THE LAC-MÉGANTIC TRAIN DISASTER AS A BASIS FOR A DESIGN PROJECT THAT EMPHASIZES SAFETY

Ralph O. Buchal, Nick Billingsley, Alex Bullock, Phil Poulin
Western University
rbuchal@uwo.ca

Abstract – Professional Engineers are ethically bound to regard public welfare as paramount, above all other considerations. Public welfare encompasses health, safety, economics, environmental and other considerations. These considerations are stressed throughout the CEAB graduate attributes. However, issues around public welfare are often absent from student learning experiences, particularly capstone design. This paper describes a capstone project motivated by the Lac-Mégantic train disaster. The students involved in this project researched the background of the accident, identified the contributing factors, and developed a problem definition to develop an improved braking system to prevent runaway trains. The proposed solution was a simple pneumatic drive connected to the handwheels of the manual brakes to reduce the time and effort involved in setting the brakes. This design could be retrofitted to existing rail cars at a cost of about $10,000 per car. Future improvements include implementation of a wireless control system to actuate and monitor the brakes from the locomotive cab.

Keywords: safety education, capstone design, railway safety, CEAB Graduate Attributes

1 INTRODUCTION

1.1 The Engineer’s Duty to Protect the Public Welfare

Engineers have a duty to protect the welfare of the public by ensuring that technical systems are as safe as possible, and minimizing the risk of injury or harm to people, property and the environment. The central role of Professional Engineers in protecting the public welfare is often not fully appreciated by the public, and by engineering students themselves. Professional Engineering is a regulated profession. Professional Engineers licensed by Professional Engineers Ontario are bound by a code of ethics that states that “professional engineers have a clearly defined duty to society, which is to regard the duty to public welfare as paramount, above their duties to clients or employers [1].” Engineers Canada defines engineering as follows [2]:

Professional engineers design products, processes and systems that protect the environment, and/or enhance the quality of life, health, safety and well-being of Canadians. They also manage world-leading companies at the forefront of emerging technologies.

This definition also highlights the paramount importance of protecting the public welfare.

1.2 CEAB Graduate Attributes

The CEAB graduate attributes also emphasize the engineer’s responsibility to protect the public welfare. The theme appears repeatedly in the attributes, as summarized below [3]. Emphasis has been added to highlight the theme.

3.1.4 Design: An ability to design solutions for complex, open-ended engineering problems and to design systems, components or processes that meet specified needs with appropriate attention to health and safety risks, applicable standards, and economic, environmental, cultural and societal considerations.

3.1.8 Professionalism: An understanding of the roles and responsibilities of the professional engineer in society, especially the primary role of protection of the public and the public interest.

3.1.9 Impact of engineering on society and the environment: An ability to analyze social and environmental aspects of engineering activities. Such ability includes an understanding of the interactions that engineering has with the economic, social, health, safety, legal, and cultural aspects of society; the uncertainties in the prediction of such interactions; and the concepts of sustainable design and development and environmental stewardship.

3.1.10 Ethics and equity: An ability to apply professional ethics, accountability, and equity.
2 DEFINITION OF SAFETY

Despite its central importance, it is difficult to find an overarching definition or framework to guide engineers in protecting the welfare of the public. Existing safety frameworks are typically restricted to specific domains, like workplace safety, transportation safety, process safety, etc. These frameworks contain common elements and methods that can be generalized to all domains, and the elements are described in a number of texts, e.g. [4, 5, 6].

2.1 Hazards, Risks and Safety Engineering

A hazard can be broadly defined as a potential source of harm. Risk is a measure of the combination of the likelihood of a hazard event, and the consequences or severity of the event. The goal of safety engineering is to design products, processes and systems in a way that reduces risks to acceptable levels. This is done by identifying and quantifying risks, and mitigating them by reducing the probability and/or consequences through a variety of measures. Zero risk is impossible to achieve, so it is important to establish the degree of risk that is acceptable. Value judgments are required to trade-off risks against benefits.

2.2 Harm

Most safety frameworks define harm quite narrowly, or leave it undefined. For example, in the area of workplace safety (occupational health and safety), harm is typically limited to injury and health effects for workers.

A broader view of harm would encompass anything that adversely affects the welfare of the public, which includes quality of life, health, safety and well-being. The issues become much more complex, and a holistic, systems view is required. A particular action or circumstance might result in short term benefit but long term harm, or might benefit one population but harm another. Difficult trade-offs are required, for example between environmental sustainability and economic growth.

2.3 Safety Management Systems

A comprehensive systems approach is needed to protect the welfare of the public by minimizing harm of different kinds, over different timescales and populations. Existing safety management systems encompass most of the required elements, but are generally discipline specific. Safety in the broad sense of minimizing harm needs to be a central consideration at every stage of the lifecycle of a system, from planning and conception to implementation to operation to end-of-life.

3 SAFETY EDUCATION

Professional engineers must weigh the benefits against the potential harm in the design of processes, products and systems. However, most engineering curricula, including design, focus on benefits and generally overlook harm. It is difficult to find mechanical engineering capstone design projects that require students to address issues of safety and public welfare.

4 A CAPSTONE PROJECT INVOLVING RAILWAY SAFETY

The recent train disaster in Lac-Mégantic provided motivation for a capstone project with an emphasis on public safety. The goals of the project were to understand the causes of the accident, and to design a system to prevent it from happening again.

4.1 The Lac-Mégantic Train Disaster

On July 6, 2013, a fully loaded train with 74 tanker cars containing highly volatile Bakken crude oil was parked unattended at the top of a hill outside the town of Lac-Mégantic. The unattended train rolled into Lac-Mégantic at high speed, derailing in the downtown core. The tanker cars ruptured, and the highly volatile oil produced an explosion and fireball that destroyed much of the downtown, and claimed 47 lives.

Officially the Transportation Safety Board of Canada (TSB) has established the following timeline and facts in railway investigation R13D0054 [7]:

- At about 23:00 on 5 July 2013, the train stopped at Nantes, Quebec.
- At 23:50, the fire was reported to the rail traffic controller.
- At about midnight, the engine was shut down, and the fire was extinguished.
- An MMA employee arrived on site to assist the fire department.
- At approximately 00:56 on 6 July 2013, the train started to move, after the fire department and MMA had left.
- The train rolled down the approximately 1.2% grade into the centre of Lac-Mégantic.
- The train derailed at approximately 01:14 on 6 July 2013.
- The locomotives detached from the rest of the train.
- There were no signals or track circuits, so the rail traffic controller would have no indication of a runaway train.

In addition, the media has reported the following information:
• The train was parked on the main-line instead of the siding because the siding is usually used for un-used train cars (even though the siding had a derailler device). The engineer left one out of five locomotives running [8]
• The engineer claims to have set manual brakes on 5 locomotives and 10 cars [9].
• Once the locomotive was shut down, it is likely that the reservoirs of air on each tank car leaked over time, releasing the brakes [10]
• The train derailed at a speed of about 101 km/h [11]
As with many accidents, the contributing factors included a combination of inadequate operating procedures, ignorance of hazards and risks, human error, equipment failure, and inadequate design.

4.2 Other Railway Accidents

Many of the risk factors contributing to the Lac-Mégantic disaster have been observed in other accidents, and the probabilities of these events is unacceptably high considering the severity of the consequences. There were 121 runaway rolling stock occurrences in Canada between 2003 and 2012 that did not result in a serious accident. In addition, 63 main track derailments were reported in 2012 [12].

Shipments of crude oil by rail have increased from 500 to 140,000 carloads per year between 2008 and 2013 [13]. Furthermore, it has been discovered that much of this crude oil is more flammable than previously believed [14]. In addition to Lac-Mégantic, derailments resulting in explosions have also occurred in Alabama and North Dakota.

5 THE PROBLEM DEFINITION

After analyzing the causes of the Lac-Megantic accident, the student design team identified the braking system as a key contributing factor. The brakes on trains are not intrinsically failsafe. The air brakes will release after a short time if the air supply is interrupted, and failure to set a sufficient number of manual brakes can result in a runaway train.

The problem was defined as follows: To design a system that will prevent a parked freight train from moving.

The design requirements were:
• Must be failsafe – failure of any component must not result in the train moving
• Must be compatible with the most common types of freight car types
• Must be intrinsically safe as per OSHA 1910.399 [15] (Class I, Div I during loading/unloading of combustible goods, different classifications based on material being transported)
• Must not require illegal modifications of train car
• Must comply with Canadian Rail Operating Rules (CROR) [16]
• Must comply with Association of American Railroads (AAR) Standards [17]
• Should improve worker safety and working conditions
• Should be economically feasible to retrofit existing train cars
• Should use standard, well tested components

5.1 Current Brake System Design and Operation

Each car has a tank of pressurized air which is used to apply the brakes when the locomotive engine is not running. These tanks inevitably lose pressure over time due to air leakage but the locomotive engine/compressor system, when running, will supply these tanks with enough pressurized air that the leakage is negligible.

These air tanks ensure that each car has the ability to apply air brakes. Because of this, the brakes are essentially always on and an engineer has to pump pressurized air to a “brake line” which switches a valve to separate the cars air tank from the brakes, effectively disengaging the brakes. As soon as this “brake line” stops supplying air pressure the valve automatically switches to reconnect the air tanks and the air brakes are applied. Over time if the engine is not running and not supplying air pressure to the tanks, air leakage can occur to make the air brakes ineffective [10].

The Canadian Rail Operating Rules TC O 0-167 [16] require the train operator to engage a “sufficient number” of manual brakes to prevent the train from moving when parked for more than two hours. Each rail company has its own requirements for the number of hand brakes to apply based on the number of cars and the grade of the rail. Setting the brakes requires an operator to walk to each car, and manually rotate a handwheel to specified minimum torque. Several dozen brakes may need to be set, and this is time consuming and exhausting work. In the case of the Lac-Mégantic accident, this was the responsibility of a single engineer to complete this difficult task at the end of a long day. There is some uncertainty about the number of handbrakes that were set, but clearly the number was not sufficient.

The current handbrake system has been in place for almost a century and is likely not to change. It consists of a vertical handwheel that is rotated to apply the brakes. The vertical wheel turns a drive shaft with simple gear reduction to pull a chain. When the wheel is turned the chain is pulled up and the wheel is locked using a ratchet mechanism that can be released manually.
Industry standards for the design of train car handbrakes are published by the American Association of Railroads, Standard S-475 [17]. The standard outlines everything from chain take up to handwheel diameter and mounting bolt hole patterns.

6 THE PROPOSED DESIGN SOLUTION

After considering many alternatives, the team decided that the best approach would be to design a device that could be added to existing handbrakes to improve their effectiveness and safety. It is not feasible to replace or extensively modify existing rolling stock, so the solution should be easy to retrofit to existing rail cars.

The final design concept (Figure 1) is described below.

- A drive sprocket is mounted to the handwheel shaft using a custom mounting collar. The collar and sprocket do not interfere with normal manual operation of the handwheel.
- A pneumatic motor and chain drive are used to rotate the shaft of the manual brake.
- The brake is locked by the existing ratchet mechanism.
- The motor is powered by the existing air tank on the car.
- The motor is controlled by a manual valve mounted on each car.

This solution will still require the operator to walk to each car to set the brakes. However, the physically demanding work of manually turning many handwheels will be eliminated. This will improve working conditions and worker safety, and reduce the probability that an insufficient number of brakes will be set. The design interfaces with existing equipment, and is inexpensive and easy to retrofit to existing cars.

The team selected and sized all components based on engineering analysis, and prepared a complete set of engineering documentation including drawings and parts list. The design includes full guarding of all moving parts. The estimated cost to build a prototype was about $12,000, including purchased components, material and fabrication costs. However, a prototype was not built.

6.1 Economic Analysis

The final design is likely to cost less than the prototype cost of $12,000. The cost to retrofit one car with this system will likely be about $10,000. CN Rail operates
about 30,000 tank cars, so the total retrofit cost would be about $300 million. If this was done over 10 years, the cost would be $30 million/year. This is about 1% of CN’s net income. The cost for other rail companies would be similar.

6.2 Risk Analysis

The proposed design aims to reduce risk of an accident by reducing the probability of a runaway train due to brake failure. While it is difficult to establish accurate values for probabilities, it is possible to argue that probability is significantly reduced due to the following reasons:

- The time and effort required to set the manual brakes will be significantly reduced. This will reduce the probability that an insufficient number of brakes will be set due to operator error or negligence.
- There is a large degree of redundancy. The manual brake system on each car is independent of other brakes. If a single brake fails, it will not result in an accident.
- The design operates an existing hand brake, so most of the system is unchanged. The existing system is well proven.
- If a failure occurs to the pneumatic drive, the brakes can still be set manually.

6.3 Occupational Health and Safety

In addition to improving rail safety, the proposed design will also provide health and safety benefits for rail workers by reducing the opportunities for accidents and repetitive strain injuries resulting from manually setting the handbrakes on many cars on a regular basis.

7 FURTHER IMPROVEMENTS

Ideally it should be possible to set the brakes from the locomotive, and to receive feedback that they have been set. Currently freight trains have no electrical connections between cars, so systems requiring wiring for either electrical power or signaling are not economically feasible. However, wireless battery-powered systems are available commercially. A suitable system would consist of an HMI and PLC located in the locomotive, interfaced wirelessly to a control node on each car. The control nodes would provide control signals to operate solenoid valves, and would collect inputs from sensors to confirm that brakes are set. Figure 3 shows a conceptual schematic of a wireless control system using commercially available DX80 Flex Power Nodes from Banner Engineering.

8 DISCUSSION AND CONCLUSIONS

Safety and protection of the public are key concerns of the Professional Engineer, and are required elements of an engineering education. This paper describes a capstone design project with a very strong emphasis on safety. It is desirable to incorporate safety considerations in most if not all capstone projects. In most cases this can be accomplished by identifying and addressing issues around safety and public welfare that would normally be overlooked or ignored. Perhaps every project should be required to answer the following questions:

- Is this design safe?
- What are the potential hazards?
- What are the risks?
- How does this project protect the welfare of the public?
- What are the long-term risks?
- What kinds of harm might result from this project?
This should be supported by broad education in the key topics of safety.

9 REFERENCES


