A Safety Case for Haul Truck Brakes

Presenter - Keith Larsen
Author - Keith Larsen

Manager, Engineering Services Department
Hastings Deering (Australia) Ltd.

Overview

A supplier Safety Case provides a proper plan for reliability of type proven commercial off the shelf (COTS) Haul Truck braking systems designed and manufactured overseas as already proven technological systems for worldwide use. Massive kinetic and potential energies are contained within normal Haul Truck operations, so to qualify for Zero Harm, proof is needed that Haul Truck brakes/retarders are always reliable. They must contain those energies by reliably slowing to a stop on grade and by being able to remain stopped indefinitely independent of external influence (other than by friction available at the rim/tyre & tyre/road interfaces). Brake failure means uncontrolled release of those energies manifesting in the generation of massive force and/or exertion of massive power.

It would be wise therefore to have sufficient excuse (delivered as proof of safety) for allowing persons to work in such places where they might otherwise be exposed to such force & power. The Safety Case could be viewed as a catalogue of excuses focusing on a simple examination/audit of reasonably accepted risk controls. The exam/audit format used is a simple substantiation to remove doubt that safety requirements are met within the chain of supply and use….Simply argued and demonstrated…Are all safety requirements met?…Yes✔ or No ✘.

Scope

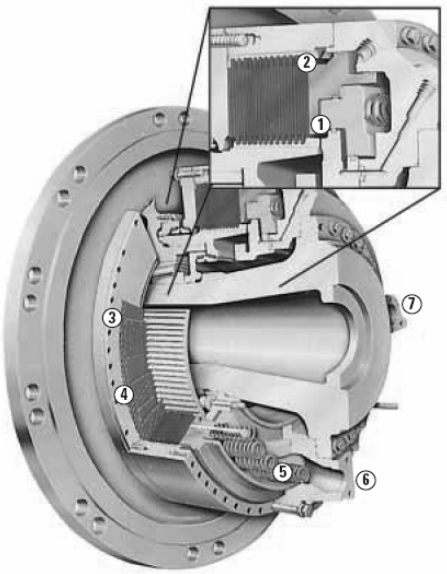
Described is a Regulator free Safety Case tool. It delivers substantiated proof necessary to prequalify for safe use, specific model Haul Trucks based on continued effectiveness of their braking systems. A Finding of proof beyond reasonable doubt is substantiated proof not justified proof. It carries no legally justified weight and has no bearing on the legal obligations of any stakeholder.

It omits Goal Seeking Notation & gives pass/fail to the system design not Probabilistic Risk Analysis or Safety Integrity Levels. There is scope for further work in the precision applied to quantifying safety integrity in the design itself in future Safety Cases. For the present however the case is rested on the current OEM design with any significant gaps seen in the safety integrity of the design catered for by User precautions and modifications in the Specific Conditions of Use (SCU) & Permit Tools developed.

It is a form of Safety Case demonstrating proof of safety in its Finding of Safe/Not Safe subject only to standard of proof, presumptions made, *reason to doubt* and complete and proper use of the Specific Conditions of Use (SCU) Tool provided. In other words Safe is *Zero Harm* and Not Safe is *Harm*. There is no in-between Safe or Harm. The Integrity of "Safe" is Yes✔ or No ✘ and subject to the above provisos.

Wet Brakes

Invented 36 years ago, the Caterpillar® designed Oil Cooled Multi Disc Spring Oil Actuated Brakes are a paramount example of failsafe design, which when maintained correctly, ensure that the machine's braking system is not vulnerable to environmental variables nor susceptible to brake fade or fire.



The take up by other OEMs of this robust wet brake technology has been slow in some instances. This means that Zero Harm outcomes for dry brake technology Haul Trucks may only be as robust as those compensatory measures undertaken by mines & quarries for such dry braked Haul Trucks.

In an age where Zero Harm is now the rule not the exception, failsafe wet brakes can redefine the operating environment by reducing the reliance on "external" backup safety measures such as traffic calmers, safety ramps, impact berms, parking troughs and wheel chocks, as well as allowing for steeper grades.

Continued Brake Effectiveness

A Finding ✔ of Continued Effectiveness in the Safety Case is bounded by its System Description (SD). The SD encompasses the technology in the brake system itself, not human factors or technology influencing tyre/rim or tyre/road friction. The SD covers the specific OEM system and any modifications recommended as part of the Finding.

Protection of people from failure of brake technology to remain effective is sustained by elements of systems engineering, quality, operations & maintenance plans invoked in the chain of supply & use, as Specific Conditions of Use (SCU) of the Safety Case.

Inevitability of Brake Failure

We are entering an age of harmonised model WHS law where one must be able to give reasonable excuse for providing high consequence workplaces. *Embracing the Age Supporting People and Technology* is providing the proof beyond reasonable doubt that critical risk controls are effective with the technology specific in the case of Haul Trucks on steep grades. Proof is demonstrated in a declaration by a mine or quarry of their adherence to a specific operation & maintenance plan called the Specific Conditions of Use (SCU) Tool providing certainty against inevitable risk/harm.

1. *With paltry excuse it is inevitable that Haul truck brakes will fail.*

2. *With ample excuse it is inevitable that Haul truck brakes will never fail.*

Accountability

All manifestations of Safety Cases have to be Facility/System Specific Cases (as defined in a Facility/System Description in the Safety Case Report) and therefore targeted in their assessment and treatment of risk. Safety Cases can not be made for notional standardised/generic forms of technology. Safety Cases also need to be open to end user and worker input as well as input from the OEM & Regulator.

Local importers/suppliers are well positioned in the supply chain to deliver Safety Case Reports for specific haul truck braking systems supplied. A Mine or Quarry finds it is able to make a declaration of proof of Zero Harm by the Finding made in the Safety Case by the importer/supplier.

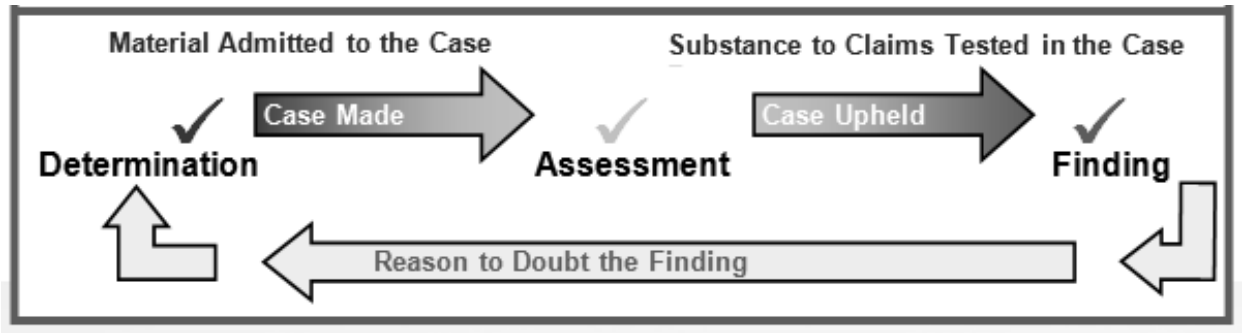
The importer/supplier is in turn able to make the Finding based on the Determination and Assessment in the case by competent & accountable persons commissioned by the importer/supplier on their behalf. (In this supplier's case the persons accountable were employee engineers functionally independent in respect of their roles in the case).

Declarations of Conformity by importer/supplier executives are contained in the Safety Case Report and are an essential part of its accountability.

Feedback Loop

The core value of the Safety Case is in the quality systems and quality information flow between stakeholders demonstrating that proof can be declared. Important information feedback would also include any *reason to doubt* aspects of the Finding of the Safety Case.

Where there is *reason to doubt*, it is expected that those reasons would find their way back to the supplier to be admitted to the case. The more the case is tested by *reasons to doubt*, the more will be the acceptance of its claim of providing a Finding of Zero Harm beyond reasonable doubt.



Framework

There is no Safety Case legislative framework covering the mining & quarrying industries. A non legislative, application specific Safety Case framework is envisaged where Claims made, are given Substance via Argument and Evidence and separately assessed. Claims arise in the 1st place from safety objectives/requirements established in conformity with authoritative and corporate texts.

Material is admitted to the Safety Case in the 1st instance by the importer/supplier. This Material is *outlined* in the Body of the Safety Case Report. *Procedural Matters* are undertaken in the Safety Case by the importers/supplier and the Mine or Quarry cooperating to allow a Mine or Quarry to ultimately self issue a Permit to operate the Haul Truck. The Permit is a declaration of Zero Harm proven as a presumption of continued brake effectiveness ensured in the Safety Case.

In order to construct the framework of this Safety Case, Procedural Matter such as Outline, Claim-Argument-Evidence (CAE), Assessment, Finding & Permit are contained in the following schedule which lists all prerequisites to the declaration of proof under the Specific Conditions of Use from the Safety Case Report.

	Procedural Matter	Purpose	Entity	Nominee here	Procedural Matter Outcome
1	**Determination**	**To Make** the Safety Case	**DA**	Hastings Deering	Determination ✓ of Merit & Admissibility of Material making the Case
2	**Claim**	To submit that safety Objectives are met	**DA**	Hastings Deering	Claim arising from each Objective
3	**Argument & Evidence**	To give *Substance* to Claims arising from Objectives	**DA**	Hastings Deering	Argument and Evidence in a Substantiation Table addressing each Claim
4	**Assessment**	**To Uphold** the Safety Case	**ISA**	Hastings Deering as Self Assessor	*Assessment* ✓ of each item of *Substance* in the Substantiation Table
5	**Finding**	**To Rest** the Safety Case	**Regulator**	Hastings Deering as Self Regulator	Finding ✓ of "Case Rests" from the sum of Determination ✓ and Assessment ✓. *SCU and Permit Tool*s then printed on the date that the Case rests.
6	**Permit**	**To Ensure** complete adherence to ***S**pecial **C**onditions of **U**se*	**Regulator**	This Mine or Quarry as Self Regulator	*Permit Tool* ensuring proof of *Zero Harm*. (Enforced *Permit* transforms "assure" to "ensure")

In this schedule, the last of the Procedural Matter # 6 is nominated as a self regulated *Permit* ensuring Proof of Zero Harm in the Safety Case.
DA – Design Authority ISA – Independent Safety Assessor

The complete Safety Case Report is copyright and purchased as a hard copy book & CD per model. The Safety Case is Haul Truck model specific & covers mines & quarries supported by the local supplier.

Outline

The Outline of the Safety Case displayed below, is constructed so as to encompass all *Material* used to build the case. The Safety Case is then **made** by Determinations (scored ✓/×) as to the Merit & Admissibility of the *Material* outlined.

	Outline			Building the Case
	Material	**Merit & Admissibility**	**Where**	**Determination as to *Material* M&A**
M1	***Specific Conditions of Use***	Essential safety outcomes clearly specified and accessible to Mines and Quarries	HDAL Engineering Services	(✓/×) ✓
M2	***Context***	Properly established for the Safety Case.	Part 6	(✓/×) ✓
M3	***Objectives***	Sufficiently broad to encompass all Claims necessary.	Part 9	(✓/×) ✓
M4	***Safety Criteria***	"Safe" properly defined in the context of "Risk". Risk controlled to "low" as defined in this SCR and mapped to an "acceptable level" under the provisions of the Act.	Annexure 1	(✓/×) ✓
M5	***Technical File***	A S/N specific process & archive enabling Configuration Management, Verification and Validation of Design, and Engineering Change Control.	Part 12	(✓/×) ✓
M6	***Safe Use Information***	Information, instructions & training available to workers to assure they work safely.	Part 12	(✓/×) ✓
M7	***Communication, Consultation, Monitoring & Review Systems***	Resources, systems & process for Vendor/User Information Flow, Feedback, Alert & Change Management of the Technical File.	Part 12	(✓/×) ✓
M8	***Sworn Declarations***	Vendor's Declarations of Conformity sworn to further assure quality & safety are properly resourced.	Annexure 14,15 & 16	(✓/×) ✓
M9	***Claims and their Substance***	Substantiation of each Claim argued and supported by detailed evidence or authoritative reference.	Parts 10, 11 & 12	(✓/×) ✓
M10	***System Description (SD)***	CAE substantiating the rigour of the Technical File of each Cat 793D Braking System at a mine.	Part 10	(✓/×) ✓
M11	***Formal Safety Assessment (FSA)***	CAE substantiating the safety of each Braking System including a register of residual risk.	Part 11	(✓/×) ✓
M12	***Safety Management System (SMS)***	CAE substantiating ongoing support for the Technical File over the system's design life and support of monitoring & review of the SCR.	Part 12	(✓/×) ✓

Establish Context

Safety Cases demonstrate safety objectives achieved in the context of claims of system safety determined by the merit and admissibility of material in the case and assessment of Substance in the claims. These establish facts in the case which remove doubt as to the safety of the system. The Safety Case therefore removes doubt that critical residual risk has been extinguished by its independent and accountable Determination, Assessment and Findings into Claims involving:

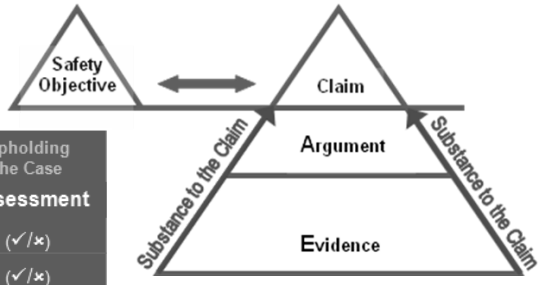
1. Examination of the Technological System….*System Description (SD)*
2. Effectiveness of its treatment of risk.....*Formal Safety Assessment (FSA)*
3. Robustness of the Safety Process……..*Safety Management System (SMS)*

Proof is established in the context of the standard of proof of beyond reasonable doubt and in the context of any premise accepted as presumption in the case.

Substantiation Table

Claims arising from Safety Objectives are individually tested for their substance S1, S2 etc (as Argument and Evidence) in a Substantiation Table which covers the System Description, Formal Safety Assessment, and Safety Management System.

The Safety Case is Made by the Determination of Material admitted to the case, but it is the Assessment of the Substantiation made from Argument and Evidence which Upholds the Case.



	Substantiation Table for Claims 1 to …		Upholding the Case
	Argument	Evidence	Assessment
S1			(✓/×)
S2			(✓/×)
etc			(✓/×)

Specific Conditions of Use Tool (SCU) & Permit Tool

Proof in the Safety Case for continued brake effectiveness and hence Zero Harm is *assured* by complete and proper use by the Safety Management Systems (SMS) of Mines & Quarries, of the Specific Conditions of Use (SCU) Tool. The SCU is offered free as a Safety Case tool to enable this confident declaration.

The SCU lists all essential requirements necessary for the continued effectiveness of the brakes. Core to this are safe down grades and payloads, condition monitoring, testing and examination and pre-failure repair/replacement of system faults before they turn hazardous. SCU1, SCU2 etc are contained in sections on *Testing, Preventative Maintenance, Other Aspects of Operation & Maintenance* and a *Conformity & Harmonisation* section. (In all 21x SCU were identified for Cat 793D braking systems).

Proof in the Safety Case for continued brake effectiveness and hence Zero Harm is *ensured* by a Permit Tool which *enforces* in that SMS, complete and proper use of the SCU Tool prior to haul truck operation as a means to ensure Zero Harm.

Probability of Zero Harm

Risk for a given level of harm is a function of probability. The risk of failure leading to harm is a probability never reaching zero as defined by normal statistics. Uncontrolled events can at best, be normally distributed and unbiased. As shown in this graphic of the population of all outcomes, uselessness lies beyond the Edge of Inefficiency whilst recklessness lies beyond the Edge of Expediency where Zero Harm is under threat.

Normal Probability

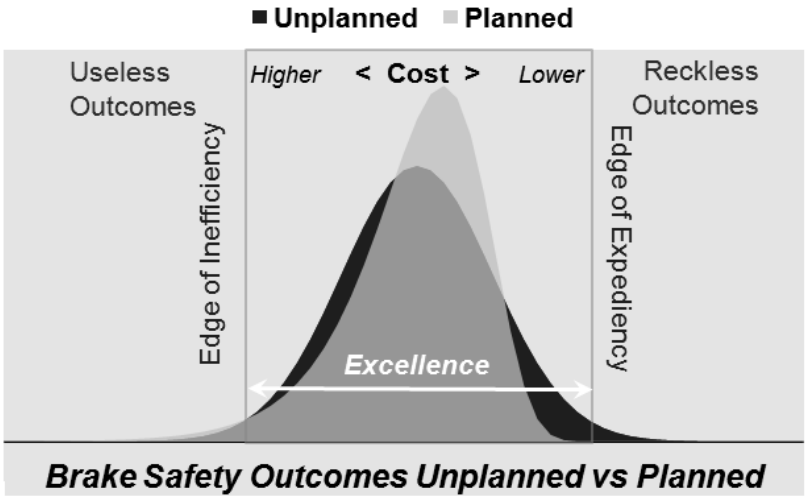
Here, Zero Harm is a probability, a chance and not practically zero. However people's lives cannot be left to chance. Normally distributed outcomes at work are unacceptable for exceptional results like Zero Harm. Working to a proper plan like the Outline and Special Conditions of Use Tool of the Safety Case promotes operating excellence to help stop stakeholders drifting over the Edge of Expediency from excellence into recklessness.

Recklessness finds opportunity with people devoid of proper information, distracted by moments of urgency, battling with inefficiency, lulled into complacency or even simply measuring failure to a justified tolerance instead of fixing the problem in the 1st place… *(The AS2958.1 In Service Brake Test of stopping distance of service brakes gives justified generic acceptance of a 25% failure/loss of stopping distance measured against a rubbery baseline. This generic approach to reliability assumes brake deterioration is progressive, overruling the OEM approach or pre-failure maintenance approach which accounts for sudden 100% failure modes of specific critical components).*

Proof of Zero Harm

Proof over probability lies in relentless quality, check & balance to minimum standards, root cause, limits, processes, tools, skill, replication, improvement and state of the art all working to account for certainty we expect. These are the elements of a Systems Engineering Management Plan (SEMP) in action; the power of a plan over probability to bias outcomes to be very much not "normal". Reliability is built in with quality assurance, redundancy and back up planned outcomes overpowering perfectly "normal" unplanned outcomes.

The following graphic displays the effect of eventual outcomes forced back from the Edge of Expediency rendering harmful outcomes harmless as a result of elements of a SEMP in place in the Safety Case which remove the faults, flaws and errors in systems and systems of work.



The dramatic loss of probability of harm to the right hand tail of the normal distribution of outcomes is reliability achieved in a way analogous to adding layers of defence in Reason's Swiss Cheese Model of safety barriers.

Commitment to Excellence

Every step of every stage in a product's lifecycle is part of a plan for success. Planning for success changes attitudes of probabilistic expectation of critical failure to determined non acceptance of failure…..it is simply not an option…not in the plan.

A Regulator Free Safety Case demonstrates a commitment to excellence transforming Technological Risk from chance and inevitability of failure into certainty and inevitability of success. It is weighed down only by the standard of proof needed to overcome *reasons to doubt* the facts established.

In effect, the Safety Case offers change:

- From dependence on likelihood (chanced outcomes) … to reliance of established fact (certain outcomes).
- From being persuaded by probability... to being convinced by proof.
- From minimising risk that is there…to doubting any risk is there.
- From a focus on possible failure to a focus on certain success.
- From justification from imposed truth (copy/paste) to substantiation through specific fact (established).
- From a hope for Zero Harm to a demonstration of Zero Harm

Reason to Doubt

The Safety Case approach harmonises with the approach taken after failure. After failure, there is no longer a risk because there is no longer probability. There is only consequence. Risk is extinguished by the event and is no more. After a bad outcome, was the risk acceptable, and is the sum total of the stakeholder's excuses enough?

Then, it is doubt not risk that takes meaning; was there *reason to doubt*? Beyond reasonable doubt, were the actions by those with influence over the consequences unreasonable…to what extent did they show disregard for the consequences, disregard for *reasons to doubt* the continued effectiveness and state of risk controls?

Substantiated Excuses

Vendors (Designer, Manufacturer, and Supplier) carry safety obligations defined by consequence, probability and legalise (*acceptable, practicable, reasonable, precautions, proper, properly, diligence, testing, examination, appropriate etc).* There are no Regulations specific to Vendors (including Mines & Quarries who assume Vendor obligations) to justify their actions. They therefore must be prepared to substantiate how they have discharged their obligations in the absence of specific authoritative justification for their action.

Substantiated risk controls targeted at risk of a specific system (as described in the SD of the Safety Case) is the basis of one's excuses for deploying massive Haul Trucks at speed & on grade. Without a specific System Description, the generic excuse offered might be a mistakenly justified, not a substantiated excuse.

Justified Excuses

Justification based on the truth of the matter is different from substantiation based on the fact of the matter. Holding true to copy/paste generic/standardised prescriptive words may harm, particularly taken at face value and without thorough examination of the fundamental specifics in each case.

On Board Wheel Chocks
Mines are required by their corporate rules to fit manually deployed wheel chocks as standard contraptions to all their Haul Trucks because they are wheeled equipment. The truth is workers are expected to use chocks in the field as auxiliary parking brakes to enhance safety. The fact established in the Safety Case is, holding true to wheel chocks reduces safety in some instances and could be dangerous in others…a just cause to dispense with on-board plastic wheel chocks for large Haul Trucks.

Dynamic Performance Testing of Service Brakes
Coal mines in Qld are regulated to make provision for dynamic brake testing in their SMS and record the results for mine workers…no more no less. AS2958.1 In Service Brake Testing has been widely adopted as an accepted truth for dynamically testing Haul Truck brakes.

However examination of the test by the Safety Case establishes the facts. The fact is that the test is neither a true nor a reliable measure of the dynamic performance of the brakes. It fails as a performance test of the true nemesis of dynamic brakes which is the effect on performance of the power and energy absorbed by the brake needed to stop a runaway truck The fact is, holding true to this test reduces safety in some instances and could be dangerous in others…a just cause to reject AS2958.1 In Service Brake Testing in specific cases such as the Caterpillar 793D.

Conclusion

Proof of Zero Harm as a presumption of Continued Brake Effectiveness in a system specific Safety Case is a way of *Embracing the Age* post the Robens Report, *Supporting People and Technology* with substantiated not justified excuse. The reality of this age is one cannot even think of brake failure as an option. The Safety Case must suffice for stakeholders to acquire belief of a specific part of a Zero Harm Target. The case is Made✓, Upheld✓, and Rested ✓ . Its Finding is substantiated by established fact, and provides ample excuse to use the Haul Truck.

If successfully challenged by *reasons to doubt*, more substance is simply admitted to the case to again establish its Finding against its standard of proof. Feedback into the Safety Case is vital for the performance of such closed loop control in this proven plan for Zero Harm.

The Safety Case gives workers (facing consequence), Benefits of Proof of Zero Harm. In return, workers give the enterprise, the supply chain & the community (facing no consequence), Benefit$ of Doubt of Zero Harm.

References

Document No	**Title** and/or **Contents**
AS2958.1 - 1995	Australian Standard, Earth-moving machinery – Safety Part 1: Wheeled machines - Brakes
ISO 3450	International Standard, Earth-moving machinery – Braking systems of rubber-tyred machines – Systems and performance requirements and test procedures.
Queensland Coal Mining Safety and Health Act 1999	Sections 37, 38 and 48
Queensland Coal Mining Safety and Health Regulation 2001	Part 10 Plant, Division 1 Fixed and mobile Plant, Section 66 – Braking Systems
Minerals industry Safety & Health Centre (MISHC) October 2001	Development of a Safety Case Methodology for the Minerals Industry - a Discussion Paper - Tilman Rasche
Safe Work Australia	Model Work Health and Safety Bill 23/6/2011
Hastings Deering Safety Case Report SCR_434E_001 Grp_ Eng Database EJ4579	Caterpillar 434E Safety Case Report
Hastings Deering Safety Case Report SCR_002_R00 Grp_ Eng Database EJ5752	Caterpillar 793D Braking System - System Specific Safety Case Report Proof of Continued Brake Effectiveness