BACKGROUND READING – TREE HOUSE OF FAILURES

A. RECAP ON FAILURE

As you have learned previously, *Forensic Engineering comes into play when* failure of a technical system occurs, *or* if failure of a technical system is suspected to be the potential cause of an adverse advent. But what is failure really?

Failure of a technical system is when that technical system cannot fulfil some or any of its intended functions in its utilization phase. Forensic Engineers may study these failures for reasons such as to determine:

- what happened,
- what caused it to happen,
- how it could have been avoided,
- how the technical system could be improved to avoid failure in the future.

The *root causes* of a failure can be in any of the life-cycle phases. And that is why you should train yourself to think about potential causes anywhere in the life-cycle of the technical system. Furthermore, it is essential to realize that any observed failure can also be a cause of another failure or a result of another failure.

B. THE TREE HOUSE OF FAILURE

Consider the proper functioning of any technical system to be a tree house. Than that tree house is supported by a foundation consisting of three carriers, each supported by a set of tree stems that all grow on a bunch of roots. The tree house will collapse when the foundation caves in because something in the foundation falls over.

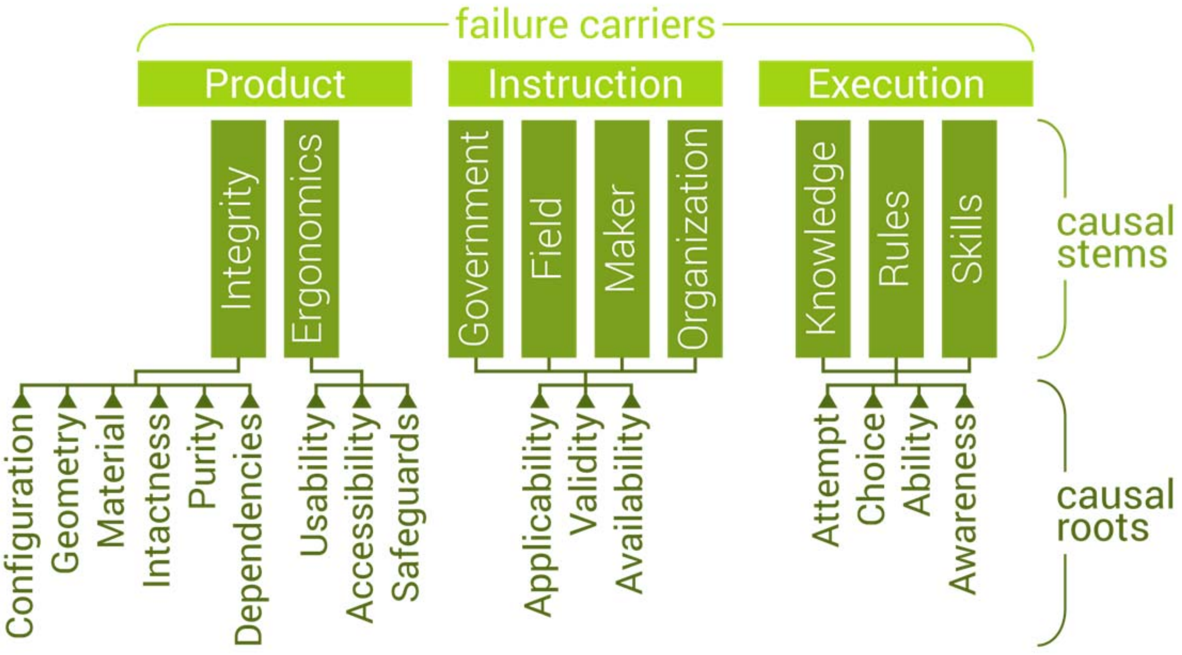

Fig. 1: "Tree House of Failure" diagram

The “Tree House of Failure” diagram (see Fig. 1) describes the foundation of the proper functioning a technical system (the tree house). The foundation has *three failure carriers*. Each failure carrier represents a group of potential causes related either to: *Product*, *Instruction* or *Execution*, which also are the names of the three carriers. Each of these has several *causal stems* that group potential causes of failure in that carrier by certain characteristics, which will be discussed later. Finally, the stems of a single failure carrier are always some sort of family. Therefore, we can define very specific sets of *causal roots* that are typical and identical for the stems of a single failure carrier. For the Product related causes, the causal roots differ for a bit for its two stems, but within the Instruction related causes and within the Execution related causes, all stems have the same set of causal roots. [...] Now let’s go through the three failure carriers and their causal stems and roots. [...]

1. *Product related causes* are to be sought for in the actual, physical, technical system itself: such as a support beam that breaks or a screw that was too weak.

   a. Causal stems. Within the product related causes the two *causal stems* that we distinguish are *Integrity* and *Ergonomics*. [...]

      - In the *Integrity stem*, you should look for issues stemming from faults in the physical integrity of the technical system, like the construction, electrical aspects, heat transfer, chemical aspects, etc.. Any physical aspect you can think of. [...] In the *Ergonomics stem*, you should look for issues stemming from how the design of the technical system helps to avoid errors and helps to make the system easy-to-use and safe-to-use.

   b. Causal roots. For the Integrity stem we have six causal roots: [...]

      - The *Configuration* of the technical system should be verified to see if the technical system was complete and well set up. Check, for example, if the right parts were used, if bolts were tightened, if software settings and motor speeds were set right and if any measuring devices were calibrated. Search for answers to questions like “Could the cement mixture of that collapsed pillar have been wrong?”, “Could the patient have died because the heart monitor software alarm did not work after the new software update?”. [...]

      - The *Geometry* of any parts potentially involved in the failure should be checked to see if nothing went wrong because of the shape or size of parts. [...] For instance, check if play between parts did not cause problems and if the fits between parts were right. Were the fuel tank seals watertight? Are there no dents, bends or other deformations that could have caused machine parts to get stuck?

      - Any deviation from the intended *Material* used in the technical system could cause failure. Chemical processes like corrosion, neutralization, separation, or decomposition can drastically change the properties of materials, causing them [...] for example [...] to jam due to rust, or to poorly conduct electricity. Or a normally neutral fluid may have become acid and dissolve metal parts. Physical processes like stress relaxation, hardening or drying can make materials weaken, loose flexibility or become porous for materials they were supposed to keep out. You should seek to answer questions like “Could rust have weakened this building’s support beams?”, or “Has the glue dried properly?”.

      - The *Intactness* of any part of the technical system may just as often be the consequence of a failure as the cause of another failure. A broken car wheel could cause a car to crash against a tree, but the wheel may also have broken due to the crash against the tree after the driver made a steering error. Always try to find an answer to the questions “Are there any signs of detachments, tears, fractures, wear, erosion, etc.?”, and “Could any of these have caused failure?”.

- *Purity* may not be such an obvious cause of failure. But we define purity as not having anything in the technical system that should not be there. It is not just about dirt, but also about things like bacteria in hospital equipment, pollution of fuel, ice on plane wings, or computer viruses in a system's control software. Try to seek answers to questions like "Could a pilot have overlooked cracks in the landing gear because they were covert by dirt?", "Could bacteria have been left behind in a surgical instrument despite the cleaning process and gotten into the next patient?", "Could the watch found between the lifting gears of the crane have dropped in accidentally, made the gears jam and cause the lifting cable to break?".

- Technical systems are barely ever isolated from their environment completely. And if they are, their functioning probably depends on being that isolated. The causal root *Dependencies* is about issues arising from connections to the surroundings, dependence on receiving information or dependence on not getting disturbed at all. You should seek to answer questions like "Did the river provide sufficient cooling water to the nuclear plant?", "Did the fire alarm depend on a phone signal to call in the fire squad?", "Could the building have collapsed because the recent flooding flushed away the soil underneath the foundation?", or "Could strong wind have pushed the crane on the building site over?".

For the Ergonomics stem we have three other causal roots. Ergonomics is most known to people to be about proper seating and not lifting too heavily. However, it is much more than that and is about *Usability*, *Accessibility* and *Safeguards*: […]

- *Usability* indicates how well it is clear or how easy it is to learn […] how the technical system should be used and what the user should do how and when. Try to answer questions like "Are the emergency exits indicated clearly?", "Are electrical switches labelled logically?", "If a green light is used to indicate an error… was that a smart choice?"

- *Accessibility* is all about making sure that a technical system and all its relevant components can be properly reached, seen, heard, controlled etcetera for users with a broad range of abilities or disabilities. Ask questions like "Are the fire alarm switches within proper reach?", or "Are the plane's altitude gauges visible in the dark?".

- *Safeguards* can be created through proper use, clear instructions and warnings, or good usability and accessibility, but should preferably exist intrinsically in the design of the technical system. Try to find answers to questions like "Is it safe to have balconies without railings?", "Is it safe to have that emergency door opening button next to an airplane passenger seat?".

2 *Instruction related causes* are to be sought for in any instruction that describes how the technical system should be designed, produced, utilized or recycled.

a. Causal stems. The *four causal stems* in this failure carrier relate to instructions coming from: *Governments*, professional *Felds*, the *Maker* of the technical system and the *Organization* within which the system is used.

- In the *Government stem* you should look for issues stemming from instructions that are laws, regulations, treaties and other government issued instructions that are supposed to be respected by… well, basically everyone. […]

- The *Field stem* contains instructions that are standards, norms, covenants etcetera. These are documents like ISO-standards that prescribe to what aspects a technical system, process or component should comply to be considered safe, suitable for trade, suitable for use or simply just […] functional. This group is called the field stem because such documents are not made by governments, but by professionals that cooperate to achieve common agreements on how things should be done. However, governments may have laws that tell you have to comply to field norms for certain things. For example, hospitals in Europe are obliged by law to only buy and use CE approved devices (CE is similar to the American FDA approval) and in order to get such approval, manufacturers often have to follow certain ISO-standards. So, the government stem and the field stem can be very closely related.

- In the *Maker stem*, you should look for issues stemming from the instructions most closely related to the product: the instructions for design, manufacturing, maintenance and use. These include design requirements, technical drawings, user manuals, safety instructions and maintenance prescriptions.

- In the *Organization stem* you should look for issues stemming from instructions that are made for internal use by the company, hospital or other organization in which the product is used [...] like a work instruction that is used in a car manufacturing company to ensure that all welders use the same welding settings [...] and to ensure that the welding machines are used safely. All these instructions can be centrally defined and in writing, but can also be given verbally and transferred between teams and individuals.

b. Causal roots. For all instructions in these four stems there are three *causal roots* to consider: *Applicability*, *Validity* and *Availability*. [...]

- Regarding *Applicability* you should seek to answer questions like "Were the correct design requirements used?", "Should any instructions have been followed?", "If so, which, and were those actually followed?". [...]

- Regarding *Validity* you should seek to answer questions like "Were the design requirements properly established?", or "Would following the appropriate instructions, that is [...] the ones intended to be used, [...] actually have led to the right results?" [...] or in other words [..] "Have the instructions ever been tested and validated, or do experts agree that they are okay?". [...] In general, it should be okay to assume that instructions in the government stem and field stem are just. But don't hesitate to check if you feel that there is any reason for it. Even governments and experts make mistakes.

- Finally, regarding *Availability* you should figure out things like "Was the manual present close to the packaging machine in the factory?", or "Was the user told where to find the online manual for his bike?", or "Did the government already publish the new law that states that all bikes should have airbags?".

[...] By now we should have found all causes of failure hidden in the product or its instructions. If these were all okay, something probably went wrong when someone tried to actually bring the instructions into practice or utilize the product. These are the execution related causes. [...]

3 *Execution related causes* are about if and how all prescribed instructions were actually executed in all of the lifecycle phases. Such as, [...] was the design made according to the safety regulations prescribed by law? Was the product made according to the drawings and specifications provided by the designer? Did the cyclist grease the bike gears according to the instructions? And did she actually ever learn how to ride a bike safely?

a. Causal stems. There are many reasons why execution could go not as supposed to, but these are grouped in *three causal stems* related to what cognitive level of a party's *behaviour* is involved. [...] Please note that we often say "a party" and not necessarily "a user", because the involved party could be a user, but also a designer, a group of people or even an entire government. [...] But let's get back to the three causal stems of executions related causes:

- In the *Knowledge stem*, you should look for issues stemming from a parties' lack of knowledge about the technical system and the context it was used in. Consider what happens if an aircraft pilot would not understand how a plane works and then has to decide what to do when a light labelled "landing gear oil pressure low" starts blinking.
- In the *Rules stem* you should look for issues stemming from parties following a wrong protocol, or wrongly applying the rules.
- Finally, in the *Skills stem* you should look for issues stemming from errors in performing an action or routine, even though the party intended to do the right thing. Think about, for example, choosing to properly put the cap on your car's gas tank, but accidentally leaving it on your car roof because you got distracted by a friend calling you before you got to actually close the tank.

b. Causal roots. There are four *causal roots* carrying the skills, rules and knowledge stems. These are Attempt, Choice, Ability, and Awareness.

- *Attempt* is closest to actual physical actions and is about things going wrong because the thing you wanted to do did not go as you intended. It's also about trying the right thing, but not being successful at it. You should try to answer questions like "Did the cyclist see the stone in time to break or was she not paying attention?" [...] or "Did the cyclist manage to squeeze the brakes hard enough to stop timely?"
- Things could also go wrong in the causal root *Choice*, which is about decision making. You should try to answer questions like "Was it the right choice to follow this particular instruction?", "Was this person fit to use the technical system?", or "Was it correct to decide to defer from the protocol because something unexpected happened?". Errors in choice usually mean someone did the wrong thing, while thinking it was the right thing. [...]
- *Ability* is about how well the involved party was capable to make the right choices or properly perform any actions. You should try to answer questions like "Was the doctor trained and able to use the X-ray?", "Did the construction worker have sufficient experience to be the project leader?", or "Could the consumer be assumed to be able to handle a hammer without an instruction manual?". [...]
- The causal root *Awareness* should lead you to answer questions like "Did and could the user have known that training was necessary?", "Did the pilot receive any signals about the failing engine?", or "Was the stone on the road visible at the time of day during the bike accident?". [...]

C. CONNECTING LIFE-CYCLE AND TREE HOUSE

The Tree House diagram is a taxonomy describing how different kinds of failure can be grouped depending on their characteristics. This can come in handy in many situations, but in this course it is of particular importance because it helps us to systematically perform forensic engineering investigations.

FAILURE EXPLORATION ROUTINE

During a Forensic Engineering investigation you will be looking for potential causes of the failures you see. To systematically search for these causes, the Life-Cycle Phases and the Tree House of Failures *together* form a great lead. Just follow this *Failure Exploration Routine*:

1. Go through each of the life-cycle phases
2. Zoom in on each step within each phase
3. For each step go through the Tree House diagram
   - A. Determine which causal stems and roots from the Tree House diagram apply to this step
   - B. For each of the roots that apply, try to think of any failure causes that could have originated in this Life-Cycle step and could have caused any of the (other) observed failures.
4. You may have to go back and forth through the Life-Cycle once or more often depending on what you find.

By systematically following this *Failure Exploration Routine* you will discover more potential causes than when looking only at the Utilize phase or when relying purely on your inspiration to come up with possible explanations for the observed failure, damage or adverse event. The resulting set of potential causes can be used to generate a hypothetical story line, also called a chain of events, to explain what happened. […] Of course, this doesn't make it proof, but once you have a proper set of hypotheses, you can systematically investigate and tests your hypotheses to rule out the wrong ones or prove the right ones. But that will be treated in a later module of this course.

CAUSE, RESULT, CHAIN OF EVENTS

It is essential to realize that any observed failure can be either a cause, a result of another failure. Consider a newly built house with a balcony supported by two pillars. If you find a broken pillar, which was not used perfectly according to its specifications, lying on top of a sturdy car that consequently broke, the failure recognized as a smashed car would be *here* in the diagram. The car was overloaded by something not supposed being there. However, if the pillar broke because its concrete was not mixed as instructed, the breaking of the pillar was a failure that was also the consequence of another failure […] the improper mixing.

In a Forensic Engineering Investigation, it is essential to establish the entire so called *chain of events*. This is because one event (improperly mixing concrete during the *Production phase*) can lead to another event (breaking of the pillar during the *Use phase*) and another (breaking of the car) etcetera. In this case, the pillars manufacturer will probably have to pay for the damage to the car because they delivered a weak pillar. But if we would have stopped searching for explanations too early, we might have concluded that the balcony was made or loaded too heavily. In that case, the car owner could have sued the innocent construction company that built the house.

So it's crucial to explore the failures using the Failure Exploration Routine with the Life-Cycle and the Tree House diagram as an aid not only to discover a single failure, but also to establish the entire chain of events as good as possible.

WHEN TO STOP SEARCHING

But what is as good as possible? How long should you keep searching to just find yet another underlying root cause, […] or for yet another totally unrelated failure that may not have anything to do with the adverse event, or may not even have caused any problems at all? Well, it's unfortunate, but that's hard to say. Often, the decision to wrap up the investigation is because the pre-set goal got achieved or because it became sufficiently clear what happened and what caused it. But just as often the decision to wrap up an investigation is based on common sense, logic and likelihood, or sometimes simply because there is no more time or money left to keep looking for less and less probable causes.

The point is that we never know if we missed anything until we discover the thing we missed. But the systematic approach you'll learn throughout this course will help minimizing the risk of missing things and to keep your investigations structured and objective. So it's good to be aware of the pitfalls of stopping an investigating too early or accepting the first found explanation for failure too easily. But it takes some experience, a bright and objective view and approach, [...] and sometimes a bit of courage to decide that enough has been done to properly wrap up a forensic engineering investigation.

LIMITED APPLICABILITY

Now, you should find most potential causes when using the exploration routine we described. But because even the Tree House of Failures may not be perfect, you should always keep an open mind and realize that each sets of causal roots has an extra, invisible root. [...] And that's the root called "other". Any explanation not covered by the Tree House diagram can go there. So use it whenever you need it.

As a final note, we should keep in mind that not all failure carriers, causal stems or causal roots may exist in all kinds of technical systems or all use situations. For example, when you buy a vacuum cleaner and use it in your own house, the causal stem Organization will not exist, because you are your own boss and you don't have to follow any company or institute work instructions [...] well, okay, maybe if you live with your parents or partner and *they* give you rules.

BACKGROUND READINGS:

Book: Failure Mechanisms in Building Construction, D.H. Nicastro (EXAMPLES OF STRUCTURAL FAILURE MECHANISMS)

Wegge K.P., Zimmermann D. (2007) Accessibility, Usability, Safety, Ergonomics: Concepts, Models, and Differences. In: Stephanidis C. (eds) Universal Acess in Human Computer Interaction. Coping with Diversity. UAHCI 2007. Lecture Notes in Computer Science, vol 4554. Springer, Berlin, Heidelberg (ABOUT ERGONOMICS)

http://www.hse.gov.uk/humanfactors/topics/types.pdf

http://www.iwolm.com/wp-content/downloads/SkillsRulesAndKnowledge-Rasmussen.pdf