ISSN 2754-1118 (Online)
ISSN 2753-6599 (Print)

A Tutorial on Varieties of Possibility Analysis

Peter Bernard Ladkin

Causalis Limited / Causalis Ingenieurgesellschaft mbH, Bielefeld, Germany

Abstract

In system safety engineering and analysis, there often arises a task to enumerate all the possible ways something can happen, or all the possible ways a situation can pertain. In textbooks and guidance documents, there is often little or no indication of how one might go about this task. This tutorial identifies two common subtasks, and proposes some orderly approaches. I call it Possibility Analysis to indicate that there is a basis for common method. This tutorial makes no pretence to be a comprehensive account. It is, rather, an encouragement to develop such common method further.

Preliminary Note

The material reported in this document is the partial results of ongoing research. All of the subject matter discussed herein, in my view, merits further study and further commentary. None of it constitutes the "last word."

1 Domains in System Safety Engineering in which Possibility Analysis is Applied

This tutorial considers Possibility Analysis in three different engineering circumstances.

- Enumeration of possibilities of future system behaviour. The purpose of Possibility Analysis here is to try to identify adverse potential behaviour. This occurs in forward engineering. Following identification of unwanted potential behaviour, the forward-engineering task is usually to devise measures to avoid or mitigate the undesired behaviour.
- Accidents. An existing system has engaged in deleterious behaviour. In most cases, the consequences are apparent but the system behaviour which led to those consequences is uncertain. Nominally, forward engineering did not identify this behaviour and address its avoidance or mitigation satisfactorily. This is thus a task in lifecycle engineering. Possibility Analysis here concerns considering known facts; addressing all behaviours which can have led to those known facts, and thereby increasing the body of known facts until a unique engineering history of the accident is obtained. The engineering task is then to establish avoidance and mitigation measures in retrospect. There are many important non-engineering tasks also addressed by a successful accident analysis (precise causal description of the unwanted behaviour).
- "Environmental catastrophe/disaster". There are events which occur, which are deleterious to human and other natural lives and societies. For example floods, wildfires, earthquakes. It is a well-established field of study — there are university professorships in catastrophe/disaster anticipation and mitigation — but it is not necessarily considered an engineering speciality. These events are not reasonably

avoidable, and not necessarily physically mitigable (floods and wildfires in part; earthquakes not at all). However, they can often be anticipated and the consequences mitigated. One example is flooding in areas of human habitat. Engineering is often involved in attempted mitigation (for example, the U.S. Army Corps of Engineers building levees in the Mississippi Delta region; fire-resistance measures and earthquake-resistance requirements in building regulations), but such measures are often piecemeal and their effectiveness is limited. Recent thinking (especially in the SCSC) has suggested a more-encompassing approach to such events, called Service Assurance Engineering. In the floods I consider here, I take it that avoidance of the natural event itself is not possible, and the Possibility Analysis concerns anticipation and ways of mitigating the deleterious effects of the events.

This is not necessarily an exhaustive enumeration of all engineering circumstances in which a Possibility Analysis is called for. The three types of analyses above are *prima facie* different. However, I suggest that they share some tasks in common, namely Conceptualisation and Completeness-Assurance:

First, there is a subtask to enumerate all possibilities. This requires some sort of Conceptualisation, so that a finite, limited, cognitively-surveyable set of possibilities is laid out for engineers and others to consider. Call this the First Subtask.

Second, there is the subtask to show, to establish, that all the possibilities in the chosen conceptual scheme have indeed been enumerated. "*How do you know you have got them all?*" We could call this Completeness. Call this the Second Subtask.

Neither of these two subtasks is trivial. Indeed I have on various occasions encountered engineers who claim that one or the other is impossible. I believe strongly that neither of them is impossible, but neither are they necessarily easy.

2 Complete Enumeration of Possibilities in Forward System Safety Analysis

2.1 Preamble

In system safety engineering, two procedures are pervasively used which require a complete enumeration of possibilities for their success.

One is Failure Mode and Effects Analysis[1], FMEA, which lists the ways ("modes") in which an engineered system may fail to fulfil its intended function, and what the behaviour of the system then is (the "effect") as a result of that specific failure mode. FMEA was initiated by the US Armed Forces in 1949 through military procedures document MIL-P-1629 "Procedures for Performing a Failure Mode Effect and Criticality Analysis"[2] (US DoD 1949) (Carlsen 2012). (The addition of "Criticality" makes this technically FMECA; criticality is not always assessed.) In the wake of the "Ford Pinto affair" in the US, the Ford Motor Company adopted FMEA in the later 1970's for safety and regulatory purposes. The affair concerned the gas tank of the Ford Pinto, considered by many to be

[1] "Mode" and "Effect" are written sometimes singular and sometimes plural.

[2] These historical comments derive from Carlsen (2012) Section 1.5. MIL-P-1629 became MIL-STD-1629A, slated for cancellation in 1994 but Carlsen reports some continued use.

particularly prone to catching fire in a collision in which the car was rear-ended, and there was public controversy over the company's approach to this safety issue (Birsch and Fielder 1994). FMEA has subsequently spread throughout safety-related industries. A recent example arises from the US Coast Guard inquiry into the implosion of the Titan submersible vessel in June 2023 (US Coast Guard 2025). In the Analysis Section, Item 5.2 concerns "*Lack of Determination of Identifying Failure Points of TITAN's Design / Failure to Properly Investigate Potential Failure Points of TITAN's Design*" and states

> *There are several different established failure mode systems used for analysis. One such method, used by Classification Societies and the USCG, to systematically determine and prioritize potential failure modes is the use of the Failure Modes & Effects Analysis (FMEA). As the TITAN design utilized untested components, new materials, and unique system interactions the use of FMEA, or another established failure mode evaluation system, would have been essential. Systems like FMEA help engineers anticipate problems before they occur, prioritize risk based on the severity and likelihood of a failure, and develop strategies to mitigate those risks. …*

The main question behind a successful FMEA is usually the Second Subtask: "how do you know that you have covered all the possible failures?". There are in fact two steps to assessing this, as noted above. The First Subtask is rarely mentioned. To fulfil the Second Subtask, an argument must be given that every failure is included in one of the listed Failure Modes. "Failure ... to address all high-risk failure modes" is Mistake #2, of 10 "Mistakes", in Carlsen's Chapter 9, "Lessons Learned for Effective FMEAs" (Carlsen 2012). There is no generally-agreed approach[3].

The second example is Hazard Analysis, which is part of Risk Analysis. Hazard Analysis consists of two steps. The first is to enumerate all the possible hazardous situations which can occur during operation of a system (and also during its non-operation — in some regions, for example, insects may build nests quickly inside the pitot tubes of parked aircraft; the pitot tubes provide measurement data essential to safe flight and must be kept clean). The second is to classify the severity of the hazard if it occurs. Risk Analysis further attempts to assign a likelihood to hazardous events, and thereby to assign an overall risk to system use by accumulating the severities of hazards weighted by their likelihood of occurrence. A Risk Analysis is required in every international standard concerning safety-related systems or activities published by the International Organisation for Standardisation or the International Electrotechnical Commission, for example ISO/IEC Guide 51 (ISO/IEC 2014). It directly follows from this that Hazard Analysis is pervasive.

Again, the question arises: "how do you know that you have enumerated all the possible hazards?". This Second Subtask is addressed, as in the case of FMEA, through categorisation of hazard classes and production of an argument that all hazards have been enumerated. Again, there is no generally-agreed approach to this task.

FMEA and Hazard Analysis are related, in that FMEA can be used in Hazard Analysis, as long as it is kept in mind that by no means all hazards arise from system failures — flying through a severe thunderstorm can be hazardous for aircraft, but the hazard arises from the environment, not from the system (= aircraft+crew).

[3] The Second Subtask is referred to as "Brainstorm Potential Failure Modes", whereby a team tries to think of all the possibilities, by (McDermott et al.(2008). "Brainstorm" does not count as a method, even though everyone pretty much knows what the phrase is intended to evoke. The international standard IEC 60812:2018, does not include any information on either the First or the Second Subtask — I have personal experience of trying and failing to get the authoring committee to write something about how to try to ensure that all failure modes are considered.

Another case of a desirably-complete enumeration of possibilities arises when considering mitigation of hazards (including failure modes).

Is the enumeration of (all) possibilities always an open-ended task which has to be "brainstormed"?

No. Sometimes there are methods which achieve complete enumeration.

For example, Ontological Hazard Analysis (OHA) first construes system-environment situations in terms of a specific vocabulary, which is used to construct a logical language (in the usual sense of formal language in logic). In some circumstances, the situations thereby described are not only finite but tractably so: even though the number of sentences in the language is infinite, formal-logical reasoning can be used to group logically-equivalent or semantically-equivalent sentences into equivalence classes (call them "situation classes") and in some cases the number of situation classes is finite and tractably so. In such a case, the situation classes can be enumerated, and those that represent hazardous situations explicitly identified. This process is guaranteed to be complete (relative to the expressiveness of the specific vocabulary chosen). The Second Subtask is demonstrably accomplished.

This approach has been applied, for example, to the safety analysis of a road-rail level crossing, and to train dispatching protocol on a single-track rail line to ensure that two trains do not occupy the track concurrently (Stuphorn et al. 2009). The result was Spark-Ada code that implements a protocol guaranteed to fulfil the fundamental safety requirement (Sieker 2010).

OHA is not the only modern form of Hazard Analysis which claims to enable and, in some cases, to attain a complete enumeration of possibilities. Another is System Theoretic Process Analysis, STPA (Leveson 2011).

2.2 A Supporting Method — Ontological Analysis

General Ontological Analysis has been supported by the Safety Critical Systems Club for many years, so I take it there is little need to explain its general why's and wherefore's here. OHA is supported by a technique we call Bielefeld Ontological Analysis (BOA), which I describe here briefly and generally. It is more methodical than "brainstorming".

BOA addresses the First Subtask. It is a means of determining a vocabulary (called the "Vocabulary") of objects, types of Objects, their Properties, and Relationships to each other, as well as Assertions that are to hold between them, i.e. engineering as well as logical requirements. The Vocabulary extended with Assertions is called OPRA (for "Objects, Properties, Relations and Assertions").

Syntactically, the OPRA follows ordinary sorted predicate logic: types of object are primitive properties (unary predicates) of objects, traditionally called "sorts". BOA is an iterative process in which the OPRA is built up during the course of analysis. For example, in the single-track rail line considered by Stuphorn et al. (2009), there is in rail operations a segmentation of a line into sections called blocks. Blocks are disjoint, and the sum total of all blocks is the length of the line. A fundamental principle in two centuries of rail operations is that no two trains shall be present in the same block (except under carefully delineated and specially-controlled circumstances). So here are two types of object: *Train* and *Block*. A Train (an object of type *Train*) may be *In* a Block, or *Out* of a Block, or *Transiting* (which one could further define as In two adjacent Blocks). Being In a Block or Out of a Block is a two-place relation between a Train and a Block.

Some logical relations should be immediately clear. Two Blocks can be *Adjacent* or *Separated* (⇔ NOT *Adjacent*). A Block is either a *Terminus*, adjacent to one other Block, or is *Continual*, *Adjacent* to precisely two other Blocks. A Train is either *In* exclusively one Block, or is *In* precisely two Blocks which are *Adjacent*, and is thereby *Transiting*. The language of logic can express fixed-block operations in such a way that one can reason rigorously about them.

The fundamental safety principle can be stated: Two distinct Trains T1 and T2 are not *In* a given Block B. This is, of course, an assertion. The development in Stuphorn et al. (2009) shows how this logical Vocabulary and the associated safety statements and operational requirements (the OPRA) may be extended, in the course of developing a dispatching communications protocol that demonstrably fulfils the fundamental safety principle.

Blocks are in this example fixed (and have been for centuries) but modern train operations have considered so-called “moving blocks” (roughly construed as specified space around trains) for many years.

Use of an explicit, constrained and incrementally developed technical Vocabulary (the First Subtask) means quite often that the number of things that can be said is limited in a way that enables the analyst to enumerate them exhaustively (Stuphorn et al. 2009). That is, the Second Subtask is demonstrably achieved. This is why BOA is a supporting technique in Possibility Analysis. An introduction to OHA, in the hazard analysis of a pressure tank, and of an (abstract) automotive communications bus, may be found in Ladkin (2017) Chapters 5,6,7. BOA has also been used to help define Use Cases for standardisation activities in Active Assisted Living and eMobility (Kaufhold et al. 2019).

Using BOA in such a manner cannot exclude all earthly possibilities, of course. Besides the possibility of a Train colliding with another Train in a Block on a track, the Train could hit a fallen tree, or a load-carrying helicopter flying overhead could drop its load onto the track. Neither of those two events can be expressed in the Vocabulary developed in Stuphorn et al. (2009). But, if used effectively, BOA can exclude (or provide incentive to mitigate) all possibilities describable in Vocabulary and this is for many engineering tasks an effective limit on what the specific-task engineering can do. (Rail engineers, for example, do not engineer helicopter load-carrying operations, nor their routes of flight. In certain circumstances, for example heliports at railway stations, there might be a case for joint rail-aviation engineering consultations.)

3 Accident Analysis — Motivation for Possibility

3.1 Accident Analysis

In the literature on how to analyse unintended and unwanted behaviour of engineered systems — accidents and incidents — various techniques are described, such as Fishbone/Ishikawa diagrams, 5 Why's, the Multilinear Events Model, Accimaps, STAMP/CAST[4] and WBA[5] (see IEC 62740:2015). All of these descriptions assume that there is a plethora of facts — events and states which are known rather than just surmised — available to investigators. Which, at the start of an investigation, there isn't. Agencies

[4] Systems-Theoretic Accident Model and Processes/Causal Analysis based on STAMP

[5] Why-Because Analysis

tasked with investigating accidents write field investigation handbooks incorporating their procedures, which are often publicly available, e.g. (US Air Force 2021). Such handbooks usually detail how they commence an investigation, but are primarily organisational guidance. There seems to be a dearth of intellectual approaches to how to commence an inquiry, when few facts may be known; on how to organise sparse information, and use it to reach early and reliable (but usually insufficient) conclusions.

One reason for wanting early, reliable but incomplete conclusions is to advise operators of similar engineered equipment as soon as possible of problems and offer or mandate prophylactic guidance (as happens in commercial aerospace with Emergency Airworthiness Directives). The case study below of the 2025 Air India accident describes one such approach to organising sparse material and effectively drawing conclusions and managing reasoning. It deserves the name of Possibility Analysis.

The First Subtask appears to be less important in aviation accident analysis, since the Vocabulary for detailed parts of aircraft systems more or less exists (a possible exception may be Human Factors, which has a number of different conceptualisations, each with advantages and disadvantages). However, First-Subtask issues can still arise, for example there was in the example below some professional-forum discussion of a specific engine-control function, TCMA[6], which some contributors believed could, in concert with a sensor malfunction, have been responsible for the reduction of thrust after lift-off (see the discussion below). All engine control functions on this aircraft are software-based, so this would be an example of a failure in the software-based control system — of which there were potentially many. An FMEA of the software-based control could have, and one hopes would have, included TCMA malfunction (I do not know). I thus accrued this specific concern to be a potential "Failure of Software-Based Engine Control", which was high on my list of causal candidates before the Preliminary Report was published (Government of India 2025). I suggest that this conceptualisation is more appropriate engineering-wise than focusing on one controversial function, for software failures have a number of similar characteristics which do not depend on the specification of the thereby affected function (and, conversely, functions implemented in software can fail, even though the software executed them as specified and programmed).

Many incident analysts like to categorise and discuss what they think is likely, and what they think is unlikely, and what they think is plausible. The disadvantage of such an approach is that incidents and accidents are by their very nature unlikely events, and human intuition is not good at characterising likelihoods relative to an unlikely event (likelihoods conditional on unlikelihood). This leads to very different analyses from different analysts, and there are few effective ways to compare them.

Other analysts like to imagine ("construct") a set of scenarios, complete or complete-ish stories about how an accident may have happened, consistent with the sparse information which is known. The disadvantages of this approach are that, (a) in a state of sparse knowledge, any given scenario involves a plethora of suppositions and there is no good method for comparing one plethora of suppositions with another, which would be needed in order effectively to compare scenarios; (b) imagination can be lacking — many possible scenarios can be missed; (c) in a situation of sparse knowledge, there are simply too many scenarios feasibly to consider (intractable combinatorial complexity).

Using Possibility Analysis, as understanding of the event progresses, then usually the possibilities coalesce into a (much lower) number of scenarios, coherent and more

[6] Thrust Control Malfunction Accommodation

complete stories about what might have happened, and it is at that point much easier to judge the likelihood of a particular event or state occurring relative to a scenario. But these scenarios are built up from still-incomplete knowledge when it is nevertheless sufficient to mitigate combinatorial complexity, which at the beginning of an inquiry is not the case. It is in this initial stage that I find the structured enumeration of possibilities along with their (possible incomplete) evidence most helpful.

3.2 Possibility Analysis for Accidents

A Possibility Analysis of an accident proceeds in stages. At a given stage, (a) there are some indisputable facts (what we know). Let us call these Facts(A). Then (b) there are things for which there is some evidence, but not necessarily conclusive (things which are likely, but we don't know for sure). Let these be Hypotheses(B). And then (c) there are things which we know were not the case (what didn't happen). Let these be Excluded(C). I call members of these sets, as well as Possibilities(D) (below), *items*.

Possibility Analysis is an iterative process. At a given stage, it takes Facts(A), Hypotheses(B), and Excluded(C); and (d) enumerates all possibilities consistent with Facts(A) and Hypotheses(B) (including some which may be inconsistent with items in Hypotheses(B), which are at this stage not confirmed), paying particular attention to how they might be constrained by Hypotheses(B). Step (d) is more art than science. An analyst has to find a way of describing all possibilities without these becoming too detailed and cognitively incomprehensible. That entails abstraction of some kind. Let the result of this step be Possibilities(D).

Step (d) results in a framing of the progressing inquiry which, in the best situation, gives hints about what to focus on next, to see how and where more facts can be added (Facts(A) increases), or connections between items in Hypotheses(B) and Facts(A) or Possibilities(D) can be further elucidated.

Step (e) is optional pro iteration. It consists in looking at the items in Possibilities(D) and elucidating the possibilities for those items, and maybe iteratively.

And then repeat.

It should be clear, in particular through Step (d), that different analysts may produce different analyses, depending on how they prefer to characterise possibilities. (This is additional to analysts deriving different Facts(A) and Hypotheses(B) depending on differing judgements.)

This is not all. Evidence for the judgements (what items are in Facts(A), Hypotheses(B), Excluded(C), Possibilities(D)) and the reasoning behind those judgements must be retained.

First, *evidence collecting*. Collecting facts, hypotheses and excluding some scenarios must be supported in an analysis by the evidence for them. Evidence usually consists of facts (which will be in Facts(A)) plus some reasoning about them. In the case of items in Hypotheses(B) this reasoning may also include other items in Hypotheses(B). It should be clear that keeping both the evidence and the reasoning behind assignments of items to categories needs to be accomplished in order to call this process "analysis". What does this Reasoning/Evidence look like? What is its "data type"? Since the products of analysis are here all denoted by terms, let the denotations for evidence be respectively Evidence(Facts(A)), Evidence(Hypotheses(B)), Evidence(Excluded(C)), and Evidence(Possibilities(D)). Each entry in one of the Evidence sets must contain (i) an ID of the item for which the evidence pertains, (ii) IDs of (pointers to) items in Facts(A),

Hypotheses(B), Excluded(C), and Possibilities(D), which are adduced as evidence, and (iii) reasoning which is used about items in (ii) that the analyst claims establishes the item (i) for which the evidence pertains. An example of such reasoning might be the application of the Counterfactual Test as used in WBA, especially if the goal of the analysis is indeed to be a WBA, represented by a WBG[7].

Second, *established reasoning*. At any point, logic or mathematical reasoning or reasoning from established parts of physical science may be used to restructure the items or to infer new items.

A brief comment now about the structure of the named sets. Facts(A), Hypotheses(B), and Excluded(C) consist of straightforward assertions of states and events during the incident. An item in Possibilities(D) consists of (a) an ID of the item for which the possibilities are being enumerated, and (b) a collection of possibilities (events and states) which causally result in the item occurring. An item in any of the evidence sets consists of (i), (ii) and (iii), as explained in the previous paragraph (but one).

This may seem like a lot of bookkeeping for a task which many experienced observers perform without such bookkeeping. There are four reasons for such bookkeeping which I find compelling.

First, there are criteria for items to be placed in the categories. At any stage, it can be asked why the items are placed in the categories in which they are placed. A *Hypothesis* can't transmute into a *Fac*t just by being repeated a large number of times by many analysts, which seems to me often occurs in discussions.

Second, for items in Possibilities(D), it can be asked at any stage whether the enumerated possibilities are indeed all there are (Second Subtask concerns). Furthermore, when possibilities are restructured, then an item <*itemID, {set of old possibilities}* > is replaced in Possibilities(D) with a new item <*newitemID, {set of new possibilities}* >. The old possibilities really do go (they might come back later, though) and the new ones are their replacements, to be further considered. Old possibilities thereby don't "hang around" in the discussion space. This is a practically important discipline in analysis.

Third, the evidence for the categorisations is collected and available. The question amongst analysts "why do you think that?" is replaced by the questions "Why do you place that item in that category?" and "What is the associated evidential reasoning for that decision?". The reasoning part of Evidence can become quite involved quite quickly. In my experience, it is important for an analyst to be able reliably and quickly to answer the question "what am I claiming and why am I claiming it" at any point in an analysis. That information is given — and held — in the Evidence sets.

Fourth, in my experience, different analysts can quickly come to differing judgements concerning items in Facts(A), Hypotheses(B), Excluded(C), and Possibilities(D). To discuss and clarify the differences, and reasons for them, it helps to have the items laid out in these categories and the reasons laid out in the Evidence sets.

3.3 An Example

In the recent crash of Air India Flight 171 in Ahmedabad on June 12, 2025, it was almost immediately suspected by many analysts that (I) there was inadequate thrust+lift to establish a positive rate of climb (RoC) after lift-off (derived from viewing the videos),

[7] Why-Because Graph

and (II) there was evidence of a substantial electrical-system failure (people thought they saw a RAT[8] deployment, and performed audio spectral analysis on the sound from one video which was consistent with RAT deployment and inconsistent with the sound spectrum when RAT is not deployed. There are specific conditions under which the RAT automatically deploys, and they are all connected with electrical system failures in some way).

One video, from CCTV beside the runway and behind the departing aircraft, shows the aircraft attaining about one and a quarter wingspans of altitude before settling. Since the wingspan of the Boeing 787-8 is 197 ft = ~200 ft, we can conclude that the *attained altitude Above Ground Level (AGL) was some 250 ft* (this we put into Facts(A)). Here, though, there was some work to be done reconciling alternatives — the Indian authorities said that the attained altitude was reported as 625 ft. How? That data must have come from an ADS-B[9] report by the aircraft on take-off (it didn't come from any ground measuring instruments because there aren't any). But ADS-B reports International Standard Atmosphere (ISA) values related to Mean Sea Level (MSL). Airport elevation is 189 ft = ~ 190 ft MSL. But QNH (the actual air pressure corrected to MSL, which is needed by pilots in order to set the barometric altimeter) was 1000 hPa, not standard-atmosphere 1013 hPa. 1 hPa is equivalent to about 30 ft of altitude, so a correction of ((1013 – 1000) x 30) ft = 390 ft must be applied, and added to the airport elevation, which gives an airport "pressure elevation" (elevation above MSL corrected for non-ISA pressure) at the time of take-off of 580 ft. So the ADS-B report of 625 ft only represents being 45 ft AGL. The aircraft was much higher than that, as shown in the video.

So *inadequate thrust+lift to establish a positive rate of climb* goes into Facts(A) and *RAT deployed* goes into Hypotheses(B). For some analysts, *RAT deployed* went into Facts(A).

Other things went into Facts(A). *Take-off roll appeared to be normal*. Evidence? First, visually, from the videos. Second, validated from data obtained from ADS-B transmissions of the aircraft, along with comparisons of the take-off roll with previous take-off rolls by the aircraft in question at that airport, compiled and made publicly available by the commercial organisation FlightRadar24.

There were no strikes of objects; in particular there was no bird strike in the engines. Evidence? The runway was searched and no remains were found. Second, there was no evidence of the smoke and flame associated with such a strike on the take-off video. So *bird strike* and *object strike* go into Excluded(C) and the evidence into Evidence(Excluded(C)). *Normal take-off roll* goes into Facts(A), as well as additional confirmation as and when that becomes available.

The *inadequate thrust+lift* in Facts(A) yields three possibilities, by simple logic: *inadequate thrust, inadequate lift, inadequate thrust and inadequate lift*. These three go into Possibilities(D): the entry thus reads *<inadequate thrust+lift, {inadequate thrust, inadequate lift, inadequate thrust and inadequate lift}>*

Let us perform Step (e). Take one of these possibilities from the previous paragraph: *inadequate lift*. There seem to be three possibilities that can cause this on a visually-normal take-off roll. One is *inadequate velocity on rotation*; one is *inappropriate configuration of high-lift devices (flaps and slats)*. The third is, of course, both of these, but this is logically included in both these possible situations, so there is no need to

[8] Ram Air Turbine

[9] Automatic Dependent Surveillance-Broadcast

consider it separately. So <*inadequate lift, { inadequate velocity on rotation, inappropriate configuration of high-lift devices }*> also goes into Possibilities(D).

We already have *take-off roll appeared to be normal* in Facts(A). It follows from this by "established reasoning" that there was *adequate velocity on rotation*. So we place *adequate velocity on rotation* also into Facts(A). A picture of the left wing lying on the ground after the crash shows, according to some analysts who would be expected to know, that *at least Flaps 5* was configured on the high-lift devices. Another picture of the leading edge of the right wing shows part of the leading-edge slat extended, and part missing but whose actuator is shown extended. Figure 7 in the Preliminary Report of the AAIB shows the outboard right wing with a flap clearly extended (Government of India 2025). So, depending on an analyst's judgement, *at least Flaps 5* goes into Facts(A) or Hypotheses(B), and those two pictures with the above commentary on the post-crash state of some of the flap and slat segments go into the associated Evidence set.

Furthermore, if at least Flaps 5 is not configured at take-off, the flight deck annunciation systems would be screaming at the CRW[10] and some normal activity to commence take-off roll would be inhibited. So we can consider putting *CRW commenced take-off while ignoring warnings* into Hypotheses(B) or into Excluded(C) depending on our assumptions.

Does *inadequately configured high-lift devices for take-off* go into Excluded(C)? This likely depends again on what the analyst has so far considered. If you have put *at least Flaps 5* into Facts(A) then you must put *inadequately configured high-lift devices for take-off* into Excluded(C).

The meteorological data (*QNH of 1000 hPa, compared with QNH in a standard atmosphere of ~1013 hPa; temperature of 39°C, wind velocity*) also needs to go into Facts(A). With Flaps 5 configuration, pilots who are type-rated on the Boeing 787 aircraft confirm that there is more than enough thrust nominally available to achieve and maintain positive RoC. So if you have *at least Flaps 5* in Facts(A), you can also *put more than enough thrust nominally available* into Facts(A).

It follows from this that there was *inadequate thrust at or shortly following lift-off*. Because if *at least Flaps 5* is in Facts(A) then, by the previous paragraph, so is *more than enough thrust nominally available* and it follows from this that that nominal thrust was not available. By "established reasoning" it follows that there was *inadequate thrust at or shortly following lift-off*.

Further, a back-of-envelope calculation by an aerodynamicist colleague showed that the aircraft could not attain the observed altitude of 250 AGL purely with the kinetic energy available at lift-off. (Such a gain in altitude purely by exchanging kinetic energy for potential energy is termed a "zoom climb".) This entails that some thrust was available at lift-off at typical lift-off speeds. So one can take the Facts(A) item *inadequate thrust at or shortly following lift-off* and specify it further: *adequate thrust at lift-off and reduction in thrust shortly following lift-off*, with the reasoning above being placed in the appropriate Evidence item.

I continue this example. There is a function called TCMA, which in one realisation is patented, that detects any discrepancy between commanded thrust (thrust-lever position on the flight deck) and actual thrust (from the engine) whilst the aircraft is on the ground, and reduces actual thrust to idle. TCMA is mandated on some aircraft by airworthiness criteria, and it is implemented on the Boeing 787-8 Full Authority Digital Engine

[10] Aircrew, i.e. Pilot Flying and Pilot Monitoring

Controllers (FADECs), built by Safran. There was considerable discussion on the pilots' forum PPRuNe[11] whether the TCMA could have somehow been involved in a reduction of thrust in both engines to idle shortly after lift-off (according to some discussants, this would involve the "ground sensing" part of TCMA fulfilling the conditions for "the aircraft is on the ground", and so on).

Suppose *reduction of thrust shortly after lift-off* is in Facts(A). Give this item the ID *RedThr*. Then, inquiring how *RedThr* can come about, it is most likely that this was commanded by the FADECs. Give this the ID *CommFADEC*. The reason for this is that the FADECs are the control devices. So, into Possibilities(D) goes the one pair <*RedThr, CommFADEC*>. The assertion the FADECs control the engines is placed in an appropriate item in Evidence.

FADECs are also digital computers. Such a thrust reduction may have been *commanded by the thrust lever position, or commanded by activation of fuel cut-off switches, or commanded by activation of the fire switches* (that is, the flight deck crew commanded it by doing one or more of those three things, or *a malfunction occurred on the signal path between these flight-deck controls and the FADECs*), or it might have been *commanded by some other logic in the FADEC*. In particular, thrust levers could be set to take-off power, and no flight-deck controls moved or activated, and yet the FADECs command the thrust reduction. You might well want to call this a *spontaneous FADEC command*. So into Possibilities(D) goes the following pair, consisting of the ID of the event and the set of possibilities that can have caused that event: <*CommFADEC, {commanded by the thrust lever position, commanded by activation of fuel cut-off switches, commanded by activation of the fire switches, commanded by activation of the fire switches, spontaneous FADEC command}* >.

3.4 Further Information

On 11th July, 2025, the Indian Air Accident Investigation Board published the Interim Report on the accident, which is required by ICAO Annex 13 within 30 days of the accident. It included the rather startling information that the fuel cut-off switches were both set to cut-off within 1 second of each other, within 3 seconds of lift-off. The Board know this from the flight data recorder. The record of the switch position is transmitted from the switch to the data recorder; furthermore the signal paths from engine controls (including FADEC) to each engine are entirely separate — there is no possibility that I can see whereby fuel switches were set (and left) to run but each engine separately, as well as the data recorder, recorded a cut-off command.

So <*CommFADEC, {commanded by the thrust lever position, commanded by activation of fuel cut-off switches, commanded by activation of the fire switches, commanded by activation of the fire switches, spontaneous FADEC command}* > comes out of Possibilities(D) and <*CommFADEC, commanded by CRW activation of fuel cut-off switches* > is placed into Facts(A).

This now fully explains the behaviour of the aircraft. It remains to be seen whether the behaviour of the CRW can satisfactorily be recounted. There are three possibilities (namely that a CRW member did this deliberately; that a CRW member did this inadvertently while intending to do something else; that a CRW member did this while

[11] Professional Pilots' Rumour Network

experiencing a fugue), and I am sceptical whether there is any way in which one or other of these can be rigorously supported, since the CRW is no longer with us.

3.5 Summary of Example

We have seen how the Possibility Analysis deals with *reduced thrust shortly after take-off* in the accident event of AI171, and further what the possibilities are that would have caused that to have happened. The Evidence for the various assertions has been systematically collected and retained. Analysts may differ on whether they consider particular evidence conclusive or merely suggestive, and therefor into which category they place the associated assertions. The structure of a Possibility Analysis (Facts, Hypotheses, Excluded, Possibilities, and the Evidence sets) is a systematic way of organising an inquiry from the start onwards, and also enables a direct comparison of different approaches by different analysts. This is advantageous in the early stages of analysis, especially in comparison with the more common approaches in which analysts propose scenarios and argue about their respective merits, or in which they attempt to judge the relative "likelihood" of various hypotheses concerning what happened.

4 An Example in "Service Assurance Engineering" — Flash Flooding and Warnings

4.1 Flash Flooding

Flash floods are floods in localised areas which arise suddenly, within seconds to minutes or a few hours, usually because of sudden very heavy rainfall channelled into a relatively narrow waterway. Such waterways are often valleys and are often populated, historically because of the advantages of proximity to regularly flowing water, e.g. the Ahr Valley in the Eifel mountainous terrain west of the Rhine in Germany in 2021, and the Valle Maggia north of Locarno in Ticino in Switzerland in 2024, but in the case of the July 4th, 2025 flood on the Guadalupe River in Kerr County in the Texas Hill Country, many people were there because of recreational visits on a holiday weekend.

The phenomenon itself, of heavy rainfall causing a sudden flood, is solely environmental and cannot be avoided. However, its effect on human society can be mitigated by evacuating all people (animals are harder to evacuate) and vehicles from the area likely to be flooded. The safety task is thus straightforwardly phrased. But executing it effectively is often hard.

The potential for flash flooding at a particular location can be predicted in advance through orographic analysis of the watershed. What cannot be predicted with any level of accuracy is the exact location (say, within some tens of kilometres) of a heavy rain shower, nor its quantity, nor its rate. When rainfall starts in a particular location, its rate can be measured accurately enough by radar, if there is radar (and thereby quantity can be assessed by integrating rate over time). Water takes some time to flow from its surface landing point, down to the watercourse, and thence downstream, maybe 30 minutes, maybe some hours. But travel it will, in the orographically determined direction.

I have already considered in detail the German-Belgian flooding of July 2021 in another venue (Ladkin 2022). I will consider here in some detail the Texas Hill Country Guadalupe

River flood of July 4th, 2025. I also refer (for I only had access to one account) to the Valle Maggia flood in Ticino, Switzerland of 29th June, 2024.

First, some details about the geographical extent and origin of the triggering rainfall, as well as details of the terrain.

The 2021 German-Belgian floods were caused by a massive build-up of atmospheric moisture that had been noted, and the information passed on, by the European Centre for Medium-Range Weather Forecasts (ECMWF n.d.), an intergovernmental organisation with three sites in Reading, UK, Bologna, Italy and Bonn, Germany, whose products are used worldwide (including in the US — they occur in some of the on-line articles of the Guadalupe-River analysts, below). The notice was initiated by the ECMWF European Flood Awareness System (EFAS) tool some four days before the event. The rainfall event itself was spread over a very large geographic area, at least some 80 km x 80 km (the heaviest rainfall was measured in Hagen, some 100km away from the most badly affected areas of the Ahrtal, the valley of the River Ahr, which flows through the Eifel to the east, eventually meeting the Rhine). In the German event, there was just over half the total precipitation per location (150 mm — 180 mm over the area) as in the Guadalupe valley event (where some 10" (= 250+ mm) was measured at some locations over the course of 3 or so hours).

In contrast to the German-Belgian event, the Guadalupe event was very localised. (Alan Gerard notes that, had the rainfall occurred some 10 miles to the southeast, the Guadalupe watershed would not have been affected (Gerard 2025d)).

The German rainfall came from a stationary, but geographically widespread, air mass. The Guadalupe event was the result of a mesoscale convective vortex, and a south-westerly low-level jet stream (at 850mb = ~ 5000 ft altitude) meeting a warm and wet remnant of a tropical storm coming north from Mexico. The Valle Maggia event was, according to eyewitnesses, the result of a continuous series of thunderstorms occurring over a period of many hours in a specific location (namely over the mountains surrounding the narrow Valle Maggia).

The Ahrtal (valley of the Ahr) was not the only watershed affected in the 2021 German-Belgian event — the Vesdre and Hoëgne in Belgium flooded to the west, and the Erft to the north — but it was the longest. The Ahr itself is some 89km long (Ahr (en) n.d.) and heavy precipitation occurred along its length, as well as to west and the north of it. Its watershed covers almost 900 square km (Ahr (de) n.d.). The highest point of the Eifel range is 746.9 m above sea level (ASL); the Ahr source is at an elevation of 474 m ASL and it joins the Rhine at 53 m ASL. The Ahrtal is appropriately described as “steeply hilly” rather than mountainous. The south fork of the Guadalupe River is some 37 km long (WaterwayMap.org n.d.). Texas Hill Country is hilly but in comparison with the Ahrtal not steeply so. The Valle Maggia is some 50 km long (Vallemaggia (it) n.d.) and is surrounded by mountains.

4.2 The 4th July Guadalupe River Flash Flood

In the early morning of Friday, July 4th, 2025 (US Independence Day), some 9" — 10" of rain (up to ~ 250 mm) fell in the watershed of the southern fork of the Guadalupe River in Kerr Country, Texas, in the Texas Hill country. This area is apparently known in local parlance as “Flash Flood Alley”, and there is a book on various historical floods which have occurred (Burnett 2008). Many people were making recreational visits to the river valley for the long weekend. There was a girls' camp, for Christian girls, Camp Mystic, on the banks of the river some 6 to 7 km up the South Fork from the confluence of the forks

near Hunt. On the Guadalupe river there are some 19 camps or recreational facilities (Hutchinson 2025)[12]. Besides these recreational sites it would be appropriate to characterise the countryside upriver of Hunt as sparsely populated. Some 8 km or so downstream of Hunt is another community, Ingram, and some 8 km or so beyond that the county seat of Kerr County, Kerrville.

There was a flash flood originating in the watershed of the Guadalupe South Fork. The river gauge at Hunt rose from 7.7 ft with 8 ft^3/sec flow at 01:10 local time (UTC–5) to 29.45 ft with flow of 120,000 ft^3/sec at 04:35, at which point the gauge failed (Gerard 2025a). Alan Gerard describes this as "*more water flowing than the average flow over Niagara Falls*" (Gerard 2025a). The Kerr County Emergency Management Director cited even larger flows of 220,000 ft^3/sec (Hutchinson 2025). The Camp Mystic director, Dick Eastland, lost his life trying to get the girls at his camp out of harm's way, but 27 of the Camp Mystic girl visitors and counsellors died anyway. The Camp had been established in 1926, 99 years previously. Eastland and his wife Willetta ("Tweety") were the third generation of the family who had bought the camp in 1939, and they had been the Directors since the 1970's (Graham 2025). With that level of experience with this site over almost 100 years, it makes clear what a uniquely devastating event this particular flood was. Reports have over 130 people killed or missing in the events, and 108 in Kerr County alone.

Laughlin Air Force Base is situated some 150+km southwest of Hunt near Del Rio on the Rio Grande, the border with Mexico. Laughlin AFB has weather radar which shows radar reflectivity and radar-estimated total rainfall (Gerard 2025a). The Multi-Radar Multi-Sensor product MRMS of the National Severe Storms Laboratory in Norman, Oklahoma (Lowry 2025) showed for the three-hourly rainfall 01:00—04:00 local time 6" — 10" of rainfall "*almost perfectly aligned with the south fork of the Guadalupe southwest of Hunt*" (Gerard 2025a). There is an MRMS product called FLASH Unit Streamflow that estimates runoff and inundation on watersheds from measured rainfall, which showed "*values indicative of potentially catastrophic flash flooding"* (Gerard 2025a).

The National Weather Service has a Weather Prediction Center in College Park, Maryland, which issues "mesoscale precipitation discussions" (MPDs). They issued a number of these before the event, and as the event unfolded. One, from 2025-07-03 at 21:00, shows a "Mesoscale Convective Vortex" (MCV), a remnant of thunderstorms in the Big Bend area west, and a "south-westerly 850mb jet", a jet stream at about 5,000 ft (850 millibars in the International Standard Atmosphere), and a comment box saying "*Storms Containing 3"/hr Rainfall Rates Likely To Cause Areas of Flash Flooding*"[13] (Gerard 2025a). What is not shown, but was known, is that the remnants of Storm Barry, which had been over the Gulf and turned north over Mexico, were due to meet this MCV and jet stream exactly at this time. Weather balloon data from Del Rio (presumably launched from Laughlin AFB) on Thursday July 3 showed "*record levels of moisture present in the upper atmosphere above Central Texas*" (Holthaus 2025). These are known kinds of weather phenomena convergence over Texas (Lanza 2025). The High-Resolution Rapid Refresh (HRRR) model from the NOAA early on Thursday July 3 predicted 10" — 13" in some parts of Texas, and up to 20" by Thursday evening (Lanza 2025). The NOAA HREF model, which uses the "probability matched mean" method to try to identify higher-risk areas for heavy rainfall, also indicated 10" or more in spots over Texas, from Thursday morning onwards

[12] Hutchinson's ABC News article reports the testimony of the Kerr County Emergency Management Director, William Thomas, to the Texas Senate

[13] A BSKY message from Peter Mullinax, who works at the WPC, explicitly included in (Gerard 2025a)

(Lanza 2025). So the high-resolution models were "getting it right", but it is not clear who was looking at them (apart, one presumes, from NWS specialists). The National Weather Service office in New Braunfels, Texas, near San Antonio, engaged in "surge staffing" for the evening of Thursday July 3rd, involving five overnight staff members on duty rather than the usual two (Lowry 2025).

The National Weather Service issued a flash flood warning at 01:14 local time on July 4th, including a notification of "*IMPACT ... LIFE THREATENING FLASH FLOODING...*" and an Impact Based Warning (IBW) of "*FLASH FLOOD DAMAGE THREAT... CONSIDERABLE*" of which the keyword "CONSIDERABLE" triggered a Weather Emergency Alert (WEA) cell broadcast to mobile phones in the area[14] (Gerard 2025b). Other warnings were issued at 01:46, 03:19, 03:35 (in which it was extended to 07:00) and 04:03, in which the IBW was upgraded to "CATASTROPHIC" and it was indicated that the Guadalupe river at Hunt was flooding (Gerard 2025a). Some on vacation in the area have noted that they actually received these WEAs on their mobile phones (Gerard 2025b), but mobile phone reception further up the Guadalupe watershed is said to be patchy.

There is an NWS program called StormReady. To be StormReady, "*a community must establish a 24-hour warning point and emergency operations center and have multiple ways both to receive severe weather warnings and to disseminate them*." (Gerard 2025c). Kerrville and Kerr County, Texas are not "StormReady communities." (Gerard 2025c).

It thus seems as if NWS and their meteorologists using NOAA products were aware in advance of potential rainfall of the magnitude which in fact occurred, and were aware of actual rainfall in real time, sufficient to issue advance warning (1—3 hours, depending on where you were on the watershed) of "*life threatening flash flooding*" with "*damage*" estimated to be "*considerable*", sufficient to trigger a cell-broadcast warning to those in the region whose phones were switched on. Did these warnings get through to Kerr County officials, and to residents and visitors in the impacted areas? Gerard suggests inadequately to trigger the appropriate evacuation activity (Gerard 2025d). This seems to be confirmed by Thomas's testimony (Hutchison 2025).

One of the potential reasons for complacency might be "alert fatigue" — people receiving many alerts when "nothing happens". How often does NWS issue WEAs and suchlike for such events in the region? Gerard: "*Over the last 5 years dating back to 2020 and prior to the event on July 4th, there were only 8 flash flood warnings issued for Kerr County: 1 in 2020, 1 in 2021, none in 2022, 1 in 2023, 2 in 2024, and 4 so far this year. Considering we are talking about an area known as "flash flood alley" it is hard to see how this could be considered overwarning that would cause alert fatigue*" (Gerard 2025d). For those who might not want to rely on mobile-phone alerts, there is another option: *"……NOAA Weather Radio. Weather radio receivers can be purchased relatively inexpensively, and programmed so that you only receive weather warnings for the county or parish you live in*." (Gerard 2025d).

Flash flooding of a similar nature, apparently unanticipated by the impacted communities, occurred on July 14th 2021 in the Eifel hill country in Germany, and the westwards watershed into Belgium. Amounts of water were lower (10", reported in the Guadalupe event, is 254mm, reported over 3 hours, and the amounts reported in the Eifel event were of the order of 160—180mm in 24 hours). But the hills and valleys are steeper and narrower, and the community memory for such events goes back many hundreds of years; some late medieval buildings were damaged, some 18th-century buildings partially

[14] Alan Gerard includes the text of the message explicitly in (Gerard 2025b)

destroyed. The potential for extreme rainfall in some area was foreseen days in advance by the ECMWF, but the resolution of predictions is rarely lower than 100 km in any direction — indeed, as noted above, in the German event the highest rainfall was 100 km away from the Eifel, to the northeast, in Hagen near the Sauerland. In the Texas event, as Gerard remarks, *"...if you shift this rainfall maximum just 10 or so miles to the southeast, it would have occurred in the Medina River basin, and the Guadalupe River would not have even seen any significant rise in river levels*." (Gerard 2025d).

There was an event in the Ticino Alps in Switzerland on 2024-06-29 in which a whole narrow valley, the Valle Maggia, suffered flash flooding and landslides, caused by a convective event that stayed stationary over the valley for many hours on a Saturday (Goodman 2025). This particular event involved at least one experienced meteorologist, who had developed software for MeteoSwiss to predict and monitor such events, who was participating in a football competition and a concluding evening concert. There were far fewer casualties in this event than there were in the Eifel in 2021 or in Texas Hill Country on July 4th 2025.

4.3 Common Themes and Important Questions Concerning Flooding

With this example, there are quite a lot of items to put into Facts(A). What do we want to learn from such events? With aircraft accidents, we want to learn how possibly to avoid them in the future. We cannot avoid such atmospheric phenomena as heavy rainfall; but we can avoid human casualties by reacting in time and evacuating impacted areas beforehand. There thus arise questions which can be addressed with Possibility Analysis. But there is a fair amount of groundwork to do before we arrive at that.

Some common themes (items to put into Facts(A)) are:

- such events cannot currently be predicted with an accuracy sufficient to warn specifically the community which is impacted;
- flash flooding is topography and watershed dependent and impacted areas for specific levels of water flow can be identified in advance;
- general warnings can be issued, but specific warnings for specific watersheds cannot currently be made with moderate-to-high accuracy;
- the amount and extent of moisture in an atmosphere can be accurately measured, as can the temperature of air masses;
- air masses can be accurately distinguished in mesoscale-physically relevant ways: MCVs, jet streams, storm remnants and so on;
- when a rainfall event commences, it may be seen and accurately assessed on radar; and
- real-time assessment using radar and other sensors allow meteorologists and hydrologists to issue specific warnings for specific watersheds 30 minutes to 3—4 hours in advance, depending on the location of the rainfall and local topographic characteristics.

The important questions are:

- how to communicate warnings from weather specialists to impacted communities within sufficient time for the communities to engage in damage/injury-preventative action?
- how to facilitate damage/injury prevention and organise rescue; this includes planning to move susceptible populations out of harm's way; identification of susceptible structures in advance; post-event identification of damaged and unsafe structures (buildings and engineered structures at risk of further collapse) and unsafe environmental features

(unsafe terrain susceptible to slippage or further flooding and structures in the slippage path)?
- how to plan recovery (debris removal, restoration of interrupted services such as electricity, water, and electric/electronic-based communications, provisional accommodation for displaced persons)?

Let me concentrate here on two aspects. First, communication. Second, immediate community anticipatory damage/injury prevention on receipt of warning.

To deal with the second aspect first. There is involved a mixture of science, engineering and political and community action.

- Science looks at the topography and identifies areas susceptible to flooding at particular water levels and flow rates (some might prefer to call this engineering). Let me call this "Susceptibility Analysis".
- Engineering identifies reliable ways of moving people out of those susceptible areas at short notice (minutes to a couple of hours). This is often harder than it sounds — finding paths out of susceptible areas that do not involve traversing other susceptible areas can be tricky. When moving people out of Area A involves traversing susceptible Area B then it makes sense that such moves be initiated not only when Area A is threatened but also when Area B is threatened. For example, when leaving a riverside facility involves crossing a bridge, then the action should surely be initiated not only when the facility is threatened but when the bridge is threatened. Moreover, say you have fifty people to move but the available vehicle only holds ten at a time. Then time-to-execute becomes critical. Such identification and analysis requires specialist expertise; it is not something that can be left to "common sense". I would classify it as engineering, let me call it "Evacuation Engineering".
- Political action is essential. Political action is required to ensure that all susceptible populations have engaged in appropriate Susceptibility Analysis and Evacuation Engineering.
- Community action is required to have the people on hand to execute evacuations (and rescue) when the need arises.

Communities also need to practice. Many of us have been subject to fire drills in larger buildings — this is a well-understood form of evacuation engineering. I was involved in one in March. When we got outside, we were informed it was a drill. The drill leader asked us if, on our way out, we had checked all office doors to see if there was someone inside who hadn't heard or hadn't understood or was ignoring it, and asked who had checked the toilets. Something which, as a visitor, I hadn't thought of doing.

Rescue and recovery is recognised to be a specialist discipline (rather, many specialist disciplines). In Germany we have a "Federal Office of Civil Protection and Disaster Assistance", BBK[15]. BBK has a large amount of technical equipment it can mobilise, organised on a local basis — state, county and city authorities can call not just on the fire department but on specialist vehicles and equipment assigned to the local "Technical Aid Facility"[16] (and all painted blue), which is a local organisation similar to a volunteer fire department but with equipment specialised for tasks other than fighting fires. In Texas, there is the Texas Division of Emergency Management. I don't know its specific

[15] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

[16] Technisches Hilfswerk

responsibilities but it does have access to statewide resources to supplement local effort. Some rescue efforts run parallel with evacuation — U.S. Coast Guard Rescue Swimmer Scott Ruskan, based in Corpus Christi, Texas, some 340 km SSE of Hunt, is credited with saving the lives of 165 girls at Camp Mystic (Minsberg 2025).

4.4 Possibility Analysis in Susceptibility Analysis and Evacuation Engineering

Both Susceptibility Analysis and Evacuation Engineering require Possibility Analysis in their details. In contrast with its application in accident analysis to control uncertainty, the application of Possibility Analysis in Susceptibility Analysis and Evacuation Engineering is in categorising and enumerating all possibilities. An example follows for each.

Consider Susceptibility Analysis and its imperfect execution. The district in which I live in Bielefeld, Kirchdornberg, is a village centred around a thousand-year-old church, built in a mild hollow in an otherwise steady incline, with an exit downhill to the northeast. Streams converge in the hollow, all channelled and mostly conveyed underground, then emerge at the exit to flow downhill northeast to Großdornberg and beyond. Bielefeld has a "flood map", indicating in detail areas susceptible to flooding. In a severe (luckily short) rainstorm on 6 August 2023, two areas in Kirchdornberg flooded (including a depression in the road just metres from my front door) and neither of them were on the flood plan. Not only that, but an area identified in the flood plan as flood prone, namely the confluence of all the streams and culverts at the northeast downhill exit from the village, didn't overflow at all. A reason for that was evident — the majority of the water that needed to flow was channelled under the road through a culvert to the stream, had backed up at the culvert entrance, and flooded buildings on the upstream side. One area identified on the flood plan as susceptible to flooding is the "Hof" (alleyway) on the east side of my building. But to get to the Hof, water has to flow down a neighbouring road (a known channel for bringing debris onto the main road whenever we have a strong rainstorm) and then make a sudden 90° left turn in mid-flow to enter the Hof. Of course it doesn't do that. It never does that. But it might if something blocks the road there, say a pile of larger debris, or a car swept away and then halted. Possibility Analysis is essential to Susceptibility Analysis. The city flood plan, an example of Susceptibility Analysis, was misleading precisely because of a failure to consider possibilities.

Simple examples of Evacuation Engineering were noted above. One example, which few people analyse carefully, is how to evacuate their house in a fire. From my third floor, where I sleep, it is some 10+m to sealed ground (paving; asphalt) on one side, but only 3m down to my balcony on the other (and then steps to the ground, away from the building). I have a metal bar on a window on each side and a rappelling rope to hand (and I have practiced — but only once). Where is the building going to burn? You don't know. There can be electrical faults; there can be a lightning strike, and lightning often ignites a roof but sometimes it comes in lower to/through a wall. Evacuation engineering involves enumerating all of the exits, given any conflagration point. But with smoke alarms one can assume that a conflagration point will be somewhat limited (say, to one room). It is all enumeration and categorisation of possibilities and planning for each. My neighbour can exit the first-floor apartment on either side via large roof-window (chairs are stationed) and then has a 2.5m jump into a flower bed on one side (caution: avoid the rose bush!); the other side is mostly paved/asphalted, but there is a pretty solid high bush in the corner by an exit window, onto which a blanket may be thrown, rendering it usable as a flop-down exit. My other neighbour on the ground floor can exit directly by door or through the window from any room. This account incorporates a thorough consideration of all possibilities, and, I propose, thereby counts as (Evacuation) Possibility Analysis.

4.5 Social and Political Communication Engineering

It was apparent both in the 2021 German floods and in the July 2025 Guadalupe River flood that warning was nominally available in advance, say 24 hours for "amber" and when/after the event began, but such warning by and large did not reach the susceptible community.

Exactly why the warnings did not reach susceptible persons differ markedly in the two events. In Germany, the BBK was informed by the ECMWF days in advance of the dangerous atmospheric moisture in a largely stationary pattern. The BBK informed the states involved (my state of North-Rhine-Westphalia, and the state of Rhineland-Palatinate). But the communication at state level, down through the responsible authorities, to the local-area politicians and other civil servants, floundered. Part of the reason for that was the structure of responsible authorities and their (lack of) communication channels.

A general overview of the communication channels as they were is given in Figure 1. Figure 2 shows one obvious way to improve them, namely giving the BBK direct communication with on-site warning and rescue teams.

But such changes to warning structure are insufficient, because they only concern civil-servant level. Going beyond that to the impacted population:– There was no on-site flood warning. There were no siren systems. There was no cell-phone broadcast.

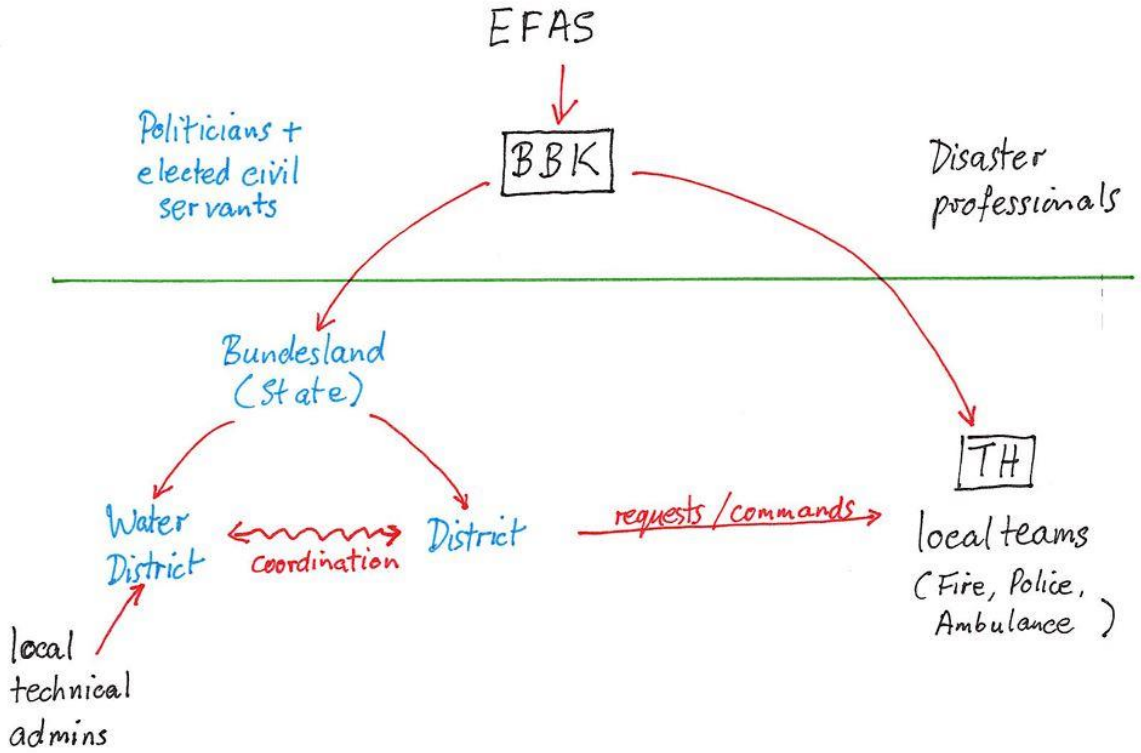

Figure 1 ~ Organisational Structure Underlying Severe-Weather Warnings in July 2021[17]

[17] EFAS is the European Flood Awareness System, (Sub-section 4.1); BBK is the Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, the Federal Office of Civil Protection and Disaster Assistance (Sub-section 4.3); TH is the Technisches Hilfswerk, the Technical Aid Facility (also Sub-section 4.3).

Things have now changed (all over). Bielefeld had, at the time, a few sirens (I know of three) used for summoning volunteer firefighters. Now it has some 170, including one in my village which makes an enormous racket (and completely frightens the cats) when it is tested once a year. There is now a Federal-government-organised cell-broadcast facility for alerts on mobile phones. That also makes quite a racket (much louder than my ring tone).

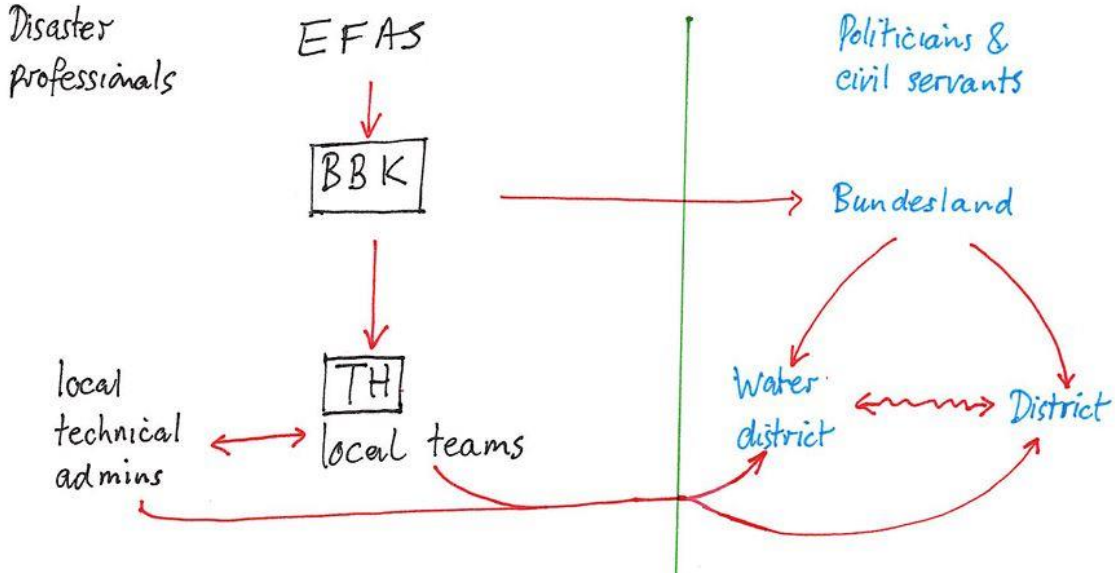

Figure 2 ~ A Potential Improvement in Severe-Weather Warning Communication Structure

Given the number of stories around the German floods, in which rescued people were lucky to have been saved, it seems plausible to the point of being certain that if the extent of the suspended moisture and possible ensuing severe rainfall along with the outflow consequences had been made known to communities a day or two in advance, and then sirens and cell-broadcast used as the rainfall event was unfolding, many people who died in July 2021 would have been able to evacuate. But here there are at least five steps involved:

1. Identification of potential rainfall events. This is well-provided by ECMWF. However, the granularity issue at the lower end of mesoscale remains a scientific limitation
2. Estimating possible rainfall amounts. This is highly variable — if a mesoscale convective event stalls, as apparently in the 2024 Maggia Valley event, then the ensuing rainfall can be many times higher in a local area that what can have been expected simply through an assessment of available atmospheric moisture
3. Estimating outflow consequences of given rainfall amounts. This can be done, and should be done, but is not always done well (cf. my experience with the Bielefeld flood plan)
4. Communicating these outflow consequences to the susceptible population in advance
5. Giving warning (sirens, cell broadcast) when an event is underway

It is fair to say that, at the time of the 2021 German floods, Step 1 was performed well. Nowadays, I would expect Steps 1 and 5 to be done well. Step 3 can in principle be performed well, but it is likely an art to ensure that it is. Concerning Step 2, we just have

to hope for advances in meteoro/hydrological science. Concerning Step 4, I think it is fair to say that this is not well advanced.

Concerning Texas, it seems as if Steps 1 and 2 were performed well, within the limitations of current science (here I am indebted to the accounts of Gerard, Lanza, and Lowry). It seems as if Step 3 was in part lacking: there is the MRMS FLASH tool, but on the other hand the rise in the Guadalupe river at Hunt exceeded the measurement capability of the device there, so the installed kit didn't measure up. Step 4 seemed to be effectively lacking. Some say the Camp Mystic Director received the WEA at 01:14 but did not initiate evacuation measures until well over an hour afterwards, and then was himself overwhelmed. Many visitors (campers and those in recreational vehicles) and some residents have given accounts which had them surprised by the event. Step 5 seems to have been "by word of mouth". There have been accounts that residents upstream would phone residents downstream when river levels became high. It was also reported that a siren system for the Guadalupe had been discussed at county-political level but was not pursued because of the cost. In contrast to Germany in 2021, a cell broadcast system (WEA) did exist and was used. But for whatever reason it did not seem to be effective. For example, the Kerr County Emergency Management Director was woken up by a colleague calling him by telephone, not by any of the four WEAs which had been issued earlier (Hutchinson 2025).

Then there is, as emphasised to me by a colleague who lives in Austin, the question of hubris and ignorance. Most people in Texas who die in floods are apparently attempting to negotiate running water in their trucks and SUVs (Dorsett 2025). They think they can (hubris) based on not realising they can't (ignorance). Then there are all those people who went camping and RVing on the Guadalupe River in "Flash Flood Alley" on a weekend with record levels of atmospheric moisture from the remnants of a tropical storm, an MCV to the west, and a strong 850mb jet stream. It is likely fair to say (and interviews substantiate) that most were not aware of the risk. That is a social problem for which I have no solution.

Correspondence Address

Corresponding e-mail address: ladkin@causalis.com.

Acknowledgments

I thank Mark Rogers, Don Hudson, and other anonymous experts for essential information on, and analysis of, Air India Flight 171 and the Boeing 787 aircraft. I thank Robert Dorsett for discussion of flooding in Texas. I am very indebted to the writings of meteorologists Alan Gerard, Mark Lanza, and Michael Lowry.

A tutorial on Possibility Analysis will be presented on Day 2 of SSS'26, the Safety-Critcal Systems Symposium, in York.

References

Ahr — English. (no date). In Wikipedia: https://en.wikipedia.org/wiki/Ahr. Accessed 23rd January 2026.

Ahr — German. (no date). In Wikipedia: https://de.wikipedia.org/wiki/Ahr. Accessed 23rd January 2026.

Birsch D, and Fielder J. H. (eds). (1994). *The Ford Pinto Case: A Study in Applied Ethics, Business, and Technology*. State University of New York Press.

Burnett J. (2008). *Flash Floods in Texas*. Texas A&M University Press.

Carlsen C. S. (2012). *Effective FMEAs*. John Wiley & Sons, Ltd. Chichester

Dorsett R. (2025). Private communication with the author.

ECMWF. (no date). *European Centre for Medium-Range Weather Forecasts*. Website. At https://www.ecmwf.int. Accessed 20th January 2026.

Gerard A. (2025a). *BalancedWx special: Tragic flash flooding in the Texas Hill Country*. Balanced Weather Substack 2025-07-05. At https://balancedweather.substack.com/p/balancedwx-special-tragic-flash-flooding. Accessed 20th January 2026.

Gerard A. (2025b). *Latest on Texas Hill Country flood tragedy*. Balanced Weather Substack 2025-07-06. At https://balancedweather.substack.com/p/latest-on-texas-hill-country-flood. Accessed 20th January 2026.

Gerard A. (2025c). *BalancedWx Special: Watches and warnings in the Texas flood tragedy*. Balanced Weather Substack, 2025-07-11. At https://balancedweather.substack.com/p/balancedwx-special-watches-and-warnings. Accessed 20th January 2026.

Gerard A. (2025d). *Row away from the rocks*. Balanced Weather Substack,, 2025-07-29. At https://balancedweather.substack.com/p/row-away-from-the-rocks. Accessed 20th January 2026.

Goodman J. (2025). *'The forest had gone': the storm that moved a mountain*. The Guardian 2025-08-05. At https://www.theguardian.com/world/2025/aug/05/forest-gone-storm-that-moved-a-mountain-climate-crisis-environment. Accessed 23rd January 2026.

Government of India. (2025). *Preliminary Report: Accident involving Air India's B787-8 aircraft bearing registration VT-ANB at Ahmedabad on 12 June 2025*. Indian Ministry of Civil Aviation, Aircraft Accident Investigation Bureau. Published 2025-07-11. Available from https://aaib.gov.in/What's%20New%20Assets/Preliminary%20Report%20VT-ANB.pdf. Accessed 20th January 2026.

Graham R. (2025). *Camp Mystic Owners' Legacy: 'If You're A Camper, You Know Who They Are'*. New York Times, 2025-08-11. At https://www.nytimes.com/2025/07/11/us/camp-mystic-texas-floods.html. Accessed 23rd January 2026.

Holthaus E. (2025). *Texas floods reveal limitations of disaster forecasting under climate crisis.* The Guardian, 2025-07-06. At https://www.theguardian.com/us-news/2025/jul/06/texas-floods-forecast-climate-crisis. Accessed 25th January 2026.

Hutchinson B. (2025). *Testimony of the Kerr County Emergency Management Director, William Thomas, to the Texas Senate*. ABC News, reported 2025-08-01 in https://abcnews.go.com/US/kerr-county-texas-lead-emergency-management-official-asleep/story?id=124237644. Accessed 23rd January 2026.

IEC 60812. (2018). *Failure modes and effects analysis (FMEA and FMECA).* IEC 60812, 3rd Edition, 2018. International Electrotechnical Commission, Geneva

IEC 62740. (2015). *Root Cause Analysis*. IEC 62740, 1st Edition, 2015. International Electrotechnical Commission, Geneva.

ISO/IEC. (2014). *Safety aspects — Guidelines for their inclusion in standards*. ISO/IEC Guide 51, 3rd Edition, 2014. International Organisation for Standardisation/International Electotechnical Commission, Geneva.

Kaufhold H, Schürmann T, Ladkin P. B. (2019). *Lifecase Extended Report 31, 2019-04-06* (in German). RVS Group, Bielefeld University. Available by request from the third author.

Ladkin P. B. (2017). *Digital System Safety — Mostly Qualitative Aspects*. eTextbook in WBA and OHA. Available at https://rvs-bi.de/publications/RVS-Bk-17-02.html. Accessed 20th January 2026.

Ladkin P. B. (2022). *The German and Belgian Floods in July 2021*. In: Parsons, M. and Nicholson, M. (eds). (2022). *Safer Systems: The Next Thirty Years, Proceedings of the 30th Safety-Critical Systems Symposium Blended Conference 8th – 10th February 2022*. Paper available to SCSC members from https://scsc.uk/r1530.pdf

Lanza M. (2025). *Making sense of the weather that led to a horrible Texas flooding tragedy*. The Eyewall blog, 2025-07-05. At https://theeyewall.substack.com/p/making-sense-of-the-weather-that. Accessed 25th January 2026.

Leveson N. G. (2011). *Engineering a Safer World*. MIT Press, Cambridge MA. Also available open-access https://direct.mit.edu/books/oa-monograph/2908/Engineering-a-Safer-WorldSystems-Thinking-Applied. Accessed 20th January 2026.

Lowry M. (2025). *Trying to Make Sense of the Unspeakable Texas Tragedy*, Michael Lowry Substack 2025-07-07. At https://michaelrlowry.substack.com/p/trying-to-make-sense-of-the-unspeakable. Accessed 25th January 2026.

McDermott R. E, Mikulak R. J, and Beauregard M.R. (2008). *The Basics of FMEA*. 2nd Edition. Routledge, Abingdon.

Minsberg T. (2025). *Terrified Girls, Helicopters and a Harrowing Scene: A Rescuer's Account at Camp Mystic*. The New York Times, 2025-07-06. At https://www.nytimes.com/2025/07/06/us/texas-floods-rescues.html. Accessed 25th January 2026.

Sieker B. M. (2010). *Systemanforderungsanalyse von Bahnbetriebsverfahren mit Hilfe der Ontological Hazard Analysis am Beispiel des Zugleitbetriebs nach FV-NE*. D.-Ing. (Doctor of Engineering) thesis, Faculty of Technology, Bielefeld University. Available (in German) at https://rvs-bi.de/publications/Theses/Dissertation_Bernd_Sieker.pdf. Accessed 20th January 2026.

Stuphorn J, Sieker B. M, and Ladkin P. B. (2009). *Dependable Risk Analysis for Systems with E/E/PE Components: Two Case Studies*. In: Dale C, and Anderson T. (eds). (2009). Safety-Critical Systems: *Problems, Process and Practice, Proceedings of the Seventeenth Safety-Critical Systems Symposium, Brighton, UK, 3-5 February 2009*. Springer-Verlag London Ltd. Available at https://rvs-bi.de/publications/Papers/StupSiekLadSSS09.pdf. Accessed 20th January 2026.

US Air Force. (2021). *Safety Investigations and Reports*. United States Department of the Air Force. Instruction 91-204, 10 March 2021. Available at https://static.e-publishing.af.mil/production/1/af_se/publication/dafi91-204/dafi91-204.pdf. Accessed 20th January 2026.

US Coast Guard. (2025). *Coast Guard Marine Board of Investigation releases report on Titan submersible*. United States Coast Guard. Press release of 2025-08-05. Available at https://www.news.uscg.mil/Press-Releases/Article/4265651/coast-guard-marine-board-of-investigation-releases-report-on-titan-submersible/. Accessed 20th January 2026.

US DoD. (1949). *Procedures for Performing a Failure Mode Effect and Criticality Analysis*. MIL-P-1629. United States Department of Defense, Washington D.C.

Vallemaggia — Italian. (no date). In Wikipedia: https://it.wikipedia.org/wiki/Vallemaggia. Accessed 23rd January 2026.

WaterwayMap.org. (no date). *South Fork Guadalupe River*. Available at https://waterwaymap.org/river/South%20Fork%20Guadalupe%20River%20000355056466/. Accessed 23rd January 2026.