SCTA: Killing 2 birds with 1 stone

Jonathan Parsons, Process Control & Functional Safety Manager Engineering Refinish UK, Stowmarket, Suffolk, United Kingdom IP14 2AD

Clive de Salis, Principal Process safety Engineer, DEKRA, Phi House, Southampton Science Park, Southampton, Hampshire, United Kingdom SO16 7NS

Abstract:

SCTA is Safety Critical Task Analysis, but what is a Safety Critical Task? ("SCT"). How do we decide what is an SCT, and how do we have a consistent method for doing so? Many companies struggle with how to decide what tasks are Safety Critical Tasks.

Once we have a consistent methodology for deciding what are SCT we often also find that some of the components of the "tasks in the safety process" are automatic and do not involve operators or human beings, but we then have the questions of tests that prove the maintenance was good and the SCT (safety critical tasks) are working properly.

We can also find that some tasks occur in more than one SCT. At this point HAZOP studies and conventional systems often do not spot everything.

At the same time we have known examples of where more than one safety critical element was being maintained at the same time, whilst the plant was safely down to allow such maintenance, and yet when each item of work was finished then one permit to work was returned as "finished" and nobody noticed that there was another permit to work, still out as unfinished and so the process was restarted with the safety system not working. This is particularly true when a SCT is actually part of more than one system.

One of the worst ever accidents showing this was the **Piper Alpha Disaster** so what lessons have we learnt?

What if a system could be used to both help operators be aware of what permits were out covering more than one SCT, and a system that gave a sensible method for revealing everything that could be a SCT and in need of a SCTA? That would be "killing more than two birds with one stone" to use the English phrase.

This paper looks at possible systems to identify what needs SCTA and help operators and maintenance staff be aware of what is unavailable when they cover multiple tasks.

Keywords:

Cyber, IEC61511, IEC61508, defence in depth, diversity, independent barriers.

2. Safety Critical Task Analysis (SCTA)

There are several subjects that we need to introduce in order to make sense of what will be discussed but let us begin with a subject that might seem unimportant but is actually the most important subject of all. In "Safety Critical Task Analysis" we often emphasize in accidents the human error and just how devastating that can be.

Let us begin with a reality check: Operators, maintenance staff and others do NOT want accidents to happen and will go to very, very great extents to prevent any accident from occurring and to keep people safe. It is true that operators and maintenance staff are amongst the most caring, careful and reliable people there are. They are also human beings and are more aware than many that they could simply make a mistake and just how devastating a mistake could be, but it is nothing more than a mistake.

Ever since my early days of safety engineering I (Clive de Salis) was aware of how often operators were blamed, when, in reality the cause of such errors was the incomplete information presented and the blame being wrongly pointed away from the design, which was often the source of the error.

2.2 How to change our mindset

Some time ago the HSE published their research on the source of accidents in a book: "Out of Control" "HSE Books 01787 881165".

This book found that:

14.7%	were connected to operator error, but ….
44.1%	were due to design mistakes, plus
14.7%	were errors in design implementation, and
5.9%	were errors in commissioning or installation and a further ….
20.7%	were errors in changes made after commissioning.

In other words, more than 60% of failures are built into a system before it is even taken into service, i.e. before operations and maintenance ever got involved. Therefore, many errors can be traced back to the process plant designers and any operators and maintenance engineers only have a small part of blame, if at all.

Even today, there are designers ready to falsely, and incorrectly, blame the operators.

So, operators and maintenance staff are doing everything they possible can to avoid any accident, irrespective of the size of the accident. So instead of blaming, let us try to help them. For that reason, the methodology used to record what is happening is usable by everyone, the software is NOT proprietary and specialised but a simple spreadsheet.

Since the operators and maintenance staff will do everything that they possibly can to avoid accidents then we need to try to do more to tell the operators what is actually going on and the tools we provide should focus on helping them.

2.3 Line of sight

It is the fact that the software used is NOT proprietary and that it introduced a benefit we did not expect to see. Operators and maintenance staff are (or should be) fully aware, that they are not experts at everything, they also realise that people make mistakes, even if they have completed the activity many times.

Permit issuers often feel pressure to sign permits, whilst they know that they are not experts on all of the activities going on. After demonstrating the usefulness of the barrier diagrams, the operators gained more confidents in the safeguards all around them. This makes the permit-to-work a shared activity in which the applicant shows the customer what they propose to take out of service for maintenance, repair, test or similar activities.

It is easier then, for the operator and maintenance staff to look along the line where the item is disabled and indicate that that entire safety loop is not functioning, rather than just the single item.

It is true that the operators and maintenance staff have method statements, but we must realise that method statements are not always as clear as they could be, and the more we can help everyone get things right, the better. Operators were also encouraging us from their willingness to discuss and to offer ideas, showing they were completely willing to participate.

It is also vital to identify, with as much consistency as possible, what are the safety Critical Tasks (“SCT”). If we fail to do so, then we are in danger of claiming that everything is a safety critical task and still miss some tasks completely. It is this aspect that causes significant trouble in many companies. You know the importance of finding, and analysing, all the SCT but many companies do not have any established and consistent way of identifying SCT.

As we go through, and talk about lessons from our own experience, we know that a lot of health and safety concepts are founded upon the approach to work of asking “what else can be done?” and “why aren’t we doing it?”. It would be nice to say that everything we could do solves the problem(s) completely, but, most times, the answer to the question “what else can we do?” are ideas that make the unwanted event less likely rather than solving it totally. It is often more mitigation than a complete barrier.

This is the case for the lessons we have learned from the Piper Alpha disaster, because you will be very pleased to know that we have nothing as bad as the Piper Alpha Disaster at all, but that is never any excuse for choosing not to learn anything from such incidents. The worst process plant accident that happened in British history (the Piper Alpha disaster), happened because TWO permits to work were out at the same time for the same part of the process being maintained. ONE permit was returned complete, and the unit was then restarted without anyone realising, or saying, that the second permit had not yet been returned as complete, and so the unit was not actually ready. That simple mistake could happen in most process plants causing small accidents and huge accidents alike.

2.4 A Picture says a thousand words

Lists of safeguards and barriers in a HAZOP study are the safety measures that are “known knowns”. The Barriers diagram below helps us SEE the barriers and safeguards and put what we know into best use for our own safety.

We need maintenance to happen and so the simple Barrier diagram (sometimes-called a Bow-tie style diagram) showing the barriers helps us see where each safety measure is in the overall risk reduction system and, therefore, allows us to note down each one that is out for maintenance.

The COMAH report defines the Control of Major Accident Hazards. When it comes to identifying “Safety Critical” we cannot say that any of the equipment that prevents a major accident hazard is not safety critical. Quite the opposite: It is safety critical. Therefore, when we have a diagram of the incidents that lead to a major accident hazard, and those barriers and safeguards that prevent or mitigate them, then all of those barriers and safeguards are safety critical items.

Take the simple example of a barrier diagram shown below here:

This is the simple case of mistaken overfill of a vessel. In this case the unwanted overfill is inside a building that contains a group of operators working.

There are high level alarms and overfill protection as expected. Even if the system does overfill then ATEX certified equipment is used to minimise the risk of ignition (notice that ATEX does not absolutely prevent ignition occurring but, rather, significantly reduces the chance of ignition).

2.5 The Event

ALL of this need's maintenance and proof-testing, and not just operation.

The diagram shows that there are:

- Three different causes of overfill (shown in blue, on the left-hand side).
- Three lines going across the diagram (each line relevant to their cause).
- The Unwanted Event (blue box in the center), an Overfill spilling liquid and creating a pool of flammable material (but, at this point it has not ignited).

So, first the spillage occurs, before the pool ignites for the Major Accident Hazard.

What this means is that all of the pink boxes on the diagram are the scope of the Safety Critical Task that can then be studied as SCTA. It is true that several of those pink boxes do not involve human factors, but it is a lot better to have studied it and found that SCTA doesn't apply than to simply ignore it.

What has happened is that, if the diagram is correct, then all of the pink boxes are the scope of SCTA study.

The three lines going across the diagram from left to right allow you to follow the initiating event through to the Major Accident Hazard that could then be mitigated so that the final event is not as bad as it would have been without the mitigating factors

Operations have also asked us to consider if text describing alternate measures could be activated by those authorising a permit to work to reduce risks. In principle it sounds useful and consideration of the potential details are now needed.

2.6 Barrier diagram

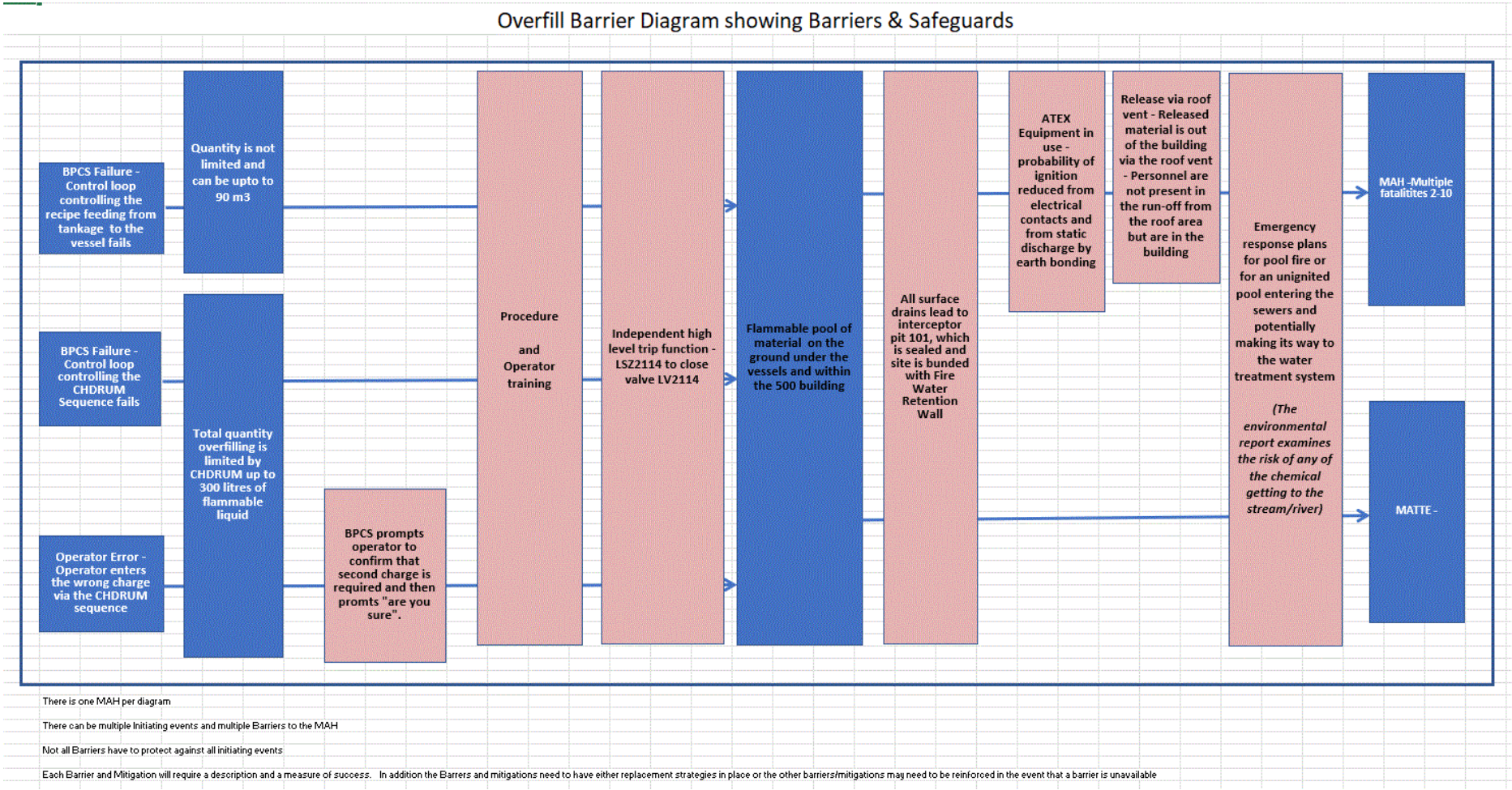

Figure 1: A typical barrier diagram with three error sources and two ultimate outcomes

2.7 Explanation of the diagram

Donald Rumsfeld, U.S. Government Secretary of Defense, once said:

There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know.

There are even things we don't know that we know!

Here we do well established safety systems to keep us all safe. This is about acknowledging what we know and using it better all of the time.

We already do good quality HAZOP studies that include everyone involved with process plant. The HAZOP studies allow us to know, and write down all the safeguards and barriers that protect us. The well-proven HAZOP study process does not write down whether a safeguard is mitigation of the unwanted event, or prevention of the same unwanted event.

The worst process plant accident that happened in British history (the Piper Alpha disaster), happened because TWO permits to work were out at the same time for a part of the process being maintained. ONE permit was returned complete, and the unit was then restarted without anyone realising or saying that the second permit had not yet been returned as complete, and so the unit was not ready.

Lists of safeguards and barriers in a HAZOP study are the safety measures that are "known knowns". The Barriers diagram below helps us SEE the barriers and safeguards and put what we know into best use for our own safety.

We need maintenance to happen and so the simple Bow-tie style diagram showing the barriers helps see where each safety measure is in the overall risk reduction system and allow us to note down each one that is out for maintenance.

A simple barrier diagram, has an important use:

On a Bow-tie diagram we can see all the safeguards and see which risks they act against by following the lines across the diagram

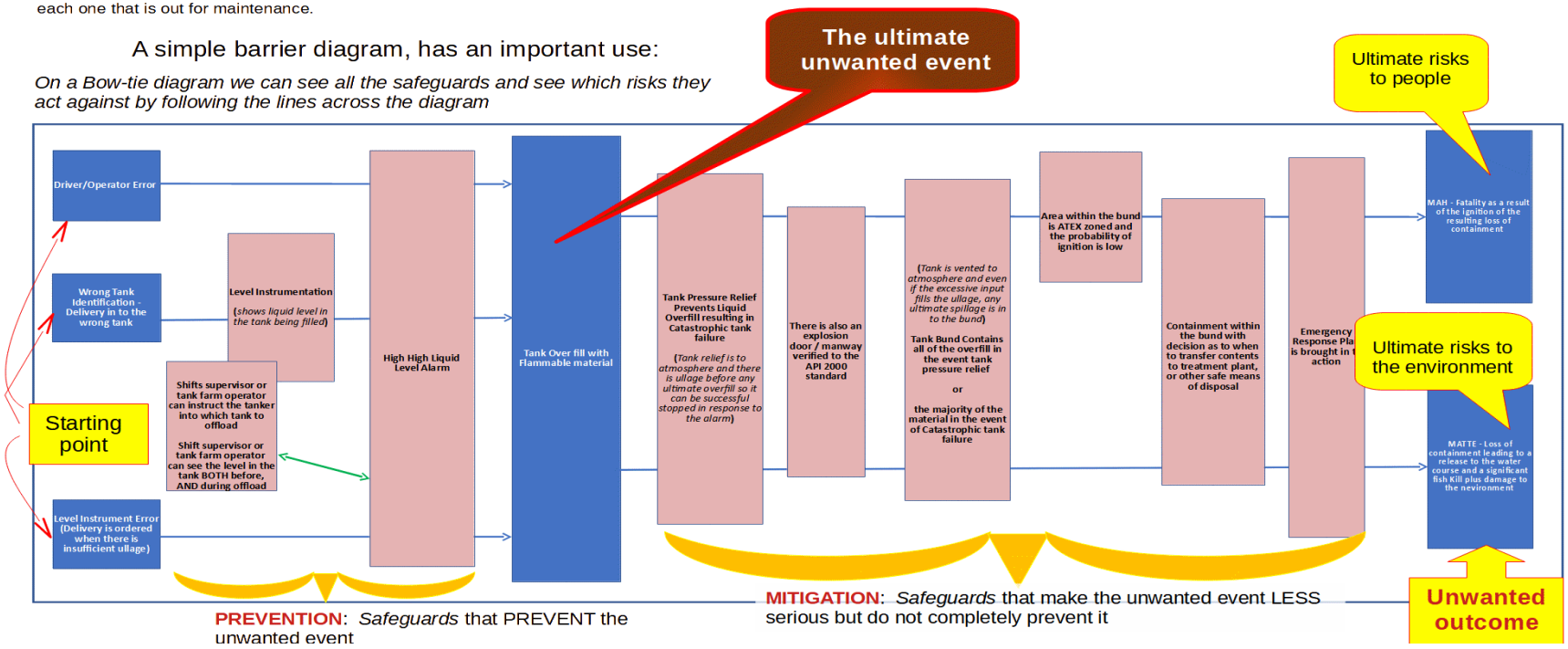

Figure 2: Explanatory text for the operators and maintenance staff, describing barrier diagrams

3. The Mechanics

In practice, the operators and maintenance staff have (2) two copies of each barrier diagram.

1. This first copy is in PDF format that cannot be altered.

2. The second copy is the spreadsheet format upon which the operators and maintenance staff can freely make notes on what is out for maintenance.

Since such notes are located on the item that is out for maintenance, or simply faulty and unavailable, it means that such a note appears directly on the left-to-right line crossing the diagram showing the complete safety system against that particular initiating event, and showing that it is not available FOR USE.

3. Once the work is complete, and the system restored, then the pdf copy of the diagram confirms how to restore the spreadsheet version of the diagram.

Every time a barrier diagram is complete then you also now have the scope of the SCTA (Safety Critical Task Analysis) for that barrier diagram.

You can now do SCTA for each critical task, and you can also label each item of equipment on the barrier diagram as being safety critical.

To be clear, a process plant will have more than one barrier diagram.

4. Summary

By using non-proprietary software, the operations and maintenance teams can use them openly. In doing so, they can more easily involve those applying for a permit to work in the process and consequences of such a permit being granted. The structure of such barrier diagrams can show the scope of everything involved in SCTA (Safety Critical Task Analysis).

The barrier diagram informs the operations and maintenance teams of all the safeguards that appeared in HAZOP studies instead of relying on the operations representative at the HAZOP to inform everybody else whilst, too often, the HAZOP report sits on a shelf unread.

5. The Authors

Jonathan Parson and Clive de Salis

April 2022

JONATHAN PARSONS

JONATHAN PARSONS

Jonathan Parsons is the lead Process Controls Engineer for PPG, originally in the UK and now for other sites.

Jonathan started his career as an electrical engineer before moving to PPG Stowmarket. At PPG, Jonathan worked as a maintenance engineer and managed the design and implementation of the trips and alarms/proof tests for new and legacy equipment. Jonathan has completed the NEBOSH general certificate, Environmental and Fire safety management. Combining his knowledge of maintenance and engineering techniques with his health and safety passion.

“Since working with Clive and Dekra we have managed to identify the SCT’s for our Major accident Hazards (MAH). We are developing a robust set of documentation that can be embraced by Permit writer, Mangers, Engineers and Operators. This will provide the visibility we require to truly see the barriers and safeguards in place. The statics on MAH are there, that proves you are more likely to have an incident during maintenance activities. This concept visualises the critical information and allows clearer visibility of the barriers that are in place, thus increasing the likelihood of us all making better and more informed decisions during maintenance activities.

Bad things happen with good intentions”

CLIVE DE SALIS

Clive de Salis is the Vice Chair of the I.Chem.E’s Safety & Loss Prevention group in the UK as well as being an International Professional Process safety Engineer. Clive is also the author of the I.Chem.E’s book on SIL systems. That book is directly referenced in IEC61511 now.

Clive de Salis is Principal Process Safety Specialist and consultant in process design safety, critical instrumentation and hazards. He writes both the IEC62443 series of standards on Cyber security and the IEC61508 series which includes IEC61511 on SIL rated systems. His main areas of expertise are process risk assessment, with extensive experience in the design and installation of safety systems and determination of safety integrity levels. His recent experience includes expert witness selected by barristers and solicitors for dust explosions.

Phone number: +44 7502 414564

Email address: clive.desalis@dekra.com