is required to define the most effective tools and methods for this type of software. Based on observation, organizations use a variety of tools. They are effectively trained on each tool (usually by the tool vendor), but do not have integrated software processes and tools that together provide the most effective development, testing, CM and software quality assurance for safety critical systems.
2) Provide in depth training for the software managers, developers, test engineers, and software quality assurance engineers. Very few software engineers are trained on embedded, real-time, safety-critical systems. Extensive hands-on certificate training should be mandatory for engineers involved in developing, testing, and verifying these software systems.

Configuration management of the software in the vehicles will also be a key safety consideration. A capability must exist to update the software in the vehicles and to ensure that all the software in the vehicle is a safe set. As the communication protocol between vehicles evolves, there must be a method to ensure backward compatibility with previous protocols and age limits on the software to ensure that old software is phased out in a timely manner. Manufacturers will have to have procedures that ensure a safe software configuration is loaded in all vehicles at all times.

Conclusions

Widespread acceptance of driverless vehicles has the potential to save many lives and enhance our quality of life. There are system safety and software challenges that must be overcome to make this a reality. The most important issues to solve are: 1) better system safety methods for proving the protocols and their implementation are correct, 2) system safety methods to identify hazards and verify hazard resolution for complex systems, 3) improved tools, processes, and training for the software organizations implementing these systems, 4) added regulatory oversight of design approval of the driverless vehicles, and 5) enhanced configuration control of the software in the vehicles.

Professional societies must help to solve these challenges now to minimize accidents as these systems begin to be fielded.

References

1. Beuse, Nathaniel. “United States Government Status Report”, National Highway Traffic Safety Administration, 2013.

2. Mui, Chunka, and Carroll, Paul B., *Driverless Cars: Trillions Are Up For Grabs,* (2013), Kindle edition.

3. U.S. Department of Transportation, National Highway Traffic Safety Administration, “Traffic Safety Facts Research Note, 2011 Motor Vehicle Crashes: Overview”, DOT HS 811 701, December 2012.

4. U.S. Department of Transportation, National Highway Traffic Safety Administration, “Traffic Safety Facts 2010, A Compilation of Motor Vehicle Crash Data from the Fatality Analysis Reporting System and the General Estimates System”, DOT HS 811 659, August 2012.

5. Center for Disease Control, “Save lives, save dollars, Prevent motor vehicle-rated injuries”, DOT HS 811 659, August 2010.

6. Texas A & M Transportation Institute, “2012 Urban Mobility Report”, December 2012.

7. Fleming, Cody Harrison, et al. “Safety assurance in NextGen and complex transportation systems." *Safety Science 55 (2013)* 173-187.

8. Rankin, J.P., “Identification of Common Cause Failures in Instrumentation and Control Systems”, Hazard Prevention, Vol. 18, No. 1 Jan.-Feb. 1982.

8. EPA Greenhouse Gas Equivalencies Calculator. Accessed June 18, 2014. www.epa.gov/cleanenergy/energy-resources/calculator.html

Biography

Gregory R. Turgeon, Software Safety Engineering Consultant, GT Software Services, LLC, Decatur, AL 35603, telephone (256) 654-1621, email – gregturgeon@gtsoftwareservices.com

Greg Turgeon is currently a consultant software safety engineer. Mostly recently he has served as a Designated Engineering Representative for the Federal Aviation Administration, reviewing civilian aircraft software. Prior to his current position, he served as a software engineer and software team lead for various projects such as jet engine controls, the International Space Station, and automotive anti-lock braking systems. . His work leading a pilot project on formal methods verification of software requirements was presented at the NASA Formal Methods Symposium. He holds a Bachelor of Science in Electrical Engineering from Wayne State University and a Master of Science in Software Engineering from the University of Michigan, Dearborn.