Introduction to Why-Because Analysis

Dipl.-Inform. Jan Sanders
Computer Networks and Distributed Systems Group
Technical Faculty, Bielefeld University
mail: jsanders@TechFak.Uni-Bielefeld.DE
web: www.rvs.uni-bielefeld.de

in Association with Causalis Limited
mail: sanders@causalis.com
web: www.causalis.com

February 1, 2012

Contents

1 Accidents and Causality

1.1 Fukushima: Three Disasters in One Day

At the time of writing the last Big Disaster happened on March 11th 2011 in Fukushima Prefecture, Japan. The first disaster was the so called Tohoku Earthquake, which occurred approximately at a quarter to three, local time. The epicenter of the quake was approximately 70 km off the Oshika Peninsula the coast with a magnitude of 9.0. A magnitude 9.0 quake is an immensely powerful earthquake, indeed it was one of the most powerful earthquakes ever recorded. The close proximity to the north eastern part of the Japanese main island of Honshu and the huge amount of power meant serious destruction.

Then there was a second disaster following immediately. Shortly after the earthquake a tsunami struck the east coast of northern Honshu. The tsunami was a direct result of the moving sea bed. The tsunami traveled as far as 10 km inland and wiped out entire villages.

After the tsunami retreated a third disaster was already becoming apparent. The Fukushima Dai-Ichi nuclear power plant was first struck by the Tohoku quake, then by the tsunami and this caused a runaway nuclear reaction. A nuclear disaster followed, which is still not under control as of December, 1st 2011.

It is unfortunate enough to be the victim of an earthquake, a tsunami or a runaway nuclear reaction. But it was not't just bad luck, since the three disasters did not occur independent of each other. The three disasters were linked causally. On causing another. The earthquake caused the tsunami and damaged the Fukushima Dai-Ichi nuclear plant. The tsunami further damaged the nuclear plant and left it in a state that was not longer controllable.

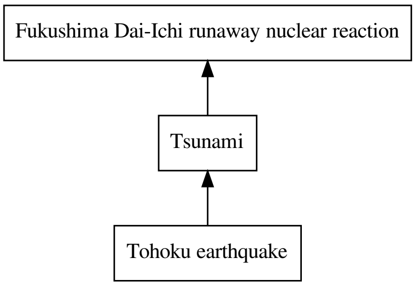

Figure 1: Simple causation from Tohoku earthquake to the Fukushima Dai-Ichi nuclear disaster

Two of the disasters are naturally occurring disasters. The nuclear crisis could only happen because there was a man-made system with the potential of an uncontrollable radioactive reaction. This potential was realized, both by the existence of the plant and the preceding natural disasters.

From the point of view of accident analysis only the man-made system is within the ability of humans to control and influence. An accident analysis will focus on the nuclear accident and try to find out what went wrong. That does not mean that analyzing the quake and tsunami does not have benefits. But since humans can only change the design of the nuclear plant, and not of tectonic plates or the sea, the two natural disasters are only of interest insofar that they concern the safe operation of the plant.

1.2 Concepts of Accident Analysis

The Fukushima story illustrates some basic and important concepts of accident analysis. Some occurrences are accidents, others are not. How do we distinguish them? Another important concept is causality. Everybody has an intuitive grasp on the concept of causality, but for accident analysis it is very helpful to have a formal understanding of the concept. As with accidents, causality in this scope will be used as a technical term, to be distinguished from its day to day use.

For the scope of this book the term Accident, and some other related terms, will have special meaning. They are technical terms, which will receive special attention in this book.

1.2.1 Technical Terms

Technical terms will be introduced throughout this book. Some are part of jargon and are widely used in safety literature. Not all literature uses the exact same definitions as I do, but they will be sufficiently similar to allow the understanding of other texts on the topic. Jargon is used to express very specific things that day-to-day language cannot easily.[1] It is helpful to learn the jargon presented here.

1.2.2 Technical Terms: Accident and Incident

There are many definitions out there that define the term Accident. One good example is the definition used by the International Civil Aviation Organization ICAO.

Accident - ICAO *"An occurrence associated with the operation of an aircraft which takes place between the time any person boards the aircraft with the intention of flight until such time as all such persons have disembarked, in which (a) a person is fatally or seriously injured [...] or (b) the aircraft sustains damage or structural failure [...] or (c) the aircraft is missing or is completely inaccessible."*

The definition concerns itself with aircraft accidents and does not aim to give a general definition of what an Accident is. The scope is even further narrowed e.g. by the "between the time" phrase. The ICAO is interested in Accidents of a specific type, so it is reasonable to exclude from the definition all occurrences e.g. not "associated with the operation of an aircraft". On a side note, "associated" is not well defined, in a formal way, but for our purposes it should

[1] Some people feel that the purpose of jargon is to distinguish between insiders and outsiders. That may well be the case, but nevertheless the benefits of having a specific technical vocabulary outweigh the costs by far.

be fairly obvious what the meaning of the statement is. ICAO is not interested in occurrences that involve injury to persons who dismantle a decommissioned aircraft. The purpose of ICAO is to set international rules for civil aviation. This includes aviation accident investigation. Since decommissioned aircraft are no longer operated in a civil aviation environment they can be excluded from the scope of interest. Note also that there has to be a certain level of loss. Light injury to a person associated with the operation of an aircraft does not constitute an Accident. One reason for this is that this would do more harm that good to investigate all light injuries. The amount of work that would be necessary can better be invested in other activities that will improve aviation safety more effectively. A second reason is, that there is probably not much to learn from most light injury occurrences. Learning from Accidents is the major reason to conduct Accident analysis in the first place. But I will leave it at that for the moment.

In the introduction I also differed between types of occurrences. I simply wrote that neither the Tohoku quake, nor the tsunami were accidents. The runaway nuclear reaction however is an Accident, I wrote. The reason to exclude the natural disasters from the list of occurrences that may be Accidents is that natural disasters differ in one very important way from nuclear power plants. Power plants are man-made, but natural disasters are not.[2] If a nuclear Accident is analyzed and understood changes can be made to other similar plants to prevent future Accidents. But we cannot change the design of tectonic plates of fluid body physics, which does not mean that we should not try to understand them. Both natural disasters were causes for the nuclear Accident and understanding their behavior can also lead to insights to improve the design of nuclear plants.

Our own working definition of Accident will now be:

Accident *An Accident is an occurrence that results in significant loss an is within our area of interest.*

This is a bit fuzzy for a good formal definition, but sufficient for our purposes. The definition allows us to state the amount of loss and our area of interest outside the definition of Accidents.

A related concept is Incident, which we will define analogous to Accident.

Incident *An Incident is an unwanted occurrence within our area of interest.*

With this definition all Accidents are also Incidents, but not the other way round. Intuitively we could say that Incidents are near-Accidents. Something went wrong so that an analysis is warranted, but no significant amount of loss resulted from the Incident.

Let's have a look at ICAO's definition of Incident.

Incident - ICAO *"An occurrence, other than an accident, associated with the operation of an aircraft which affects or could affect the safety of operation."*

[2] I will not discuss the amount of man-madeness in natural disasters that may or may not result from global warming. While that may be true, it is a bit beside the point here.

This definition is defined relative to the definition of Accident, but here Accidents are not Incidents. They have been explicitly excluded. Both ways are OK of course if they fit their purpose.

I chose to define Accidents to be a subset of Incidents so that I would not have to write "Accidents and Incidents" throughout this book. I prefer to just write "Incidents" where I mean both, which will be most of the time.

1.2.3 Technical Terms: Causality

The Tohoku earthquake caused the tsunami and both contributed to the nuclear crisis. Did both cause the crisis? Intuitively we would say, Yes they did. But when I rephrase the above statement to "The Tohoku earthquake caused the tsunami and both triggered the nuclear crisis" then the phrasing implies that there have been other causes to the nuclear crisis.

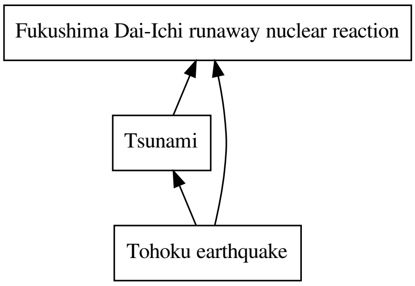

Figure 2: The earthquake and the tsunami both contributed to the nuclear disaster.

One occurrence causing one other occurrence is a special case. Some things need a large set of causes before they can happen. Consider the number of safety systems in your car: anti lock brakes, anti skid, airbags or the crush zone to name a few. In order for a frontal crash to be fatal a number of these must either be ineffective or inoperative. Each safety system is supposed to increase the number of causes necessary for a fatal frontal crash by one. Commonly speeding, fatigue or DUI would count as "the cause" of a fatal frontal crash.

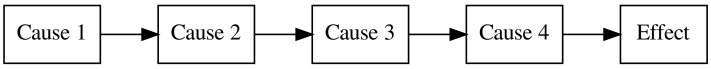

Figure 3: Causal chains are too simplistic to explain complex causal relationships.

The latter point of view is sometimes called a "causal chain", which suggests one-to-one causal relations between causes and effects. For simple Incidents that may be sufficiently explanatory. But complex systems tend to have complex cause and effect relations that require a more rigorous approach to causality.

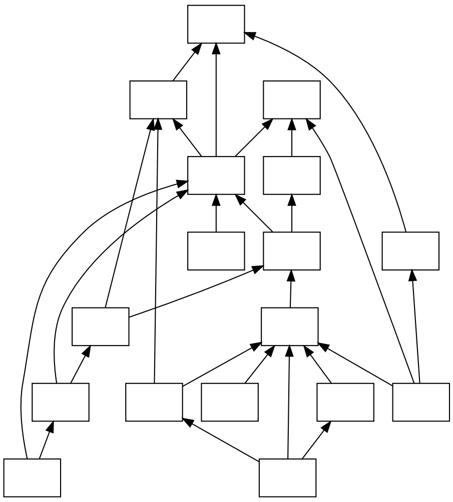

Figure 4: Causal relationships can be quite complex. This does not bear any resemblance to a chain.

WBA is built upon one such rigorous notion of causality, which are called Counterfactuals. There are other notions of causality, but for the purpose of learning WBA I will only consider Counterfactuals here.

The word Counterfactual seems to suggest something along the lines "Counter to Fact", which is correct. David Hume argued, that two occurrences are causally related as cause and effect if they pass the following test:

Counterfactual Test *C is a cause for E if, and only if, had C not happened E could not have happened*[3].

In other words, contrary to the fact that C and E both happened, we assume that C would not have happened. In that case can E happen? If the answer is yes, then C is necessary causal factor for E. If the answer is no, then C is not necessary for E to happen, E would have happened anyway.

In WBA speak we say:

Necessary Causal Factor (NFC) *Cause C is a Necessary Causal Factor for effect E if C passes the Counterfactual Test for E. C is a NFC for E.*

Please note that even though C is a Counterfactual for E, the Counterfactual Test does not answer whether C is the only cause for E. C alone may not be sufficient, other causes may be needed so that E occurs.

[3] All else being equal

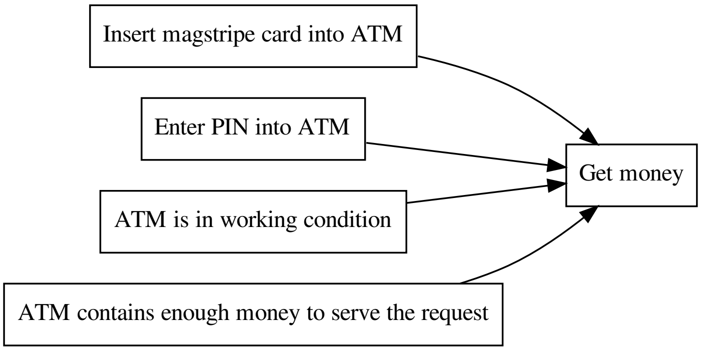
Insert magstripe card into ATM
Enter PIN into ATM
ATM is in working condition
ATM contains enough money to serve the request
Get money

Figure 5: Necessary and sufficient causes to get money from an ATM

An example: You want to withdraw money from your bank account. This can most easily be done at an ATM[4]. You insert a mag-stripe card into the card slot of the ATM and then enter your PIN[5] and the ATM will dispense the amount you requested. Would you receive the money if you had inserted the card, but would not have entered the PIN? No, the PIN is necessary. Would you receive the money if you had entered the PIN, but would not have inserted the card? No, the card is also necessary. Card and PIN are necessary, but none is sufficient on its own.

I have already presented the Counterfactual Test, and there is a complementary test for sufficiency:

Causal Sufficiency Test *Causes C1, C2, ... and Cn are causally sufficient for effect E to happen if, and only if, E inevitably happens when C1, C2, ... and C3 happen.*

With both tests, the Counterfactual Test and the Causal Sufficiency Test, it is possible to determine if a suspected cause-effect relation really is one. And if the causation of an effect can be completely determined.

1.3 Check your Understanding

Exercise 1 On 14th of April 1912, the RMS Titanic collided with an iceberg. Even though the ship was thought to be unsinkable, the iceberg inflicted an unrecoverable amount of damage. Among the factors that contributed to the loss of 1517 people were

- Excessive speed. The captain of the ship aimed to make the fastest Atlantic crossing, winning the blue ribbon.

[4] Automated Teller Machine

[5] Personal Identification Number

- The collision occurred at night.
- RMS Titanic did not have sufficient life boat capacity for crew and passengers.
- The ship was thought to be unsinkable.
- RMS Titanic was unable to evade the iceberg after it was spotted by the lookout.

This is by far not a complete account of the fate of RMS Titanic.

1. What do you consider to be the Accident? Try to be as precise as possible to define the Accident event.
2. Which of the five given factors are causally related according to the Counterfactual Test?
3. How many of the five factors are NCFs of the Accident?
4. Do the Accident and its NCFs pass the Causal Sufficiency Test? If not, what is missing?

Exercise 2 On 26th of April 1986 a nuclear disaster occurred at the power plant at Chernobyl, Ukraine (former USSR). Which of the following factors would you name the Accident? Why?

- Point beyond which the nuclear reaction was controllable.
- Explosion of the rector containment building.
- Release of radioactive material into the environment.

Exercise 3 You get back to your car to discover that you have been fined for parking in a no-parking zone. At the time you parked your car you were not aware of the no-parking zone.

- Give all NCFs for begin fined.
- Which of the NCFs change had you been deliberately parking in a no-parking zone.

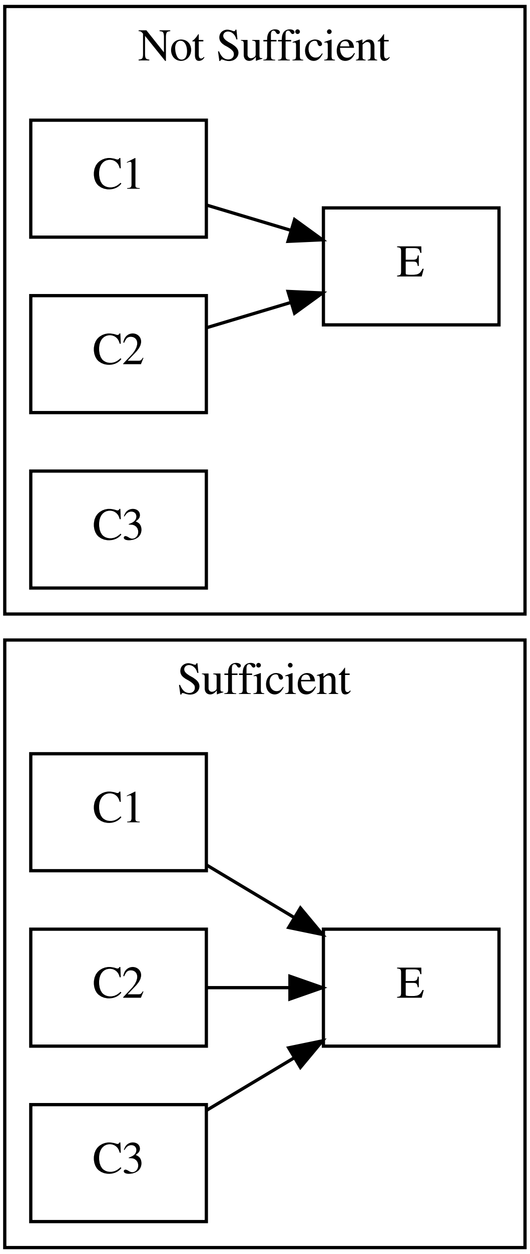

Figure 6: Sufficient and Insufficient Set of Causes for E

2 Counterfactual Reasoning

2.1 Seeing it Coming

On July 1st, 2002 two aircraft collided mid-air over Lake Constance in southern Germany. The Accident happened despite the fact that both aircraft were equipped with collision avoidance systems. But before a collision avoidance system alerts the crew a ground based system alerts the air traffic controller. The ground based system, called Short Term Collision Avoidance STCA, sounds an alarm if it detects a possible mid-air collision within approximately two minutes. The air traffic controller then has to instruct the aircraft to keep them sufficiently separated.

The airborne system, the Traffic Collision Avoidance System TCAS only warns the crew a little under 50 seconds ahead. In case of a potential mid-air collision the air traffic controller usually has advance warning and the airborne TCAS is only needed if the air traffic controller cannot keep the aircraft separated.

The air traffic controller at Zurich, Switzerland, did not have the STCA system at his disposal due to maintenance. The radar the air traffic controller was using was running in a degraded mode, but was deemed sufficient for the low density night time traffic, that was to be expected. Another system was down due to maintenance on the same night: One of the telephone systems used to contact other air traffic controllers in other air control centers.

Air control center Zurich was not the only air control centers whose radar covered the flight path of the two aircraft that were about to collide. The so called upper area control center at Karlsruhe, Germany, was monitoring the situation, but was not responsible for air traffic control in that area. But the STCA in Karlsruhe was fully operational and a controller tried to phone Zurich three times immediately before the collision. Unfortunately the air traffic controller at Zurich was busy directing an air craft to the airport Friedrichshafen, Germany. The Zurich controller was not continuously monitoring the situation over Lake Constance. Please note that the situation was a little bit more complex that outlined here, but this simplified version is better suited for learning the concepts of Counterfactual Reasoning. For the same reason lets focus on the inability of Karlsruhe to reach Zurich by phone. Please excuse the rather cumbersome statements below, but I will try and keep the form of the Counterfactual Test intact.

- Could the mid-air collision have happened, had the air traffic controller at Zurich been monitoring the situation?
- Could the the air traffic controller at Zurich not have been monitoring the situation, had the air traffic controller at Karlsruhe been able to reach him by phone?
- Could the air traffic controller at Karlsruhe have reached Zurich by phone, had the phone system not been offline for maintenance?

If you read the three Counterfactual Tests another question suggests itself: *Could the mid-air collision have happened, had the phone system not been offline for maintenance?*

2.2 Counterfactual Conclusion

Intuitively we would answer the last question in the mid-air collision story with No, if we would answer the three preceding three Counterfactual Tests with No. Please note that I have refrained from calling the last question a Counterfactual Test. It is related, but not the same. But just to make sure, the right answer to the question is No, just as common sense would suggest. The factors we used in the three Counterfactual Test in our simplified account of the Lake Constance mid-air collision are

- **A** - mid-air collision
- **B** - the air traffic controller at Zurich is not monitoring the situation over Lake Constance
- **C** - the air traffic controller at Karlsruhe is not able to reach Zurich by phone
- **D** - part of the phone system at Zurich is offline for maintenance

As the three Counterfactual Tests showed D is a NFC[6] for C. C is a NFC for B. B is a NFC for A.

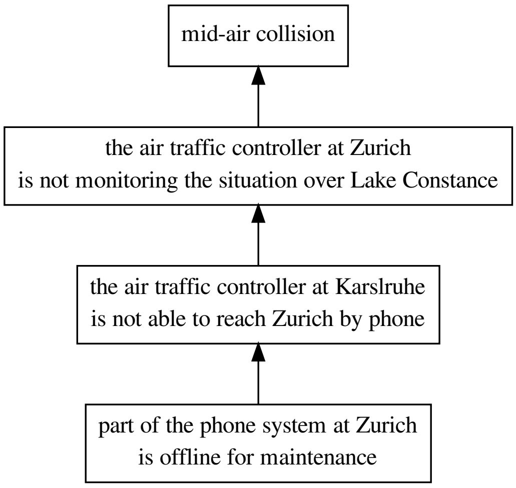
mid-air collision
the air traffic controller at Zurich is not monitoring the situation over Lake Constance
the air traffic controller at Karlsruhe is not able to reach Zurich by phone
part of the phone system at Zurich is offline for maintenance

Figure 7: Simplistic causation of the Lake Constance Mid Air. Note, that this graph does not fulfill the Causal Sufficiency Test.

Is D a NFC for A? No. If that would be that case there would be no need for B and C. But that does not mean, that this is a general statement. In other cases, which have the same form, D could well be a NFC for A. If D was a NFC for A we would not feel the need to explain A, the Accident, using B or

[6] Remember: Necessary Causal Factor

C. This is an important criterion. In a later section I will show the differences between analyzes that differ in their level of detail. It may well be possible to omit detail and suddenly two factors are NCFs, because intermittent factors fall away. For the moment the important thing is to understand, that the phone system's maintenance is a cause for the mid-air collision, but not an NFC. There is however another word that we will use for this causal relationship.

Technical Term:Counterfactual Conclusion *If two factors F1 and F2 are causally linked by NCFs N1, .., Nn, so that F1 is an NFC for Nn, ... N2 is an NFC for N1 and F2 is a NFC for N1, the Counterfactual Conclusion is that F2 could not have happened if F1 had not happened.*

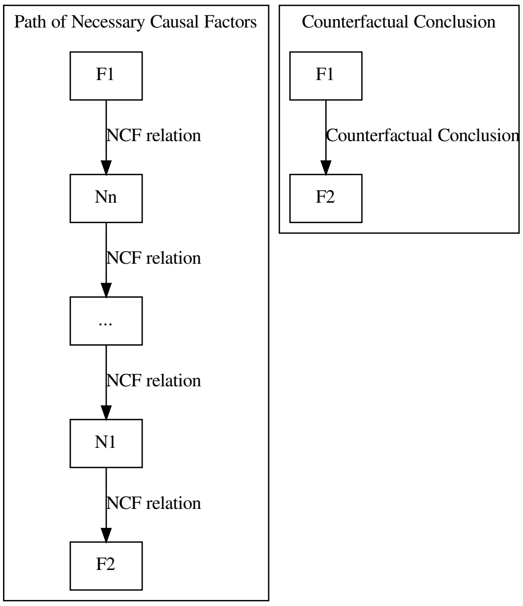
Path of Necessary Causal Factors
F1
NCF relation
Nn
NCF relation
...
NCF relation
N1
NCF relation
F2
Counterfactual Conclusion
F1
Counterfactual Conclusion
F2

Figure 8: Counterfactual conclusion: F1 and F2 are not direcly related as Necesary Causal Factors, but the Counterfactual Conclusion makes them causally related.

To make things a little simpler,

Technical Term: Cause *If F1 and F2 are either related by the Counterfactual Test or are subject to the Counterfactual Conclusion, the we simply say F1 is a Cause for (or caused) F2.*

Not only was our story a simplified version of the real Lake Constance mid-air collision, but our selection of factors for the Counterfactual Tests was also limited. There are other Causes for the collision within the simplified story.

- Could the mid-air collision have happened, had the STCA not been inoperative?
- Could the STCA have been inoperative, had it not been taken offline for maintenance?
- Could the air traffic controller at Zurich not have monitored the situation over Lake Constance continuously, had he not been busy directing incoming traffic for Friedrichshafen airport?

2.3 Countermeasures

The main driving factor behind the analysis of Accidents is to improve systems. If a system fails, an Accident analysis is conducted, the results are evaluated and this may lead to the change in the design of system. This is the way in which Accident analyzes can make the world a safer place. Counterfactual reasoning is one way of bridging the gap between an Accident analysis and the decision to change a system's design.

What can we learn from our simplistic story of the Lake Constance mid-air collision? From the Counterfactual Conclusion we know that the Accident has many Causes whose disappearance would effect the disappearance of the Accident. If we want to eliminate this Accident, or to be a bit more ambitious, many similar Accidents, then we have to implement Countermeasures that eliminate one of the Causes of the Accident. There are Causes in our simplified version of the story that we do not have influence on. For example non of the equipment used for air traffic control is maintenance free. We cannot assume that simply not doing maintenance work will solve the problem, simply because the equipment will deteriorate and then the air traffic controllers are again in a similar, if not worse, situation with degraded radar or telephone functionality.

What about a rule that requires maintenance to be conducted on only on one system at a time? In our case the Karlsruhe air traffic controller would have been able to phone the Zurich air traffic controller. This would surely be an improvement, but only for those Accidents where there is a second air traffic controller monitoring neighboring controlled air space. An additional rule requiring the notification of other air traffic controllers on the reduced functionality of an air control center may further improve the odds of preventing another Accident of this type.

If we develop Countermeasures we can use our Accident analysis for a first effectiveness check. From every Accident analysis we can derive a number of Countermeasures. Even from our simplified example we can infer Countermeasures that would also hold in the real thing, given that all the information given in the simple story also hold in the real one. That shows that it is possible to divide labor. Some Countermeasures may be of technical nature, others may be of legal nature. Thus different people can each work on Countermeasures from their field of expertise.

2.4 Check your understanding

Exercise 4 In Exercise 1 we have seen the story of the RMS Titanic.

- Which of the Causes of the RMS Titanic Accident are withing human ability to influence?
- Which Countermeasure would you suggest in case the imaginary RMS Titanic II would try the same voyage?
- Give the Counterfactual Reasoning for your suggested Countermeasure.

Exercise 5 On a particular stretch of road the accident rate increases. The road bends sharply and several cars crash into the hard shoulder on the side e of the road. The following Countermeasures are discussed:

- More warning signs.
- Installing a speed camera.
- Rerouting the road to make the bend less sharp.

Discuss the effectiveness of the Countermeasures in comparison with each other. Which Countermeasure, would you prefer? Why?

Exercise 6 A car hits a person unintentionally. The was speeding a bit, going 40 km/h on a 30 km/h road.

- Discuss in how far excessive speed was a Cause for the Accident.

The driver argues, that excessive speed is not a Cause. He agrees that had he been going slower he would not have been at point of the Accident at the same time, but later. This Accident might have been prevented. But the driver also argues, that had he been going faster he would also not have been at the point of the Accident.

- Discuss in how far the argument holds for a single Accident and in how far the argument is valid for Accidents in general.

3 The First Accident Analysis

If you are using the WBA Software Tool you will find instructions to the topics covered in the following sections at the end of each section. Instuctions will not be very detailled. It will be assumed that at least the Quick Start Guide has been read.

3.1 Technical Term: Why-Because Graph (WBG)

In previous sections we have already learned the concept of Causal relations. Causal relations are directed, which means that it is important which occurrence is at which end of a Causal relation. One is a Cause and the other is an Effect. If we revert the relation it will denote something different. Something very different.

There have already been some diagrams depicting Causal relations using boxes and arrows. The arrows are always pointing from the Cause to the Effect, which is the same direction in which a time-arrow would point. For a complex Accident analysis many such relations exist and it is often helpful to visualize complex data if possible. If we draw boxes for all ocurrences and arrows for all Causal relations in one diagramm then we have a constructed a WBG.

The WBG is a directed graph, which is mathmatician-speak for a graph where the arrowsi[7] have arrow heads. Following the arrows must not lead to circles. This would mean that causality is circular which violates the laws of causality. So a WBG is a *non-circular directed graph.*

Other technical terms that will be used are

- A **Node** will be a box in the WBG.
- An **Edge** will be an arrow in the WBG.
- An **Effect** will be the box at the pointy end of an arrow.
- A **Factor** will denote the same a Node, but needs not neccessarily be a part of the WBG. In other words

3.2 Friendly Fire isn't

For the next sections the following story will be used to illustrate the steps of performing a WBA. The story is a retelling of an article that was published in the Washington Post, by Vernon Loeb, a Staff Writer, on March 24th, 2002. It describe a Friendly Fire accident which occurred in Decmber 2001 during Operation Enduring Freedom in Afghanistan.

The version given here is a redacted one which does not accurately resemble the events described by Vernon Loeb. The Friendly Fire Accident is used as a first WBA case during System Safety lectures at Bielefeld University and during industrial courses given by Causalis Limited. Since I have experience with both, I changed the story to be more study-friendly and less accurate. In an interactive environment many of the unknown concepts can be explained on demand and the lecturer can substitute for a lack of domain knowledge on the side of the students. But the main aim is that this introduction to WBA should allow self study, so some trade-offs have to be made.

[7] The mathmatician uses the term Edge, or directed Edge in this case, instead of arrow.

3.2.1 The Setting

The Accident happens during the first months of Operation Enduring Freedom in Afghanistan. U.S. Forces have invaded Afghanistan and combat operations are still on an all-out-war level.

3.2.2 The Accident

A team of U.S. Special Forces soldiers, operating in Afghanistan, were engaging a Taliban position. The U.S. Special Forces soldiers called in an air strike on the Taliban position. The targets GPS coordinates came from a device called a "plugger". The official acronym of the device is PLGR, which is short for Precision Lightweiht GPS Receiver. The plugger can be used to calculate positions for air strike targets. The U.S. Special Forces air controller, the person responsible for calling in an air strike, successfully used the plugger to strike the Taliban position. The controller called in a U.S. Navy F/A-18 which attacked the Taliban position using GPS guided munitions[8]. A couple of minutes later the U.S. Special Forces intended to strike the same Taliban position a second time. The first calculation of GPS targeting coordinates was done using the GPS minutes-seconds format. An example would be 57 deg 38' 56.83" N, 10 deg 24' 26.79" E, which would mean 57 degrees, 38 minutes, 56 seconds and 83 hundreds of a second northern latitude and 10 degrees, 24 minutes, 26 seconds and 79 hundreds of a second eastern latitude. A different format is the degrees-decimal format. 57.64911 10.40744 would be the same position, but with minutes and seconds denoted as fractions of degrees. The F/A-18 required the minutes-seconds format, but for the second strike a B-52 was tasked with the attack. But the B-52 neede the degrees-decimal format, so some additional calculation was required. The U.S. Special Forces air controller was doing the calculation, but before transmitting the coordinates to the B-52 crew the plugger's battery died. A replacement battery was put in the plugger which came back to life. Unknown to the air controller the plugger initializes itself with its own positions, rather that the last displayed one, which was what the controller was assuming. Not recognizing the difference in coordinates the controller transmitted the displayed coordinates to the B-52. The air strike hit the U.S. position killing three soldiers and injuring 20.

3.2.3 Some Unknowns

It is not clear from the article how exactly the calculation of targeting coordinates is done. The plugger knows its own position. Ways of aquiring the target position could be by using precise maps, by laser designation and range finding or simply by estimation of distance and direction of the target realtive to ones own position.

Also it is unknown which other aids were used by the air controller to help in calculating the target coordinates.

Since the distance between the U.S. position and the Taliban position is not known the number of digits that were different in their respective coordinates is not known.

[8] So called JDAM, Joint Direct Attack Munitions

Figure 9: Precision Lightweight GPS Receiver, source: Wikipedia

Why the F/A-18 and the B-52 required different formats for targetting is also not known.

3.2.4 First Things First

Technical Term: Damage What is the damage in the story? Clearly the loss of life and the injuries inflicted to friendlies.

Accident What is the Accident? Which event caused the damage done? Clearly the bomb, dropped by the B-52, caused the casualties.

A quick check using the Counterfactual Test: Had the bomb not been dropped on the U.S. Special Forces Soldiers postion, had the three Soldiers died and 20 others been wounded?

The dropping of the bomb also was sufficient. The bomb did not need the presence of other Factors to do the damage.

Technical Term: Proximate Causes Lets find the proximate Causes. We term all those Causes Proximate Causes that immediately precede the Accident. This is dependent on the level of detail of an analysis. An analysis of a greater level of detail may have other Proximate Causes, that an analysis of a lower level of detail. The simple reason being, that higher detail may describe the same set of events in multiple Factors, that a lower level of detail may subsume in one Factor.

In this case there is only one Accident Factor. This may not always be the case, so do not try to force the structure of your WBG on the presence of only one Accident.

In this case lets start with the Causal Sufficiency Test, to gather all Factors that enable the bomb to be dropped on the U.S. Special Forces Soldier's position.

- There had to be an aircraft that was capable of GPS guided ground attack.

- The air traffic controller and the air craft had to communicate in order to coordinate strikes.
- The aircraft needed clearance and target coordinates to commece an attack.

When all these three Factors come together then the Accident can happen. We check with the Counterfactual Test:

- Had there been no aircraft equipped with GPS guided munitions, had the bomb been dropped? No.
- Had there been no way of communication between the aircraft and the air controller, had the bomb been dropped? No.
- Had the aircraft not been cleared to target the GPS coordinates received by the air controller, had the bomb benn dropped there? No.

On a side note, observe that the Counterfactual Test reveals two different kinds of question. The first two questions concern themselves with whether the bomb had been dropped or not. The last question concerns itself with the location the bomb had been dropped.

Since the intention of the U.S. Special Forces soldiers clearly was the release of a bomb, but on a different location, the latter question is clearly the one leading us to where things went wrong.

What is it called again? Students who work on this case often no not use precise descriptions or names. One example is confusion between the terms *position* and *coordinates*. In the above story the term *Taliban position* denotes the physical location of the Taliban, while the term *coordinates* is used to denote the GPS data. When the original story is taken the distinction is not obvious and many students use the terms interchangeably. There is also use of value judgements. For example some students describe the bombing of the U.S. position as attacking the *wrong* coordinates. But it is not clear in whose frame of mind the coordinates are wrong. The coordinates are valid in that there is a physical location on the earch surface that corresponds to them. The coordinates are within the B-52s area of operation and the B-52 crew successfully attacks the position belonging to the coordinates given to them.

We will use the following terms from here on:

- *Soldiers* will denote the U.S. Special Forces soldiers as a group.
- *Air Controller* will denote the soldier, member of the Soldiers, who was responsible for calculating targeting coordinates and calling in air strikes.
- *F18* will denote the F/A-18, the aircraft that conduted the first airstrike on the Taliban Position.
- *B52* will denote the B-52 bomer aircraft, that conducted the second airstrike, which hit the Soldier's Position.
- *Taliban Position* will denote the physical location of the Taliban which the Soldiers intended to strike.

- *Soldier's Position* will denote the physical location of the Soldiers.
- *Taliban Coordinates* will denote the GPS coordinates that correspond to the Taliban Position.
- *Soldier's Coordinates* will denote the GPS coordinates that correspond to the Soldier's Position.
- *Displayed Coordinates* will denote the GPS coordinates that appear on the display of the plugger.
- *JDAM* will denote a GPS guided bomb.

3.2.5 Factorizing the Narrative

We already introduced the technical term Factor. We want to take the Accident narrative, our story above, and extract all relevant information so that we can determine the Causes of the Accident. In other words our analysis aims to produce a WBG from the data given in the text. But in almost no case would we be able to take the narrative verbatim. There are many sentences that do not lend themselves to the Counterfactual Test or the Causal Sufficiency Test. Instead we formulate new sentences, new Factors, that preserve the meaning of the original narrative, but are better suited to be tested. In the above paragraphs that describe the Damage for example I have already done that. If you reread the last sentence of the narrative you will find, that there are two factors in the same sentence. In the same sentence the Accident, JDAM dropped on Soldier's Position, and the Damage, 3 dead and 20 wounded, are mentioned.

In general we want aim for each Factor to

- accurately depict data from the narrative (or other sources of Accident data) and
- not be further divisible into meaningful statements.

For example the sentence "I hit the brakes to slow (the car) down." contains three pieces of information. The sentence can be expressed by the three following Factors:

- I intend to slow down.
- I hit the brakes.
- The car slows down.

The "not further divisible" criterion strongly depends on the level of detail. If the level of detail is increased then "The car slows down" could be further explained or substituted by the mechanical interactions from pedal to tires. Another question is if other implied Factors of a statement add insight into the Accident analysed. It would not make much sense to include a Factor like "I am in the car."

Even though we have two rigorous tests, the Counterfactual Test and the Causal Sufficiency Test, there is still plenty of room for an analyst. As long as the analyst is satisfied with the choice the Counterfactual Test and Causal

Sufficiency Test should suffice in assuring the correctness and completeness[9]. If the correctness and/or completeness is challenged consider if the challenge is appropriate by

- checking if the challenge considers one Factor or more,
- estimating the impact on the descriptive value of a new Factor or a changed Factor,
- performing the Counterfactual Test to find out if a disputed Factor is a Cause or not and
- performing the Causal Sufficiency Test to find out if a disputed Factor is indeed missing.

This means to write up an argument for the choice made and refuting claims of incorrectness. This not part of the WBG to be constructed, but it is part of the WBA. This is another reason to be careful with the formulation of Factors and the naming of actors, objects and concepts.

3.2.6 The First Graph

After these first steps the WBG should look like this:

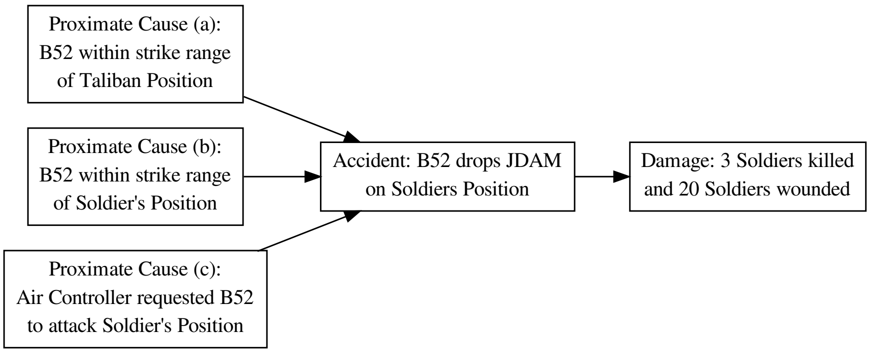
Proximate Cause (a): B52 within strike range of Taliban Position
Proximate Cause (b): B52 within strike range of Soldier's Position
Proximate Cause (c): Air Controller requested B52 to attack Soldier's Position
Accident: B52 drops JDAM on Soldiers Position
Damage: 3 Soldiers killed and 20 Soldiers wounded

Figure 10: The first Nodes of the Firendly Fire WBG.

The Node texts are compliant with the non-divisible criterion and also use the terms we defined earlier. But that does not mean that this is the only solution. Feel free to change the statements.

[9] Completeness is very hard to argue. Here I use the term loosely. Someone questioning your choice of Factors will always find something which will violate completeness in a more rigorous sense. Just imagine listing each law of physics that is applicable. It just would not add to the descriptive value of the WBG.

3.3 If you use the WBA Software Tool

Create a new project in the project view. In the Graph View create a new Node, the Damage Node. As Node text set *3 Soldiers killed and 20 wounded.*. Then add a Cause to the Node, the Accident Node, with the text *B52 drops JDAM on Soldier's Position*. Which in turn has the following Proximate Causes: *(a) B52 was equipped with JDAM. (b and c) B52 was within strike range of (b)Taliban Position / (c) Soldier's Position. (d) Air Controller requested B52 to attack Soldier's Coordinates.*

3.4 Check your understanding

Exercise 7 The following statements are not yet Factors that we would like to use in a WBG. Rephrase them to fit the requirements.

- The F/A-18 attacked the Taliban with GPS guided bombs.
- The air controller did not recognise that the plugger displayed corrdinated different from those before the battery had to be changed.
- The B-52 attacked the wrong coordinates.

Exercise 8 Given the inital WBG of 5 Nodes that was constructed here. The following challenges are brought forward:

- The air controller had to change the batteries of the plugger. This should be a Proximate Cause, because it was the main Cause in this whole Accident.
- Isn't is a Proximate Cause that the JDAM reliably hit the targeting position? After all it could have been faulty or stray from its intended trajectory.
- There is no mention of who authorized the air strike. That should be included somewhere.

Excercise 9 In Germany cars with trailers must not exceed 80 km/h, even on the Autobahn. Car C drives on the Autobahn with a trailer, but travels 110 km/h. The trailer is empty and does not have its own brake system. At 110 km/h the trailer, when empty, will start to bounce behind the car, which can be felt in the car. The correct way to handle such a situation is to slow down very gently. If the deceleration is too fast then the trailer will overtake the car, and the driver looses control. The driver of car C notices the bouncing of the trailer and panics. He hits the brakes, the trailer maintains momentum and car C and trailer end up at right angels to the direction of travel. A following truck sees it coming and hits the brakes. The truck comes to a halt and does not hit car C or the trailer. But instead car D, which was following the truck, but did not keep a safe distance, rear-ends the truck. Car D is damaged beyond repair, the driver of car D is severly injured and the truck is lightly damaged.

- Determine the Damage, Accident and Proximate Causes of this Accident.
- Explain the difference between Accident causation and who is to blame.

4 First Accident, contd.

In the previous section we have seen how to start our work of Accident analysis using WBA. This is not the only way to start, there are probably as many as there are different analysts. But the scope of this introduction is limited, so we cannot explore in depth the pros and cons of different approaches. Be assured, that with each WBA your approach will differ more and more from the one initially presented here. The approach presented here needs to take into account the readers limited knowledge of the concepts of WBA. As those concepts become clear there are less restrictions on how to conduct an analysis.

In this section we will continue with our analysis of the Friendly Fire Accident from the previous section.

4.1 Factors from the Narrative

In the last section we already constructed an initial WBA with a Damage Factor, an Accident Factor and Proximate Cause Factors.

Lets go through the Proximate Causes and see if we can find out their NCFs and discover some other aspects of WBA along the way.

4.2 The Stopping Rule

Proximate Causes (a, b): B52 was within strike range of Taliban Position / Soldier's Position Although there are plenty of Causes, why the B52 was where it was, there is little value in further analysis. The military operation, as conducted during Operation Enduring Freedom, was designed to include combat air support (CAS). Even though we would prevent this accident had there been no CAS available, from a military strategic point of view this would be extremely undesirable.

Stopping because of insufficient explanatory value Every NFC has to be checked by the Counterfactual Test. Some Factors cannot be explained from the Accident narrative alone, but require further research. At some point the cost of further explaining the Causation of some Factors is prohibitive. It is better to stop and concentrate on Factors that offer greater insight if they are further analyzed.

Stopping because of infeasability of countermeasures The Accident could have been prevented had there been not CAS. No bomb could have been dropped on anybody. But this is also the prohibiting Factor. Ceasing CAS operations would (most probably) endanger more friendlies than it would harm them. The availability of CAS is a Factor of both positive and negative consequences, but the positive consequences largely outweigh the negative ones. The aim of investigating this Accident should not be to eliminate CAS, but rather to reduce the negative consequences.

Stopping because of insufficient influence If a Factor is beyond influence, there is little need to further investigate its Causes. Consider the Tohoku earthquake mentioned in the first section. There is no way that earthquakes could be prevented. It is beyond human capability. Within the scope of an

Accident analysis there is little value in determining the Causes of such Factors as earthquakes.

4.3 Further Analysis

Proximate Cause (c): Air Controller requested B52 to attack Soldier's Position We do not know if the Air Controller was directly communicating with the crew of the B52 or if there were intermediaries. But even if there were intermediaries, for example air combat controllers on board of an AWACS[10], they would only have relayed the information given by the Air Controller to the B52. So for all practical purposes we can assume that the Air Controller was communicating directly with the B52 crew.

It is also unclear who authorized the strike. If a different party from the Air Controller authorized the strike, there was no way of checking whether the Air Controller had done his job properly. Again we can safely assume that the Air Controller authorized the strike, since another party's authorization would have resulted in the same course of action.

What are the necessary and sufficient Factors for this Proximate Cause?

- The Air Controller's intention was to call in an a second air strike on the Taliban Position.
- The Air Controller (mistakenly) thought that he was giving the Taliban Coordinates to the B52.

Are those NCFs? A quick check using the Counterfactual Test:

- Had the Air Controller requested an air strike on the Soldier's Coordinates if he had not intended to strike the Taliban Position a second time? No.
- Had the Air Controller requested an air strike on the Soldier's Coordinates if he had not (mistakenly) assumed that they were the Taliban Coordinates? No.

And the Causal Sufficiency Test? All the B52 needs to strike a target are GPS coordinates. They were provided with the Soldier's Coordinates. There is no reason why the B52 would not target the coordinates given if requested. There is also no reason why the Air Controller would not request an air strike on an assumingly enemy position. The two Factors are sufficient.

Rephrased to fit the phrasing requirements mentioned in the previous section:

- *Cause (a): Air Controller intends to call in air strike on Taliban Position.*
- *Cause (b): Air Controller believes Soldier's Coordinates to be Taliban Coordinates.*

The WBA now looks as like Figure 8:

Now we again have two Factors that we wish to further investigate. Cause (a) and Cause (b).

[10] Airborne Warning And Control System

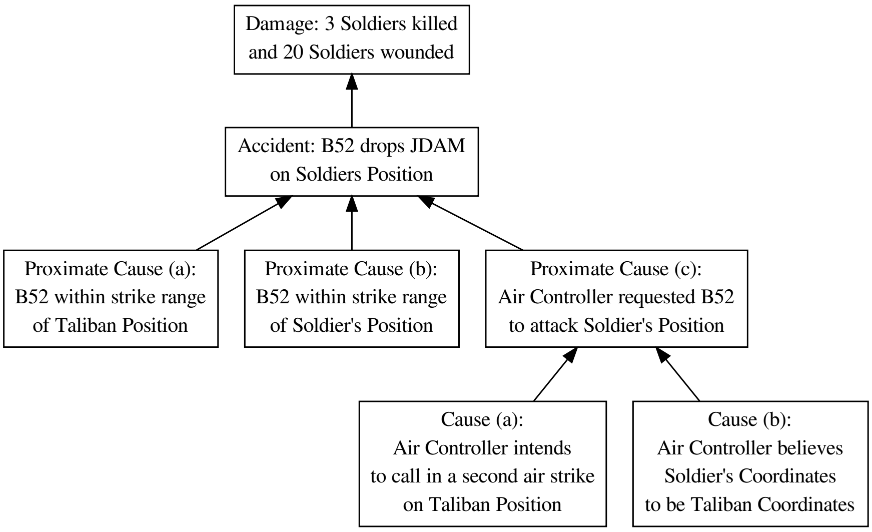

Figure 11: Friendly Fire WBG, so far.

Cause (a): Air Controller intends to call in air strike on Taliban Position. The narrative is not explicitly stating the reasons why the Air Controller intended to strike the Taliban Position a second time. But we can reasonably assume that the Soldiers were engaging the Taliban and the first air strike was insufficient to win the engagement.

As Factors:

- *Cause (c): Soldiers engaged in combat with Taliban*
- *Cause (d): F18 air strike insufficient to neutralize Taliban*

The Counterfactual Test:

- Had the Soldiers not been engaged with the Taliban, had they intended a second air strike on the Taliban Position? No.
- Had the F18 air strike been sufficiently effective to neutralize the Taliban, had the Soldiers intended a second air strike on the Taliban Position? No.

We include both into the WBG, see Figure 9:

Cause (b): : Air Controller believes Displayed Coordinates to be Taliban Coordinates. We continue, breadth first. We could also continue width first, there is no reason why one should be better than the other.

What are the Causes of Cause (b)? The narrative states that the Air Controller used the coordinates the plugger displayed. He believed the coordinates displayed on the plugger to be the Taliban Coordinates for a number of reasons:

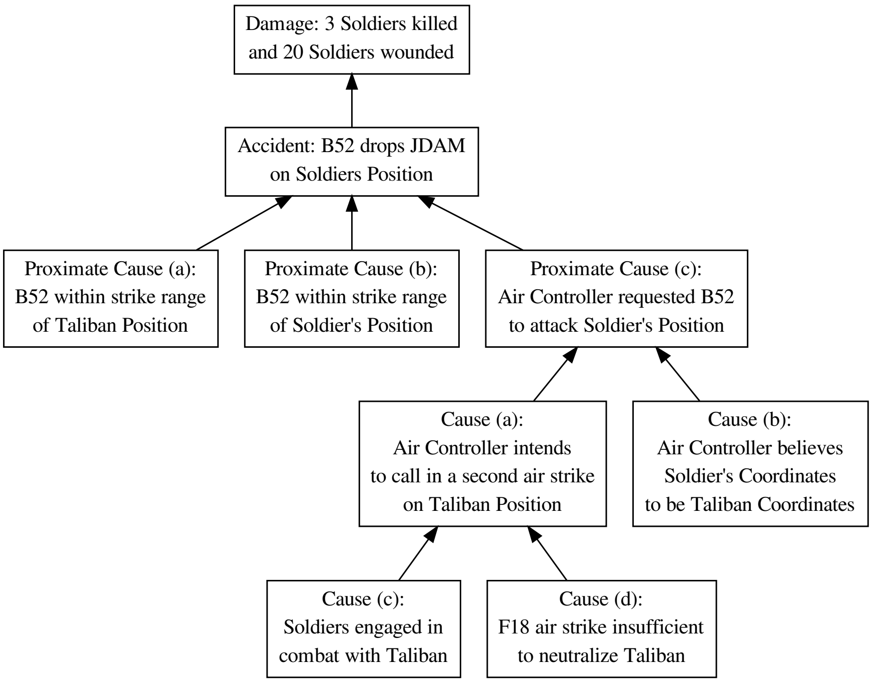
Damage: 3 Soldiers killed and 20 Soldiers wounded
Accident: B52 drops JDAM on Soldiers Position
Proximate Cause (a): B52 within strike range of Taliban Position
Proximate Cause (b): B52 within strike range of Soldier's Position
Proximate Cause (c): Air Controller requested B52 to attack Soldier's Position
Cause (a): Air Controller intends to call in a second air strike on Taliban Position
Cause (b): Air Controller believes Soldier's Coordinates to be Taliban Coordinates
Cause (c): Soldiers engaged in combat with Taliban
Cause (d): F18 air strike insufficient to neutralize Taliban

Figure 12: Friendly Fire WBG; Version 3.

- The Air Controller could not tell the Soldier's Coordinates from the Taliban Coordinates.
- The Air Controller was predisposed to believe that the Displayed Coordinates were Taliban Coordinates.

As always we check with the Counterfactual Test:

- Had the Air Controller been able to tell the Taliban Coordinates from the Soldier's Coordinates, had he believed that the Displayed Coordinates were Taliban Coordinates? No.
- Had the Air Controller not been predisposed to believe, had he believed that the Displayed Coordinates were Taliban Coordinates? No.

We introduce our new Factors into the WBG, see Figure 10.

Cause (c):Soldiers engaged in combat with Taliban Following this one up is of little value for our analysis. The soldiers were supposed to take part in combat operations.

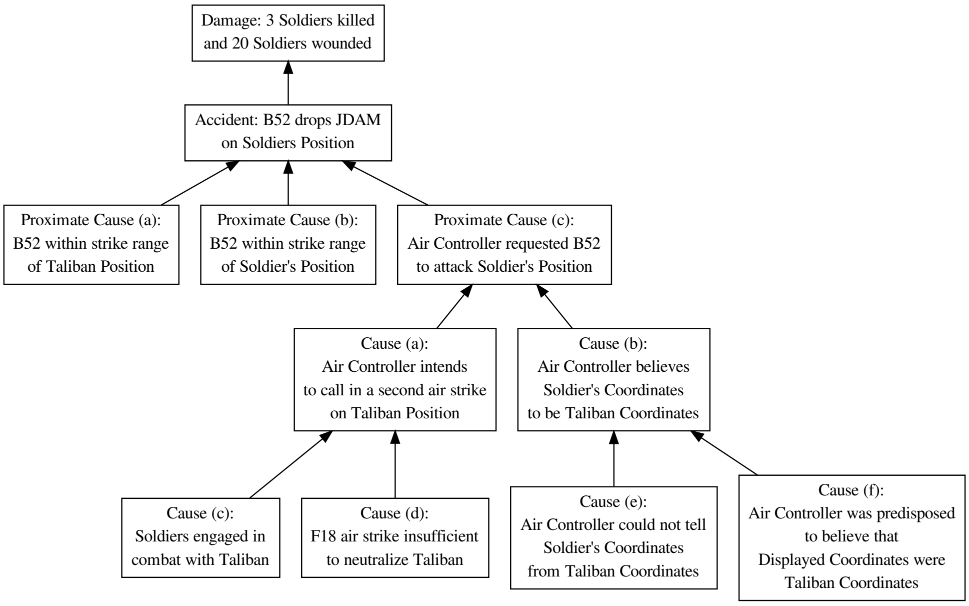
Damage: 3 Soldiers killed and 20 Soldiers wounded
Accident: B52 drops JDAM on Soldiers Position
Proximate Cause (a): B52 within strike range of Taliban Position
Proximate Cause (b): B52 within strike range of Soldier's Position
Proximate Cause (c): Air Controller requested B52 to attack Soldier's Position
Cause (a): Air Controller intends to call in a second air strike on Taliban Position
Cause (b): Air Controller believes Soldier's Coordinates to be Taliban Coordinates
Cause (c): Soldiers engaged in combat with Taliban
Cause (d): F18 air strike insufficient to neutralize Taliban
Cause (e): Air Controller could not tell Soldier's Coordinates from Taliban Coordinates
Cause (f): Air Controller was predisposed to believe that Displayed Coordinates were Taliban Coordinates

Figure 13: Friendly Fire WBG; Version 4.

4.4 Unknowns in the Analysis

Cause (d):F18 air strike insufficient to neutralize Taliban Unfortunately we do not have enough information to completely follow up on Cause (d). We know that there was an air strike, had there not been one it could not have been insufficient:

Cause (g): F18 air strike on Taliban Position.

We do not know the strength of the Taliban attacked, the precision of the strike nor if the bomb performed below its expected effectiveness. From the narrative we know that the strike happened and from the need for a second strike we can infer that the F18 strike was insufficient. But we cannot tell why. Instead of a NFC we will introduce a Node into the WBG clearly marking our lack of information. We know that there was a Cause for this. We have no reason to assume that this unknown Cause is beyond our ability to control, neither that it would not be a valuable insight. Needless to say that this Factor will not be further causally analyzed and will remain a leaf Node, as in Figure 12: *Unknown (a): Strength of Taliban, Performance of JDAM and strike precision are unknown.*

4.5 Technical Term: Assumption

Cause (e): Air Controller could not tell Soldier's Coordinates from Taliban Coordinates We know that this must have happened, even though the narrative does not explicitly state this. But why did the Air Controller not recognize the difference? The different coordinates mapped on different locations, so they had to be different. Nevertheless we can safely assume that the visual difference was not that great. Degrees latitude and longitude, the left most digits in GPS coordinates irrespective of format, are the most prominent. They mean the greatest difference in physical location relative the the digits more on the right. If the distance between the Soldier's Position and the Taliban Position is not very great the difference in the sequence of digits may be very small. The Air Controller was using different formats for different calls for air strikes, which may have contributed to his inability to have a clear memory of the Taliban's Coordinates. Please note that, although this may qualify as another Assumption, it is more speculative.

Assumptions are also tested using the Counterfactual Test:

- Had the Taliban Coordinates and the Displayed Coordinates been visually sufficiently different, had the Air Controller been able to tell the Taliban Coordinates from the Displayed Coordinates? Yes[11].

That is why I would not introduce it into the WBG, but leave it here as an explanation for the original Assumption.

We introduce our first Assumption into the 6th version of our WBG, see Figure 13: *Assumption (a): Taliban Coordinates and Displayed Coordinates did not visually differ sufficiently.*

Cause (f): Air Controller was predisposed to believe that Displayed's Coordinates were Taliban Coordinates. According to the narrative the Air Controller was working on the Taliban Coordinates for the second air strike. The Air Controller obviously did not expect the plugger to display different coordinates from the ones entered after a power cycle.

The Counterfactual Test:

- Had the Air Controller not been entering the Taliban Coordinates into the plugger, would he have been predisposed to believe that the Displayed Coordinates were Taliban Coordinates? No.
- Had the Air Controller known that entered coordinates would not survive a power cycle, would he have been predisposed to believe that the Displayed Coordinates were Taliban Coordinates? No.

We introduce two new Causes:

- *Cause (h):Air Controller entered Taliban Coordinates into the plugger.*
- *Cause (i):Air Controller did not know that power cycling the plugger changed Displayed Coordinates.*

Our new WBG looks like Figure 14.

4.6 Not a Tree anymore

One of the Causes of our newly introduced Cause (h) is already part of the WBG.

[11] To pass the Counterfactual Test this time the answer must be Yes, because the second part of the question was rephrased from "could not tell" to "been able to tell".

- Had the Air Controller not intended to call in an air strike on the Taliban Position, had he entered the Taliban Coordinates into the plugger? No.

Cause (a) is already part of the WBG. All we need to do is add an additional Edge, giving the WBG its new form, as depicted in Figure 15.

Cause (i):Air Controller did not know that power cycling the plugger changed Displayed Coordinates. No information is given in the narrative why this would be the case. Following this Factor would only lead to speculation, which is what happened in the original narrative by Vernon Loeb. Insufficient training and stress during battle were candidates for Causes for Cause (i). In an ongoing analysis this indicates where further investigation is warranted. The Causes of Cause (i) could provide valuable insight into the way the plugger is used by soldier in the field and it could provide a good point for introducing Countermeasures.

4.7 The Rest

There are not many Factors that are left for the final WBG.

4.8 If you use the software

If you use the software tool try to recreate the WBG the way we have done here. Please be aware that the rendering algorithm used for the layout may not render your graph the same as you saw here. How it is lay outed is not important. It is important that the same Nodes are connected by the same Edges. If you do not like the lay outing feel free to use other software tools, but be reminded, that having automatic layout greatly reduces time and effort. Try to draw the last WBG using a conventional boxes-and-arrows toolkit and compare the time it took and the aesthetics of both.

In the *Graph View* use the *Edge Detail* sub-view to keep track of the NFC justifications.

4.9 Check Your Understanding

Exercise 10

- Which of the Nodes has to be further analyzed? Assume that the Air Controller would be available for an interview and that military procedures could be reviewed.
- Give the reasons why it is worthwhile or not.

Exercise 11 Complete the WBG. Pay special attention to the facts

- that the battery of the plugger has died and
- that the Taliban Position has already been successfully attacked

Exercise 12 Now you have seen one analysis in depth. Before you go on to study further concepts you should be practicing your skills. You can find lots of Accident analyses on the WWW. For a start the Wikipedia offers articles on Accidents. For practicing you do not need authoritative resources, just a source for stories. If you prefer authoritative resources I would recommend national investigation boards for various domains. A good source is the U.S. National Transportation Safety Board (NTSB). On the NTSB website[12] you can find analyses on aviation, railway, marine and road accidents. Some domain knowledge is necessary, but road accidents should be analysable by everyone who holds a driver's license. Another source would be the WBA Textbook, to be published.

[12] www.ntsb.gov

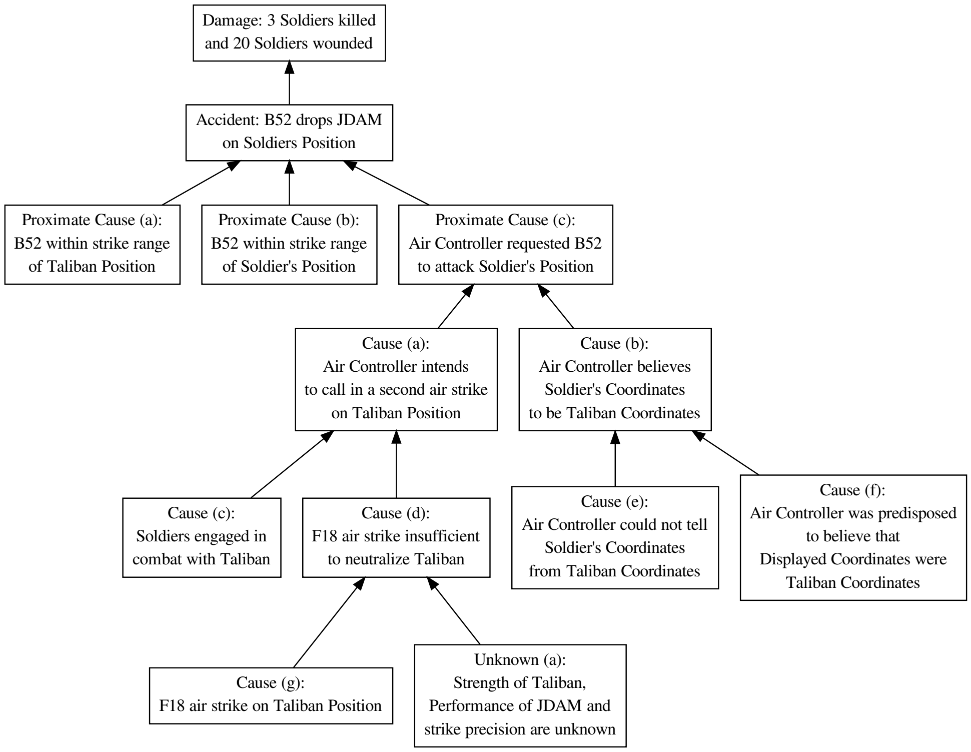
Damage: 3 Soldiers killed and 20 Soldiers wounded
Accident: B52 drops JDAM on Soldiers Position
Proximate Cause (a): B52 within strike range of Taliban Position
Proximate Cause (b): B52 within strike range of Soldier's Position
Proximate Cause (c): Air Controller requested B52 to attack Soldier's Position
Cause (a): Air Controller intends to call in a second air strike on Taliban Position
Cause (b): Air Controller believes Soldier's Coordinates to be Taliban Coordinates
Cause (c): Soldiers engaged in combat with Taliban
Cause (d): F18 air strike insufficient to neutralize Taliban
Cause (e): Air Controller could not tell Soldier's Coordinates from Taliban Coordinates
Cause (f): Air Controller was predisposed to believe that Displayed Coordinates were Taliban Coordinates
Cause (g): F18 air strike on Taliban Position
Unknown (a): Strength of Taliban, Performance of JDAM and strike precision are unknown

Figure 14: Friendly Fire WBG with the first indicated Unknown Factor.

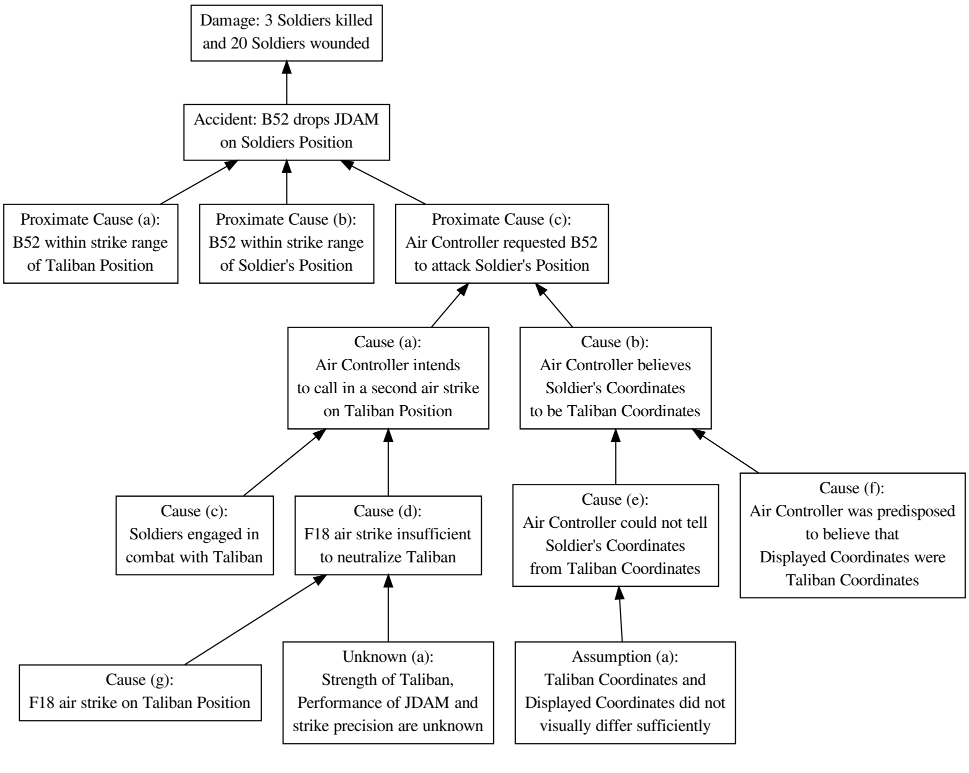
Damage: 3 Soldiers killed and 20 Soldiers wounded
Accident: B52 drops JDAM on Soldiers Position
Proximate Cause (a): B52 within strike range of Taliban Position
Proximate Cause (b): B52 within strike range of Soldier's Position
Proximate Cause (c): Air Controller requested B52 to attack Soldier's Position
Cause (a): Air Controller intends to call in a second air strike on Taliban Position
Cause (b): Air Controller believes Soldier's Coordinates to be Taliban Coordinates
Cause (c): Soldiers engaged in combat with Taliban
Cause (d): F18 air strike insufficient to neutralize Taliban
Cause (e): Air Controller could not tell Soldier's Coordinates from Taliban Coordinates
Cause (f): Air Controller was predisposed to believe that Displayed Coordinates were Taliban Coordinates
Cause (g): F18 air strike on Taliban Position
Unknown (a): Strength of Taliban, Performance of JDAM and strike precision are unknown
Assumption (a): Taliban Coordinates and Displayed Coordinates did not visually differ sufficiently

Figure 15: Friendly Fire WBG with Assumption.

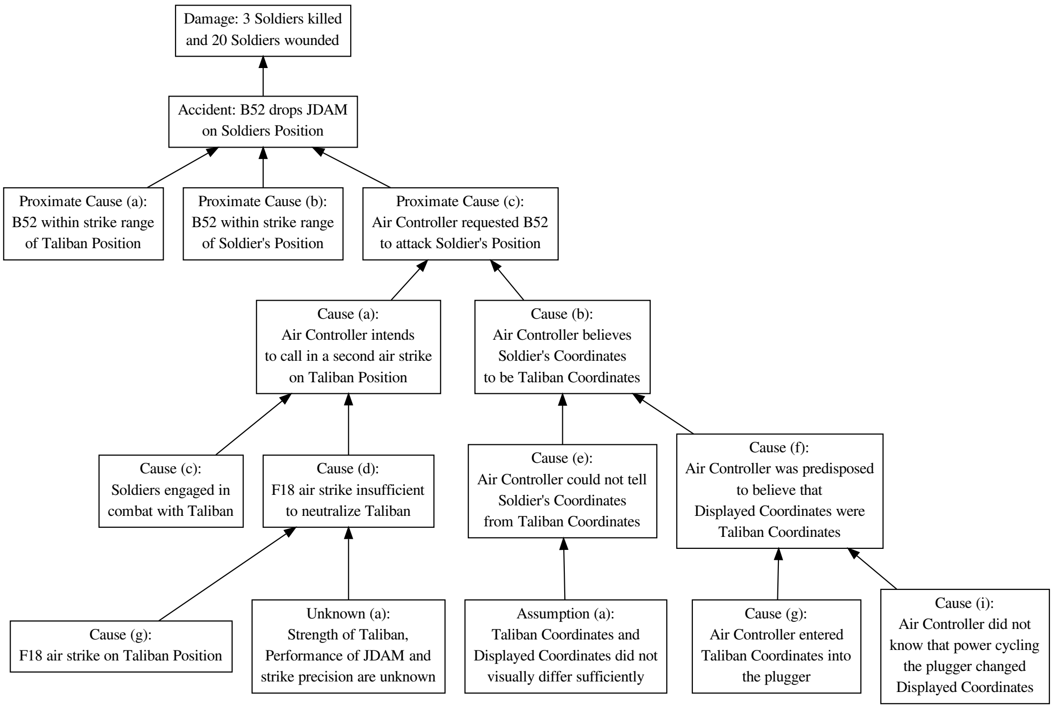
Damage: 3 Soldiers killed and 20 Soldiers wounded
Accident: B52 drops JDAM on Soldiers Position
Proximate Cause (a): B52 within strike range of Taliban Position
Proximate Cause (b): B52 within strike range of Soldier's Position
Proximate Cause (c): Air Controller requested B52 to attack Soldier's Position
Cause (a): Air Controller intends to call in a second air strike on Taliban Position
Cause (b): Air Controller believes Soldier's Coordinates to be Taliban Coordinates
Cause (c): Soldiers engaged in combat with Taliban
Cause (d): F18 air strike insufficient to neutralize Taliban
Cause (e): Air Controller could not tell Soldier's Coordinates from Taliban Coordinates
Cause (f): Air Controller was predisposed to believe that Displayed Coordinates were Taliban Coordinates
Cause (g): F18 air strike on Taliban Position
Unknown (a): Strength of Taliban, Performance of JDAM and strike precision are unknown
Assumption (a): Taliban Coordinates and Displayed Coordinates did not visually differ sufficiently
Cause (g): Air Controller entered Taliban Coordinates into the plugger
Cause (i): Air Controller did not know that power cycling the plugger changed Displayed Coordinates

Figure 16: Introducing Causes (h) and (i).

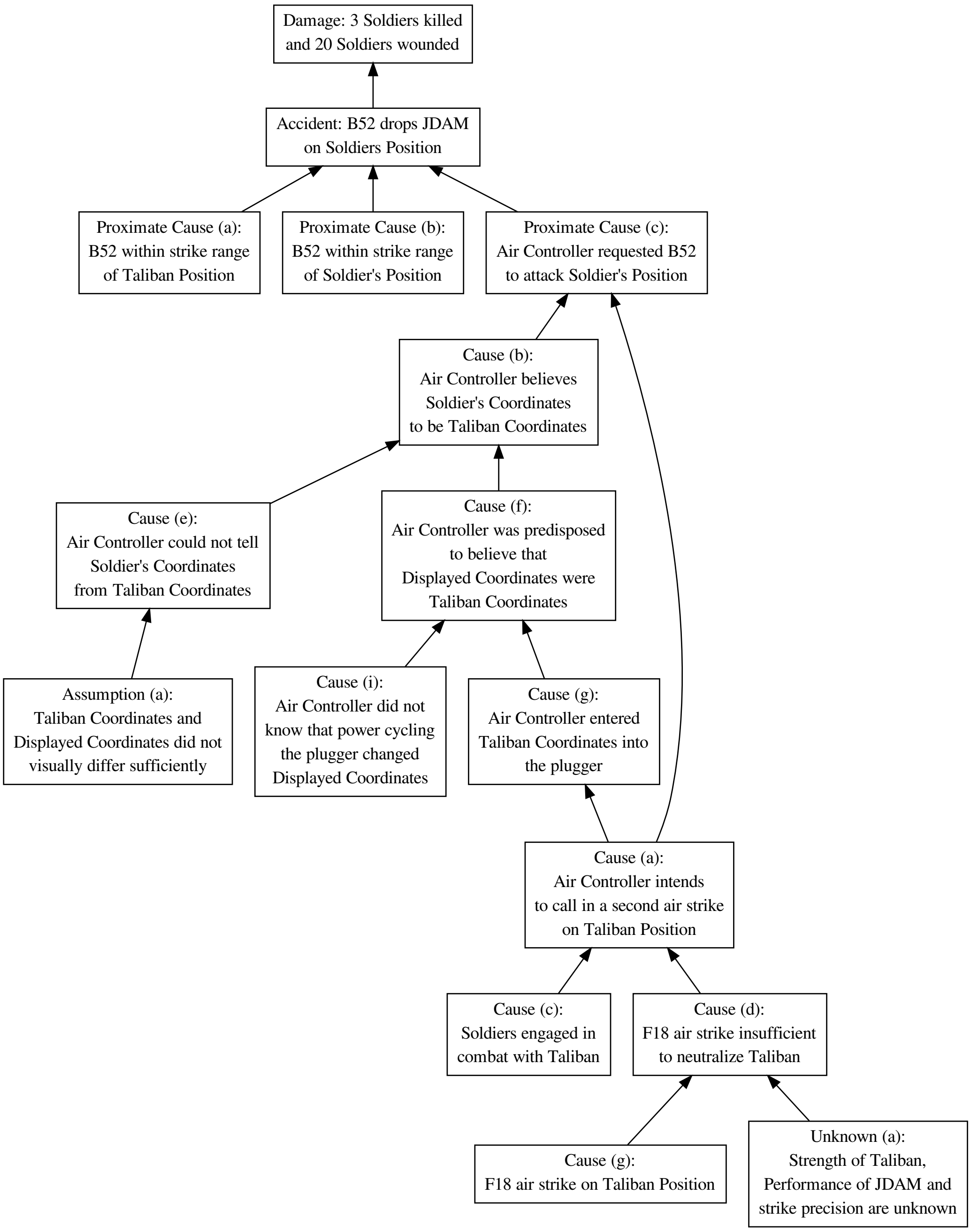
Damage: 3 Soldiers killed and 20 Soldiers wounded
Accident: B52 drops JDAM on Soldiers Position
Proximate Cause (a): B52 within strike range of Taliban Position
Proximate Cause (b): B52 within strike range of Soldier's Position
Proximate Cause (c): Air Controller requested B52 to attack Soldier's Position
Cause (b): Air Controller believes Soldier's Coordinates to be Taliban Coordinates
Cause (e): Air Controller could not tell Soldier's Coordinates from Taliban Coordinates
Cause (f): Air Controller was predisposed to believe that Displayed Coordinates were Taliban Coordinates
Assumption (a): Taliban Coordinates and Displayed Coordinates did not visually differ sufficiently
Cause (i): Air Controller did not know that power cycling the plugger changed Displayed Coordinates
Cause (g): Air Controller entered Taliban Coordinates into the plugger
Cause (a): Air Controller intends to call in a second air strike on Taliban Position
Cause (c): Soldiers engaged in combat with Taliban
Cause (d): F18 air strike insufficient to neutralize Taliban
Cause (g): F18 air strike on Taliban Position
Unknown (a): Strength of Taliban, Performance of JDAM and strike precision are unknown

Figure 17: The WBG looses its tree structure.

5 Sufficient, but Not Neccessary

There are cases where one Factor is a Cause, but does not pass the Counterfactual Test. Consider the following: Two stone throwers destroy a window. Both are throwing their stones simultaneously. Had stone thrower A not thrown his stone, would the window have been destroyed? Yes, because stone thrower B would have thrown a stone to destroy the window. And vice versa.

Both Factors are sufficient in themselves. One stone thrower alone would be enough to destroy the window. Indeed, one stone thrower would also pass the Counterfactual Test, were it not for the other stone thrower.

5.1 Similar Factors

In the above example both Factors were very similar. The action describted for both stone throwers is essentially the same. The difference is only that there are different persons throwing stones.

We need not make the life of the analyst unneccessarily difficult. In this case we can simply combine the two factors into one. This violates the general rule, that Factors should not be further divisible[13]. But it is justified here, for the following simple reason: One of the aims of the analysis is to develop Countermeasures. In this case the two Factors are so similar that we can reasonably expect them to be handled by the same Countermeasure. In most cases both Factors may be a result of a so called common Cause, which in turn suggests that a common Countermeasure may fix the problem. Installing tempered glass may be an effective Countermeasure to both thrown stones. Improving riot prevention may be an effective Countermeasute to the emergence of stone throwers.

5.2 Dissimilar Factors

Let's consider a different story with not-so-similar Factors.

This one is a little artificial. There is still a stone thrower who wants to destroy the window. The same instant that the stone thrower throws the stone an earthquake happens. The earthquake is sufficiently powerful to destroy the window.

Now we have two events, dissimilar, without a common cause, both of which destroy the window. Installing tempered glass still counters the stone thrower. It may even prevent the glass from shattering during an earthquake. But there is not Countermeasure that will prevent both Factors from happening.

Aggregating these two Factors into one only complicates things. The cleanest way[14] would be to make two WBGs. One analysing the stone thrower scenario and one analysing the earthqake scenario. This assumes that both Factors are not dependend on one another and do not share a common cause. If they do both WBAs will reveal that the independence assumption did not hold.

But making two WBAs is more work that one. To cope with this, rather strange and in my experience very rare, situation, we introduce a way to state the fact that there are two Causes that are sufficient, but in this very situation, not neccessary. Keep in mind that this is a substitute for having two WBGs

[13] As with every good rule there is an exception.

[14] From an academic point of view

and that the Counterfactual Test and Causal Sufficiency Test should hold for the virtual WBGs.

6 Factor Types

Before you start on Factor Types you should have your causal analysis close to being finished. If you are learning WBA you should first focus on learning the Counterfactual Test and Causal Sufficiency Test. Get familiar with basic concepts that were presented during the GPS Friendly Fire case before moving on.

6.1 Which Factor Types are there?

Do you need Factor Types? Factor Types are classifications of Factors[15]. The classification presented here is not neccessarily the only one. You may come up with any other classification of it suits the goal of an analysis. The classification presented here consists of the folloging Factor Types, which will be discussed in detail:

- Event
- Process
- UnEvent
- State
- Assumption
- Contraindication
- Countermeasure

The WBG software tool supports all of the above. Each of the Factor Types corresponds to a node shape, so they are easily identifiable at a glance.

6.1.1 Event

An Event in WBA is a change of the state of the world. Unfortunately, taking this literally is not very helpful. For the purpose of Accidnet analysis, Events are changes in states of things smaller than the world. These things, commonly called systems, are not definable in advance. Usuall an Accident analyst will choose a system definition implicitly when analysing the systems behaviour, which is a sequence of Events.

If I go 50 km/h in my car and accelerate to 60 km/h it may be suffiently details to say that there was one Event, acceleration from 50 km/h to 60 km/h. When my car moves at 50 km/h it constantly chagnes its position. Each change in position may be an Event under the definition, but it may not be one in the idealizes system used to describe Events that make sense from an Accident analysis point of view.

If more detail does not give us additional insight into an Accident, we should omit it.

[15] Remember: All Causes are Factors, but not all Factors are Causes.

6.1.2 Process

Processes are sequences of similar events. In our above example the acceleration of the car from 50 km/h to 51 km/h to ... to 60 km/h, can be described as a series of more detailed Events. Processes are used to describe the Process nature of a Factor. The above described Event may well be described as a Process. If the acceleration of the car is described as an Event or a Process depends on the relative analytical value of the two descriptions. If the Process nature should be emphasized it should be described as a Process.

In other cases the choice for classifying a Factor as a Process is simpler. If other Factors ocurr during a Process, which may still be going on after the Accident that is analysed, it is much easier to classify a Factor as a Process, than it is to describe the Process in terms of Events and correlate them with other Factors. During the meltdown of a nuclear power plant there are other Factors going on. Safety barriers fail, heat and pressure build, radiation emerges, monitoring and control devices fail. All these things may happen during a meltdown, and the meltdown may, at least in part, be a Cause for all of them.

6.1.3 UnEvent

An UnEvent is an Event that should have happened, but did not. A car that crosses a red light is an Event. But there is also an UnEvent in there. The rules of the road say that cars should stop before a red light. The car did not stop, but it should have been, so the UnEvent is that the car did not stop before the red light. Intuitively there is not much of a difference between saying *car crosses red light* and *car did not stop at red light*. It is clear to almost everybody that there are rules. The UnEvent explicitly states that

- something did not happen and
- that it should have happened.

When classifying a Factor as an UnEvent there must be a Factor that says *there is a good reason that something should have happened.* In most cases this *good reason* is some kind of rule. How explicit this rule is may well be a Cause.

6.1.4 State

States are true over the whole of an Accident. The rules mentioned above are good examples of States. The rule that says *stop before a red traffic light* holds throughout the Accident. There is no point in time where it does not hold. If you check your WBG for plausibility be reminded that an UnEvent usually has a State as one of at least two NCFs.

Another plausibility check that involves States is that no non-State Cause should only have States as Causes. If that were true, then the Cause would be true all the time and be a State itself.

6.2 Assumption

If there is not enough evidence to support a Cause, but it is clear from the Causal Sufficiency Test, that something is missing, the missing bit may be introduced as an Assumption. The Assumption should state what is assumed[16] Ideally, in an ongoing investigation, Assumptions may reveal loose ends and be resolved to be "real" Factors.

6.2.1 Countermeasures

In an analysis is finished Countermeasures can be implemented. To illustrate the effectiveness of Countermeasures they can be part of a WBG, but they are not first class citizens, as the Causes are. Including Countermeasures as Factor Types helps illustrate the way the Countermeasure would affect and prevent or mitigate an Accident.

6.2.2 Contraindication

Contraindications, like Countermeasures, are also second class citizens. They are not Factors or Causes, but in a sense, the opposite.

In an ongoing investigation there may be more than one hypothesis for the Causation of parts of an Accident. All findings that support one hypothesis go into the WBG and become Causes. But findings that challenge or contradict the main hypothesis should also be presented, as it is not helpful to exclude challenging Factors just because they don't fit in the Counterfactual Test. Ideally, like with Assumptions, these can be eliminated after an invesigation has been completed.

6.3 Check Your Understanding

Exercise 16 The following is from the summary of a U.S. National Transportation Safety Board (NTSB) investigation[17]

The truck driver was negotiating a left curve in the right lane on the connection ramp, which consisted of two southbound lanes, when the combination unit began to encroach upon the left lane, occupied by a 2007 Volvo S40 passenger car. The truck driver responded to the Volvo's presence in the left lane by oversteering clockwise, causing the combination unit to veer to the right and travel onto the paved right shoulder. Moments later, the truck driver steered counterclockwise to redirect and return the combination unit from the right shoulder to the right lane.

The truck driver's excessive, rapid, evasive steering maneuver triggered a sequence of events that caused the cargo tank semitrailer to roll over, decouple from the truck-tractor, penetrate a steel W-beam guardrail, and collide with a bridge footing and concrete pier column supporting the southbound I-465 overpass. The collision entirely displaced the outside bridge pier column from its footing and resulted in a breach at the front of the cargo tank that allowed the liquefied petroleum gas to escape, form a vapor cloud, and ignite. The truck-tractor came to rest on its right side south of the I-465 overpasses, and the decoupled cargo tank semitrailer came to rest on its left side, near the bridge footing supporting the southbound I-465 overpass.

The truck driver and the Volvo driver sustained serious injuries in the accident and postaccident fire, and three occupants of passenger vehicles traveling

[16] It could also state that the only thing known is that there is something missing.

[17] see www.ntsb.gov and search for NTSB Number: HAR-11-01

on I-465 received minor injuries from the postaccident fire. At the time of the accident, the sky was overcast, winds were calm, pavement was dry, and the temperature was about 58Â° F.

The following safety issues were identified in this investigation:

- *Essential elements of a comprehensive rollover prevention program.*
- *Rollover propensity of cargo tank motor vehicles, which provides little tolerance for operator error.*
- *Safety implications of reduced shoulder cross slope on the roll stability of heavy commercial vehicles with a high center of gravity.*
- *Lack of quality data necessary for conducting meaningful risk analyses to evaluate the crash performance of U.S. Department of Transportation specification cargo tanks.*
- *Absence of guidelines for identifying and protecting bridges vulnerable to collapse if struck by errant heavy commercial vehicles negotiating direct and semi-direct connection ramps.*

Create two WBGs from the Accident description.

Exercise 17 The NTSB safety recommendations are (among others):

- Require all intrastate and interstate hazardous materials carriers to submit annually the number and types of U.S. Department of Transportation specification cargo tanks that are owned or leased in addition to data displayed on the specification plates of such tanks and, if necessary, modify the appropriate database to accept additional data fields.
- Work with the Pipeline and Hazardous Materials Safety Administration, as appropriate, to develop and disseminate guidance that will assist hazardous materials carriers in implementing comprehensive cargo tank motor vehicle rollover prevention programs, including the active participation of drivers, dispatchers, and management through training, loading practices, delivery schedules, and acquisition of equipment.
- Require all in-use cargo tank trailers with a gross vehicle weight rating greater than 10,000 pounds to be retrofitted with a rollover stability control system.
- Conduct a comprehensive analysis of all available accident data on U.S. Department of Transportation specification cargo tanks to identify cargo tank designs and the associated dynamic forces that pose a higher risk of failure and release of hazardous materials in accidents. Once such cargo tanks have been identified, study the dynamic forces acting on susceptible structures under varying accident conditions and develop performance standards to eliminate or mitigate these risks.
- Once the performance standards in Safety Recommendation H-11-5 have been developed, require that all newly manufactured cargo tanks comply with the performance standards.

Include those recommendations that are suitable as Countermeasures. Explain how the Countermearures effect the prevention of the Accident.

Execise 18 Classify all Causes according to the Factor Type classification scheme presented in this section.

7 Continuous Functions

7.1 A Train Derailment

On the 15th of November 2004 the *City of Townsville*, a diesel tilt train, derailed near Berajondo in Queensland, Australia. One of the Factors was speed. The train was going at a speed of 112 km/h into a curve that was limited to 60 km/h. There are other Factors but in this section we want to examine continuous functions.

To illustrate the point we do the Counterfactual Test naively:

- Had the train not been travelling at 112 km/h, would it have derailed?

There are a number of possible answers to that question, depending on how to interpret it. Had the train been travelling at 113 km/h then it would have derailed. Travelling at 113 km/h is not-travelling at 112 km/h, which satisfies the constraints put by the Couterfactual Test. So the answer to the Counterfactual Test is Yes? This does not seem to be right and we would correctly point to the fact, that increasing speed increases the likelyhood of derailing. A rephrasing of the Conterfactual Test would be in order.

- Had the train not been travelling too fast, would it have derailed? No.

Is speed really a Cause?

We know for certain, that taking the curve at 60 km/h would have derailed the train. Would travelling at 61 km/h have derailed the train? We do not know, but intuitively we would say that this is close enough to 60 km/h and the train would have safely passed the curve. What speed is the limit for safely passing the curve? Do we need to know that if we want to determine if speed was a Cause?

7.2 Continous Values vs. Discrete Values

Let's take a step back and have a look at the general problem. The Counterfactual Test asks a Yes-No question. It is used to give an answer to the original question "Is it a Cause or not?", which is also a Yes-No question. But train speed is not an on-off issue. Train speed can be any number between 0 and the train's top speed. It need not even be an integer. What we need is a way to map the continuous values, such as train speed, to the Yes-No answers[18].

Intuitively we would select a point in the continuum, a speed number in the derailing train case, which separates the Yeses from the Nos. For example:

- If the train travels at or slower than 60 km/h then speed is not a Cause.
- If the train travels faster than 60 km/h then speed is a Cause.

60 km/h is an obvious candidate. First we know from experience that 60 km/h is safe, because other trains went through the curve at 60 km/h without incident. Second, there is a speed limit.

[18] Mathmaticians and Computer Scientists call this Discretization, just in case you'd like to know more about the general problem.

7.3 Back to Reality

The above mapping from speed to Yes-No, simplifies matters a little to much. Imagine that something brought the train to derail and it was traveling at 63 km/h. In court it is argued that speed was a Cause and so the driver is to blame.

No engineer would design the track without a safety margin. The train probably derails at higher speeds than 60 km/h, so is it right to put the blame on the driver for going 63 km/h[19].

Let's assume that the speed at which the train derails is 90 km/h. If we know that then we could change the mapping to

- If the train travels at or slower than 90 km/h then speed is not a Cause.
- If the train travels faster than 90 km/h then speed is a Cause.

This way a driver going 63 km/h would still be liable for exceeding the speed limit, but speed would not be a Cause for a derailment.

But is it a clear cut mapping with 90 km/h? The derailment speed may be dependend on a number of factors. The distribution of the train's mass affects its center of gravity. Environmental influences like gusts or precipitation affect train performance. Wear and tear do so, too.

All these factors may shift the derailment speed in one or another direction. In this example the shift may not be great, but we cannot assume that to be generally the case.

At different speeds speed has a different state as a Cause:

- **0 km/h - 60 km/h:** Speed is not a Cause.
- **60 km/h - lowest derailment speed (LDS):** LDS is the speed at which all environmental influences must work together in order to derail the train. From 60 km/h up to LDS the train would not derail and speed is not a Cause.
- **LDS - lowest certain derailment speed (LCDS):** LCDS is the lowest speed at which the train derails given no additional environmental factors. In between LDS and LCDS speed is a Cause, but it is not sufficient. Other Causes are neccessary.
- **LCDS - maximum speed (MS):** In this case there is no more need for external influence. Speed is sufficent as a Cause[20].

7.4 Conclusion

The train derailment is only an illustrative case. We have mapped a continuous function on three different results (see above). In principle we would have to map on four different results. We have not examined the case where a Factor is sufficient, but not neccessary. This would have complicated things a bit and there will be a section devoted to it. I do not see a situation where a

[19] We will get back to the issue of Cause verus Blame. They are not the same, even if my story seems to suggest that.

[20] Remember that Causes are necessary by definition.

continuous function would have such a result. Here we only have examined one-dimensional continuous functions, there may be cases where multi-dimensional continuous functions may have to be mapped on four results: neither sufficient nor necessary, necessary but not sufficient, sufficient but not necessary, necessary and sufficient.

7.5 Check Your Understanding

Exercise 13 A car hits a wall. The collapsible zone can only absorb a certain amount of energy. At some point the speed exceeds the absorption and injury or death to the driver is inevitable. Give reasonable mappings for

- Damage to the car.
- Injury to the driver.
- Death of the driver.

Explain your mappings.

Exercise 14 An aircraft approaches a runway to land. After touchdown the braking procedures start, but they work only partially. The pilot is required to go around[21] if he realizes that brake performance is insufficient. How does he do it? He monitors the planes performance and at some point had to decide to continue or to go around. The question is how long should he wait? There is no well defined point and there is no distinct event that signals insufficient braking.

- Give a mapping for the time between touchdown and the decision point.
- Explain how the speed of the plane on touchdown affects the mapping.

[21] Cancel the landing, apply maximum thrust and become airborne again