CHAPTER 5

OHA of a Pressure Tank

A pressure tank has been a canonical example on which to perform hazard identification and analysis since its appearance in the Fault Tree Handbook [18]. In this chapter I perform a hazard analysis of a pressure tank, to illustrate the application of OHA.

The first step of an OHA is an OPRA, identifying the objects, their properties and the relations amongst them that will be subject to the hazard analysis at the starting level (reification), along with any important assertions about these. I elucidate the physical causal relations amongst various of the OPR, which will result in a description of the pressure tank. The description is somewhat abstract, leaving out for example details of the actual physical construction of the tank and its appendages. This System Description Level 0 (SDL 0 or simply Level 0). In SDL 0 we can define an "accident" (one of what would ultimately be a number of events which could be classified as AEs if we were to go the whole hog). We perform a analysis of hazards expressible in SDL 0 which causally lead to the accident so defined. This analysis results in an extension of the OPRA ontology, SDL 1. SDL 1 derives from SDL 0 in so far as the design of the tank in SDL 0 precludes the hazard condition from being avoided or mitigated by deliberate physical means.

We ultimately wish to reduce risk where possible (in the words of English law, where "reasonably practicable"). One achieves risk reduction by

- reducing the chances that a hazard condition pertains, or
- reducing the exposure of the system to the hazard condition, or

- reducing the chance that an accident will result from the hazard condition, or
- reducing the severity of any accidents which might result, or
- any combination of the above

Since we are performing hazard analysis here, and not risk analysis or assessment, we shall not quantify these characteristics. However, we shall see that we use them qualitatively to introduce a design of a system less susceptible to a hazard condition than its predecessor.

We construct and refine a Causal Control Flow Diagram (CCFD) of the operation of the pressure tank. A CCFD uses the same counterfactual notion of causality as a Why-Because Graph, but as well as states and events as in a WBG, it shows the continuous phenomena which causally influence each other as the pressure tank continually operates. We call these phenomena *value-influence factors*. Unlike in a WBG, such causality can loop; there can be causal feedback, which results in a loop. In the case of control-system CCFDs, such value-influence factor loops will commonly be seen.

We shall see that the CCFD allows a straightforward identification of countermeasures in this example. The countermeasures constitute architectural additions to the system, resulting in System Description Level 1. SLD1 does not enable complete avoidance of an accident, for at any given time these additional functional features all may fail, and the modified pressure tank would then be in the original situation described in SDL 0, in which it is susceptible to an accident. However, we can show that any single failure does not disable the mitigation mechanisms.

To show that any single failure does not disable mitigation, we use a semi-formal method. We fix specific values of some of the parameters in the CCFD; this results in what we call a *Causal Specificity Diagram*, CSD. We propagate these values through the CCFD to see if the hazard condition remains mitigated, or now pertains. (We can do this here by means of a simple visual test. We place the CSD over the CSD with the hazard scenario unmitigated, and see if the values fixed at any of the nodes are contraries. If so, the hazard remains mitigated, since the two diagrams are incompatible. If not, then the failure allows the hazard scenario to pertain and the mitigation fails.)

One of the standard ways of showing failure dependencies in systems and subsystems of complex engineered systems is through qualitative *fault trees* (FTs) (there are

also quantitative fault trees, but their quantitative aspects are controversial, because they depend on statistical-independence assumptions which often do not pertain). CCFDs may be converted into fault trees if desired, and we show how to do this in Chapter 10 of [8] . There are many good, thorough texts explaining how to use fault trees in system analysis, for example [4], [5], [1] so we will not devote space to the construction and use of fault trees in this book. In [8], the fault tree automatically generated from the CCFD of SDL 1 is compared with some other fault trees proposed in other texts for the pressure vessel at SDL 1. This comparison shows how the preliminary CCFD analysis leads to a more helpful, because more accurate, fault tree than one is likely to obtain by generating the fault tree through simple intuition.

I focus here on the causal and hazard analysis of the pressure tank at two levels only, System Description Level 0, derived from the simple functional diagram in Figures 5.1, and System Description Level 1 in Fig 5.7, which is derived from Level 0 by considering how to avoid the accident event at Level 0, and thereby supplementing the system (and its OPRA). Possible second-level refinement steps, and further, are left to the exercises.

5.1 OPRA: Object, Properties, Relations

The Pressure Tank The simple pressure tank is shown in Figure 5.1. It contains three input streams, for steam, hydrocarbon and catalyst, on the left. Each stream is controlled by a valve. The tank itself has a pressure sensor, shown above the tank, not currently connected to anything. It contains three output streams, one for the normal output of the product and two vents.

The Accident We have discussed the definition of what constitutes an accident. Normally it is concerned at least with possible injury or death to people, or damage to the engineering environment in some way. This pressure tank has steam input, which could rupture and theoretically cause injury to nearby people; it likely has hot sections (for example an uninsulated steam pipe) which could injure someone who comes into contact with it; maybe very hot sections that could cause other sorts of damage. Pressure tanks are also susceptible to overpressure, which results in rupture that may have a very sudden character, like an explosion, resulting not only in physical damage through impact of parts with the surroundings, but also the uncontrolled release of

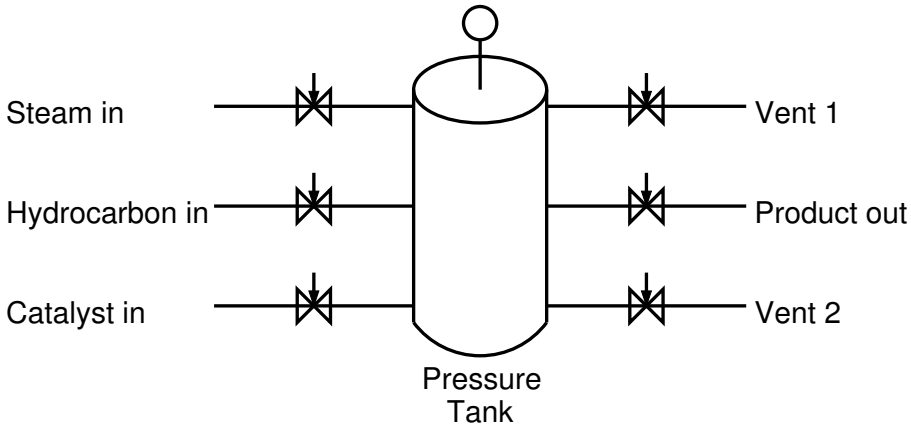

Figure 5.1: The Pressure Tank Without Safety Mechanisms

potentially damaging substances into the local atmosphere.

For the purposes of this analysis we will select just the overpressure-rupture event as the dangerous event likely to result in damage - the Accident Event in our terminology.

The severity of the Accident Event will depend upon, for example, how many people are in the neighborhood of the tank when it ruptures, and how effluent discharged through the rupture is contained. Most installations will have a pressure tank with possibly damaging contents installed in some sort of containment structure, and also restrict the access of people to the containment structure when the system is in operation. Neither of these mitigation measures are expressible in the preliminary OPRA, and they will not arise in our current analysis, for we do not go that far. This is consistent with the way that the other books cited consider the pressure tank when constructing their preliminary fault trees. OHA will of course go further than this during the refinement process, and other practical hazard analysis methods will also identify the possibility of damage mitigation through containment and restriction of personnel, for these are standard mitigation techniques throughout the process industries.

Preliminary OPRA The design has been given to us by means of a labelled diagram. Given the manifest objects in the diagram, we can specify certain properties and predicates amongst the components of the system through general physical considerations,

for example the quantity, temperature and pressure of steam, hydrocarbon, catalyst, and product; the open/closed states of the valves and maybe even which components (tubes, tank, valves) are fulfilling their specification (which we are not given) and which not.

There are other components, such as joints, screws, surface coatings, controlled climate, and so on, which we are not given in the diagram and do not belong to the preliminary OPR. We therefore do not assess the state or behavior of these components at this stage, although such might be a significant factor in any real accident behavior. For example, the pressure tank may rupture because of high-, not over-pressure, which causes a weak riveted joint in the vessel, that fails to fulfil its specification, to give way. The point is this: one considers only the ontology with which one is presented at a given SDL. One cannot infer anything about things, properties or relations not in the ontology at that SDL. Weakness of joints because of non-specification riveting are not part of the preliminary OPRA.

Objects We have already performed the OPRA for SDL 0 in Chapter 3. We repeat it here in Figure 5.2 for convenience.

Properties The properties identified in Chapter 3 are listed in Figure 5.3.

- *Tank*
- *SteamPipe*
- *HCPipe*
- *CatalystPipe*
- *ProductOutPipe*
- *VentPipe1*
- *VentPipe2*
- *TankPressureSensor*
- *SteamPipeValve*
- *HCPipeValve*
- *CatalystPipeValve*
- *ProductOutPipeValve*
- *VentPipe1Valve*
- *VentPipe2Valve*
- *Steam*
- *HC*
- *Catalyst*
- *Product*

Figure 5.2: The Objects at SDL 0

- *Intact* and its contrary *Ruptured*, to *Tank*, *SteamPipe*, *HCPipe*, *CatalystPipe*, *ProductOutPipe*, *VentPipe1*, *VentPipe2*;
- *Open*, *Closed* and *Partopen*, to *SteamPipeValve HCPipeValve CatalystPipeValve ProductOutPipeValve VentPipe1Valve VentPipe2Valve*;
- *Temperature*, *Pressure*, *Quantity*, to *Steam HC Catalyst Product*. Although we have called these properties, in fact they are fluents, taking values; different values at different times.

Figure 5.3: The Properties in SDL 0

5.2 Causal System Analysis (CSA)

Formal Definition of Accident Event We use a semi-formal language, namely the mathematical-expression-type language of predicate logic, to describe aspects of the pressure tank at SDL 0. This is a form of controlled language, at this point purely syntax, with an intuitive semantics (namely, whatever you think the English equivalent means). The Accident Event is the rupture of the tank:

Ruptured(Tank)

How Do We Proceed? The causal antecedents to the accident at Level 0 are fairly restricted. An appropriate refinement process will delimit at each level the causal antecedents to events and system states. A certain amount of qualitative physical understanding of such systems is required, although this amount is limited, as we shall see. Hazard analyses are most appropriately conducted with the involvement both of domain experts, who know the systems physically in detail, and of general safety analysts, who know how to conduct hazard analyses effectively. Standards often explicitly require an analytical team to contain both sorts of expert.

What Can Cause The Accident? A rupture in the tank can only occur if the tank is breached from outside, or if there is a sustained overpressure in the tank above a certain level. This is a causal statement. Let us concern ourselves in this analysis just with sui generis accidents, not with interventions from outside the system (say,

someone sabotaging the system), and rule a breach from outside out of consideration. With this restriction it follows that, if an accident occurs, then *the accident would not have happened had there not been sufficient overpressure over a particular length of time in the tank*.

We use the symbol "$\gg$" to denote "*is a necessary causal factor of*". We can thus write the causal relation between accident and condition:

$$Pressure(Tank) > N \ \textit{ units over duration } \ T \gg Rupture(Tank)$$

We can define

$$OverpressureOverPeriod(Tank,N,T) \triangleq Pressure(Tank) > N \ \textit{ units over duration } \ T$$

and restate the NCF relation to the AE thus

$$OverpressureOverPeriod(Tank,N,T) \gg Rupture(Tank)$$

It may be physically more accurate to consider the likelihood of occurrence of the accident (a number between 0 and 1) to be a function, not of simple overpressure for fixed time, but as some function of overpressure and time that is monotonic in both arguments. There is probably some overpressure value N under which the tank would rupture instantaneously. Intuitively much more likely is a sustained but lower overpressure. Nevertheless, our expression of overpressure above a fixed value over a fixed time interval is adequate for our purposes. The reader should keep in mind that, while correct, this is a simplification of the actual physical situation.

Hazard Condition We might want to consider $Pressure(Tank) > N$ intuitively to be a hazard condition, on the basis that when this condition persists for an appropriate length of time, T, a rupture occurs. We also likely know that N is not so large that a rupture occurs instantaneously when an overpressure of N is reached. There are various definitions of what constitutes a hazard condition, some of them enunciated in Chapter 9. They concern increased chances of or reduced barriers to an accident. Let us try to construe this intuitive hazard condition $Pressure(Tank) > N$ as one of these.

There are continuous physical processes at work here. To reach an overpressure of N, where N is not a boundary value of acceptable pressures, then there will have

been a period of overpressure building up to N. The $Tank$ will have been designed to a range of "acceptable" pressures, whatever "acceptable" might mean. Let A be the upper bound of those acceptable pressures. Any $N > A$ is by definition an overpressure. To reach an overpressure of N at time t_1, where $N > A$, there will have had to have been a period of overpressure before and leading up to t_1. If N is just a little bigger than A, then this time may be short. If N is a lot larger than A, then this period will be longer. Say t_0 is a time at which the pressure first becomes greater than A. We will have had a period from t_0 to t_1 at which $Tank$ has been in increasing overpressure up to overpressure N at t_1.

If N is moderate overpressure, we are also likely to know some time period T_{short} shorter than T during which an overpressure of N will not by itself cause the tank to rupture. That is,

$$\neg(OverpressureOverPeriod(Tank,N,T_{short}) \nRightarrow Rupture(Tank))$$

where $\neg$ is logical negation, which we have previously been writing as NOT. This period T_{short} gives us then a period in which to react to overpressure and perhaps avoid it continuing for T and the $Tank$ thereby rupturing. An accident is not inevitable provided that the pressure is sensed and reduced inside T_{short} and stays reduced. Indeed, that will be the way most engineers would look to avoid a rupture accident caused by overpressure.

Let us introduce times on ruptures: $RuptureAtTime(Tank,t)$ holds if the tank ruptures (say, starts rupturing, which ends with a ruptured $Tank$) or is already ruptured at time t. Let us suppose for the convenience of our reasoning that a ruptured tank is not repaired:

$$\forall t_1(RuptureAtTime(Tank,t) \wedge t_1 > t \rightarrow RuptureAtTime(Tank,t_1))$$

If at any time t, starting at t we have pressure greater than N, and this persists until time $t + T$, we know there will be $RuptureAtTime(Tank,t + T)$. We can define $Overpressure(Tank,N,t_1,t_2)$ to mean that an overpressure greater than N is present at t_1 and persists until t_2. It should be clear that

$$Overpressure(Tank,N,t_1,t_2) \rightarrow OverpressurePeriod(Tank,N,(t_2 - t_1))$$

where $\rightarrow$ is logical (material) implication. It also follows, from what we already know, that if there is an overpressure for longer than time period T, there will be a rupture.

We have to be a little careful how we say this, for when the $Tank$ ruptures, there will no longer be an overpressure. So, for example

$$\forall t_1, t_2(Overpressure(Tank,N,t_1,t_2) \rightarrow (t_2 - t_1) \leq T)$$

as well as that if an overpressure continues for a period of time of length T then the Tank has certainly ruptured. We have to be careful how we say this, for it may rupture beforehand and if it ruptures we don't have overpressure any longer. So let us define first that $Tank$ is over pressured at N or ruptured for a time period:

$$OverpressureOrRupture(Tank,N,t_1,t_2) \triangleq$$

$$\forall t(t_1 \leq t \leq t_2 \rightarrow$$

$$Overpressure(Tank,N,t,t) \ \vee \ \exists t_k \ (t_k \leq t \wedge RuptureAtTime(Tank,t_k)))$$

Then we can say that if the $Tank$ is $OverpressureOrRupture$-d for a length of time T (or longer) then it is most definitely ruptured:

$$\forall t_1, t_2((OverpressureOrRupture(Tank,N,t_1,t_2) \wedge (t_2 - t_1) \geq T \rightarrow$$

$$\exists t(t \leq t_2 RuptureAtTime(Tank,t))$$

Consider the situation at an arbitrary time t_0. A sufficient condition for an accident to occur is $Overpressure(Tank,N,t_0,(t_0 + T))$. This is true of any time we designate as t_0. Now consider a time t_1, at which there has already been an overpressure for, say, s time units: $Overpressure(Tank,N,(t_1 - s), t_1)$. A sufficient condition for an accident now to occur is $Overpressure(Tank,N,t_1,(t_1 + T - s))$. Semantically, that is a weaker sufficient condition than for rupture at t_0: at t_0, T time units of overpressure is sufficient for an accident, whereas, at t_1, $(T - s)$ time units suffices, a lesser period. Suppose further that $(T - s) \leq T_{short}$. Then

$$(Overpressure(Tank, N, t_1, (t_1 + T_{short})) \rightarrow RuptureAtTime(Tank, (t_1 + T_{short}))$$

whereas, at time t_0, it is not the case that the stated overpressure for this time period T_{short} will result in rupture:

$$\neg((Overpressure(Tank, N, t_0, (t_1 + T_{short})) \rightarrow RuptureAtTime(Tank, (t_1 + T_{short})))$$

Let us define the *precondition* at time t to be the condition $Overpressure(Tank, N, t_m, t)$, where t_m is the earliest time t_k for which

$Overpressure(Tank, N, t_k, t)$. If $\neg Overpressure(Tank, N, t, t)$ we say that this is the *null precondition*. Let us further say that the precondition $Overpressure(Tank, N, t_m, t)$ is *stronger* than the precondition $Overpressure(Tank, N, t_n, t)$ if $t_m < t_n$; and we say that any precondition $Overpressure(Tank, N, t_m, t)$ with $t_m \neq t$ is stronger than the null precondition. Let us say the precondition $Overpressure(Tank, N, t_m, t)$ is *critically strong* if $T - (t - t_m) < T_{short}$. If time t has a critically strong precondition, then overpressure for a further time T_{short} will result in rupture, whereas if time t has, say, the null precondition, it will not. So in a clear sense a time with a critical precondition is a more hazardous situation to be in than a time with a null precondition: you need to react faster with prophylactic measures at a time satisfying a critical precondition than at a time satisfying a weaker precondition.

This can all probably be phrased in terms of Bayesian probabilities, in which the conditions above set the priors. However, I hope that the discussion above has shown how qualitative conditions can rank as hazards even when no probabilities are explicitly attached. In the example, we have been discussing just one type of hazard condition which leads to an accident. For most systems, we would expect there to be in general many conditions which can be identified as hazard conditions.

Safety Requirement The point condition of which the duration over time leads to a hazard is $Pressure(Tank) > N$. I will refer to this henceforth as the *hazard condition*. The safety requirement derived from the hazard condition $Pressure(Tank) > N$ is as usual straightforward: it is the negation of the hazard condition, $\neg(Pressure(Tank) > N)$, which with some trivial arithmetic manipulation can be expressed as

$$Pressure(Tank) \leq N$$

In order to figure out how to achieve the safety requirement, we analyse the hazard condition causally.

Causal Factors of the Hazard We now inquire about the causal factors of the hazard condition. The Gas Laws in physics tell us that the pressure in the tank is a monotone increasing function of the quantity of the product $Quantity(Product)$ and the temperature of the product $Temperature(Product)$. "*Monotone increasing*" means that the value increases with each increase in each argument. Let us make

the further assumption here, which must be justified through chemical knowledge (domain expertise), that the pressure of the product rises as the hydrocarbon and steam convert into the desired product. Thus the pressure of the product for given inputs and temperature is itself an increasing function of time:

$$Pressure(Tank) = F(Quantity(Product), Temperature(Product), time)$$

We are not concerned with the exact form of the function F, just in knowing that it is monotone increasing with its arguments.

We may express this formally by amending the notation we have already introduced, as

$$Quantity(Product) \Rightarrow^{+,t} Pressure(Tank)$$

$$Temperature(Product) \Rightarrow^{+,t} Pressure(Tank)$$

The superscript "$+$" indicates the monotonic increasing dependency of values, the superscript "t" that there is *hysteresis*, a lag in time of the effect following the cause.

Discrete Factors and Value-Influence Factors The simple counterfactual definition of "$\Rightarrow$" talks about the presence or absence of factors. We call such factors *discrete factors*, for which it makes sense to talk about their presence or absence *simpliciter* in a behavior.

But we have moved from a simple counterfactual notion of causality to describing a causal tendency:

- not only that one extensively-measurable state predicate, one fluent, is a causal factor in another extensively-measureable state predicate, but
- that the measurements depend upon each other in a certain way: namely monotonically increasing or decreasing, or threshold-triggered, or time-triggered.

We call such causal factors *value-influence factors*. We assert here without further argument (although see the Exercises) that these specific four features may be brought within the counterfactual definition in a straightforward way; for example, we have shown how time-triggering may be handled in our discussion of the condition $Pressure(Tank) > N$ *for time* $s < T$ above.

It may well be that these qualitative features of quantitative causal regularities are all that is needed for an adequate causal analysis for safety purposes, but maybe

some others are also useful. The study of Qualitative Physics, as pursued also under the rubric of "Common-Sense Physics" by some AI researchers, could well have a role to play in adequate causal analyses for safety. For example, our analysis here is an exercise in qualitative physics, amongst other things.

Following Causality Backwards We now consider the causal factors of the fluent $Quantity(Product)$. Through simple chemistry, these are $Quantity(Steam)$ and $Quantity(HC)$. Furthermore, $Quantity(Product)$ is monotonic increasing in these values. $Quantity(Catalyst)$ remains unchanged and does not contribute – this is the property of a catalyst. Thus

$$Quantity(Steam) \Rightarrow^{+,t} Quantity(Product)$$

$$Quantity(HC) \Rightarrow^{+,t} Quantity(Product)$$

We say that a quantity is *positively causally dependent* on another if the first is causally dependent on the second, and if this causal dependency is monotonically increasing. Similarly, we say that a quantity is *negatively causally dependent* on another if the first is causally dependent on the second, and if this causal dependency is monotonically decreasing.

Boyle's Law of gases tells us that, for fixed volume, such as contained in the inside of a pressure vessel, the pressure rises with the temperature. If the chemical reaction is *exothermic*, the temperature of the product is positively causally dependent on the quantity of reactants (steam and hydrocarbon). If the reaction is endothermic, the causal dependency is negative. Let us assume the reaction is exothermic. Then we have

$$Quantity(Steam) \Rightarrow^{+,t} Temperature(Product)$$

$$Quantity(HC) \Rightarrow^{+,t} Temperature(Product)$$

and of course what goes in must come out, so the temperatures also show a positive causal dependency, but without hysteresis:

$$Temperature(Steam) \Rightarrow^{+} Temperature(Product)$$

$$Temperature(HC) \Rightarrow^{+} Temperature(Product)$$

$$Temperature(Catalyst) \Rightarrow^{+} Temperature(Product)$$

5.3 The Causal Control Flow Diagram

Just as we represented the causal factors resulting in an accident by means of a discrete graph, a WBG, so we can also represent them in this continuously-operating system with its control. We call such a graph a *Causal Control Flow Diagram* (CCFD). Because there may be feedback in such systems (occurring, for example, in feedback control), CCFDs with their value-influence factors may have causal loops in them, which in the case of a WBG with its discrete causal factors is not possible.

The CCFD corresponding to the causal influences we have discussed without value-influence annotations is shown in Figure 5.4. The CCFD with value-influence annotations added is shown in Figure 5.5. This CCFD is not the only CCFD we could draw. Node 1 could read simply "*Pressure(Tank)*" because that is the quantity whose value is being changed through the causal flow. That CCFD is more general, and indeed we do this in the modified version in Figure 5.8, but we are primarily interested here in hazard resulting through the pressure exceeding N, so the hazard condition "$> N$" is included, as is the accident event resulting therefrom. It is sometimes helpful to see this when we are trying to move to a system in which the hazard condition is mitigated and the accident does not happen, as we shall see.

Is the CCFD in Figure 5.5 in some sense complete?

- Yes, in the sense that the "leaf" nodes (the nodes without a predecessor) contribute to the hazard (and the accident) in the specified ways, and that the behaviour of these quantities is sufficient to determine whether the hazard condition is achieved or not.
- No, in the sense that not all pertinent properties and relations of SDL 0 are included in the diagram, as we shall see below.

There is a "*stopping rule*" used. I have taken the condition *Fixed Volume V units* in Figure 5.5 as given, and did not attempt to explain this causally further. That is, I stopped here. (You could query, though, whether I used a "rule" in doing so.) I shall change my mind on this shortly.

Is the CCFD in Figure 5.5 in some sense general?

- Yes, in that our focus is a specific accident event caused through a specific hazard. It is general *given that the hazard pertains*.
- No, in the sense we mentioned above, that it could describe more behaviour,

general behaviour, of the system at SDL 0 than just this hazard behaviour. For example, Node 1 could just be *Pressure(Tank)*, rather than *Pressure(Tank)* $> N$, and Node 0 would be absent (we presume), since not all general behaviour of the *Tank* results in a rupture.

We might well want to say that some CCFDs are "*general*" to a given system, and others refer to *specific* behaviour with conditions, captured in node labels, which do not pertain for all behaviours of the system. So the CCFD in 5.5 is specific in this sense: it refers to a specific condition, *Pressure(Tank)* $> N$, and ensuing rupture, that (we hope!) is not present in all behaviours of the system.

In the interests of figuring out how to mitigate the hazard, I now question the stopping rule I used. Note first that there are a couple of pertinent objects included in Figure 5.2 missing from the CCFD in Figure 5.4. Neither *VentPipe1Valve* nor *VentPipe2Valve* are mentioned. Let us call these *Vent1* and *Vent2* for short. They are there present, but apparently closed, and nothing is said about their behaviour, so we may assume they remain closed. But maybe they could be opened? Let us include them. Say, as in Figure 5.6, where they are present and closed, as hinted in Figure 5.1.

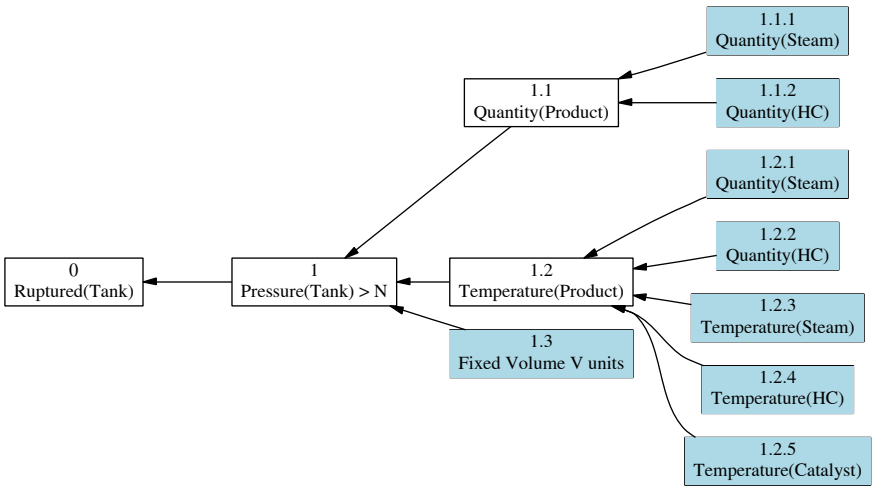

Figure 5.4: The CCFD for the Pressure Tank at SDL 0

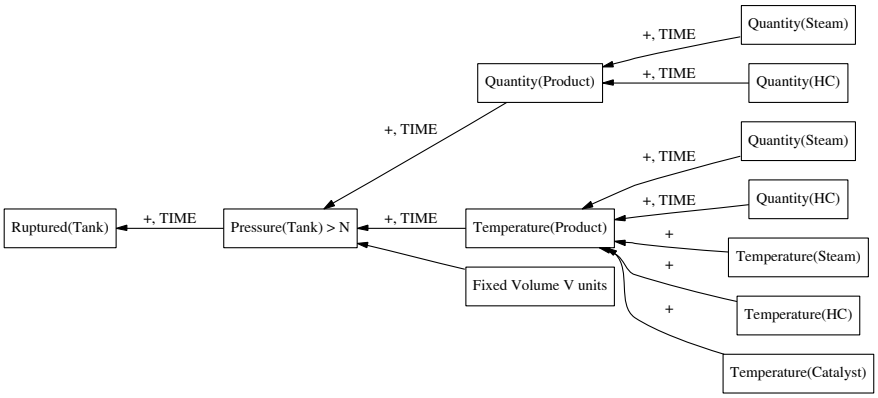

Figure 5.5: The SDL 0 CCFD with Value-Influence Attributes

5.3.1 Analysing the CCFD

Conditions Derived From the Meaning of Causal Factor The CCFD in Figure 5.5 shows the causal influences on the processes in the pressure tank at System Description Level 0 which lead to an accident. There are two consequences of the fact that the causal conditions are all necessary conditions, demonstrable from the meaning of "$\Rightarrow\!\!\!\!\!+$":

discrete factors removing any one of them will lead to avoidance of an accident;

value-influence factors decreasing any one of the monotone-increasing influences in sufficient quantity will lead to amelioration of the conditions causing the accident

Removing a single discrete factor will avoid the accident. However, it is not enough simply to reduce the value of a value-influence factor by itself to avoid the accident, for a number of reasons:

- the lowest value to which one can reduce the factor *simpliciter* may not be enough to avoid the accident by itself, given the unaltered values (of value-influence factors) or (concerning discrete factors) the presence of other factors;
- if one reduces the value of a value-influence factor, it may turn out to be the case that remaining at this reduced value for a longer period of time has a similar effect. Here, if significant overpressure for a short time is capable of

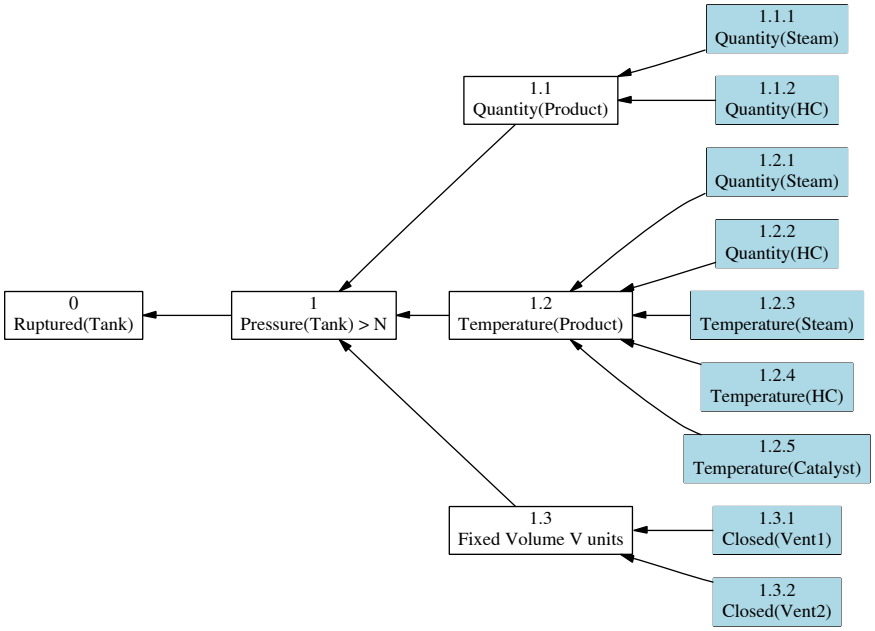

Figure 5.6: The SDL 0 CCFD, without annotations, assuming normal operation (closed vents) but explicitly including the vents

rupturing the tank, then a slightly lower overpressure for a longer period might (generally will) be equally capable of causing a rupture.

One may well have to consider reducing the value of multiple value-influence factors in order to avoid the accident.

How To Proceed We work backwards from the accident through the graph in the reverse direction of the causal arrows. The motivation for this process is that seeing how one may possibly ameliorate the immediate causal factors of an accident is the most direct form of avoiding the accident.

The Top Condition We start at the top, the hazard condition. Can we ameliorate ($Pressure(Tank) > N$) *simpliciter*? We cannot, because it is a value-influence factor, hence we have to look at its causal determinants. These are

- *Fixed Volume V units*
- *Quantity(Product)*
- *Temperature(Product)*

We observe that *Fixed Volume V units* is a discrete factor. We can remove it as a discrete factor by changing the value of V. But then, we generate a new discrete factor *Fixed Volume* V_1 *units* with a different quantity, V_1. We cannot remove *Fixed Volume* as a factor generally; it is always going to be there with some value. We represent the volume here by a symbol representing an unknown, namely V.

What we may be able to do is change its nature. By Boyle's Law, volume is a value-influence factor of pressure, so changing the available volume dynamically will influence the pressure, maybe in a way which might help us reduce risk. And of course there are two factors of the *Volume* in Figure 5.6 by means of which we could do this, namely the vents.

Changing Volume According to Boyle's Law, the volume V is a negative value-influence factor of pressure, the property occurring in the hazard condition. Accordingly, we can consider dynamically increasing V appropriately, to decrease pressure. We can achieve such a dynamic increase in volume, for example, by opening either *Vent1* or *Vent2* in response to an overpressure or high-pressure condition. Let us insert in SDL 1 a mechanism to do this:

- we put *Vent1* under computer control from the pressure sensor in the tank top;
- we put *Vent2* under human operator control; inform the human operator of the pressure via a warning signal (a discrete overpressure warning, or simply a pressure reading dial); and put procedures in place for the operator to open *Vent2* under suitable states of the indicators.

We can then ensure that this measure *by itself* is sufficient to increase the volume enough to remove the factor $Pressure(Tank) > N$ (ideally by reducing the pressure below A).

5.4 Modifying the Pressure Tank: SDL 1

The modified system in configuration SDL 1 is shown in Figure 5.7. The idea is that an overpressure sensor, upon overpressure, sends two signals simultaneously: one to

a computer controller which automatically opens *VentPipe1Valve*, and another to a human operator, which activates a warning (without loss of generality we take this to be a warning light). We take the human operator to react to the warning light by activating a *VentPipe2Valve*-opening device (say a switch or lever). We are not concerned at this stage with the detailed mechanics or psychology of these procedures; just with their highest-level definition.

Additions to OPR We have three new objects, namely *(Overpressure-)Sensor*, *Warn-Light* and *ComputerControl*. The *Sensor* has two states, *Off* and *On*. The *Warn-Light* is similarly *Off* or *On*. The *Operator* may *perceive Off(WarnLight)* as well as *On(WarnLight)* and may *command* either state of *Vent2*. That looks to be all we need here, in the way of objects, but note that the constant factors *Closed(Vent1)* and *Closed(Vent1)* are no longer constant: we can have *Open(Vent1)* and *Open(Vent1)* now also, and *Open(Vent1)* entails $\neg$*Closed(Vent1)*, *mutatis mutandis* for *Vent2*.

We now see another way in which Figure 5.5 is specific. The condition of the valves *Vent1* and *Vent2* is not static - they can be *Open* or *Closed*. Rather than use the cumbersome node label *(Open(Vent1)* $\vee$ *Closed(Vent1))* for this extended state, *mutates mutandis* for *Vent2* , it would generally be convenient to bring in two fluents, *Status(Vent1)* and *Status(Vent2)*, which take values in { *Open*, *Closed* }, and label the corresponding CCFD nodes with these two fluents. I will not do that here, for some visual reasons. I shall shortly want to place a first CCFD (for SDL 1) "on top of" a second CCFD, namely that of Figure 5.6, and observe that two node labels, *Open(Vent1)* in the one and *Closed(Vent1)* in the other, contradict each other and thereby that the CCFDs are incompatible, meaning that in a situation described by the second CCFD, the situation described in the first CCFD, including the hazard and ensuing accident, cannot happen. It makes this visually clear if the incompatible values are retained in the node labels. (In general, though, incompatibilities in OPRA values must be explicitly inferred - they are not all visual.)

5.4.1 Analysing The Modified System

The CCFD for SDL 1 We need to generate the CCFD for the modified system at SDL 1. When the *Vents* are both closed, then the system behaves physically in the way the system at SDL 0 behaves, as illustrated in Figure 5.6. But now they can be opened. By adding the *Vents* and their properties of being *Open* or *Closed* activated by the sensor,

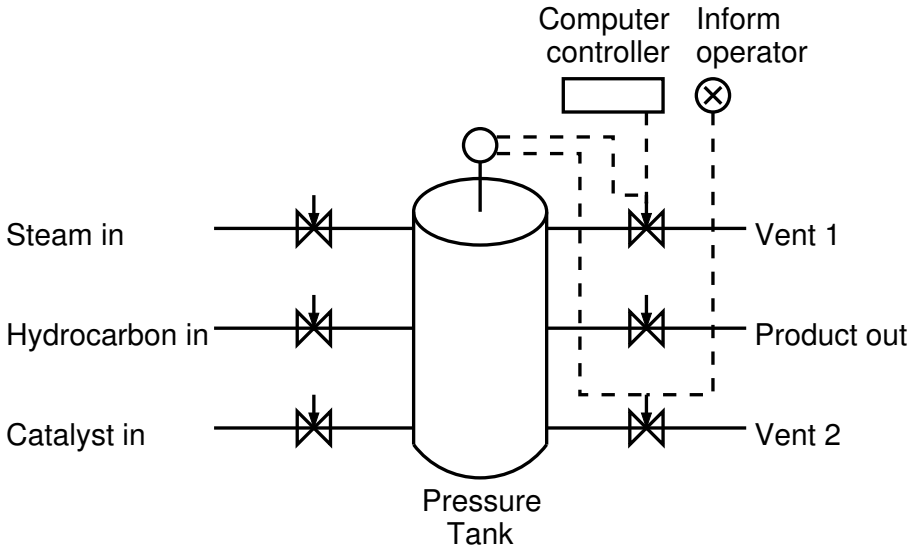

Figure 5.7: The Modified Pressure Tank at SDL 1

we introduce a feedback loop between the hazard condition *Pressure(Tank)* $> N$ and these properties of the valves. The CCFD is shown in Figure 5.8. This CCFD shows only the objects we have already introduced at SDL 0, though, along with the new fluents *Status(Vent1)* and *Status(Vent2)*. Because of quirks of our rendering software, we show the annotations in curly brackets, to draw attention to them and make them easier to read, and also show the negative-influence factor between the *Volume* (node (5)) and the *Pressure* (node (2)) as a double-minus sign.

For visual simplicity, we shall illustrate the remainder of the construction and analysis of the CCFD for SDL 1, with the new mechanisms for opening and closing the vents, just through the sub-CCFD consisting of the relevant factors involved in *Pressure(Tank)*, *Status(Vent1)*, and *Status(Vent2)*. This (sub-)CCFD is in Figure 5.12 (the figure turns out to be lengthy with the annotations included, so we have positioned it at the end of the chapter).

To begin with, we introduced two new discrete factors into the CCFD, namely *Closed(Vent1)* and *Closed(Vent2)*. Concentrating on these as discrete factors led us to consider removing these factors as a way of ameliorating the hazard condition. "Removing" the factors here means changing the *Status* of one or both valves to

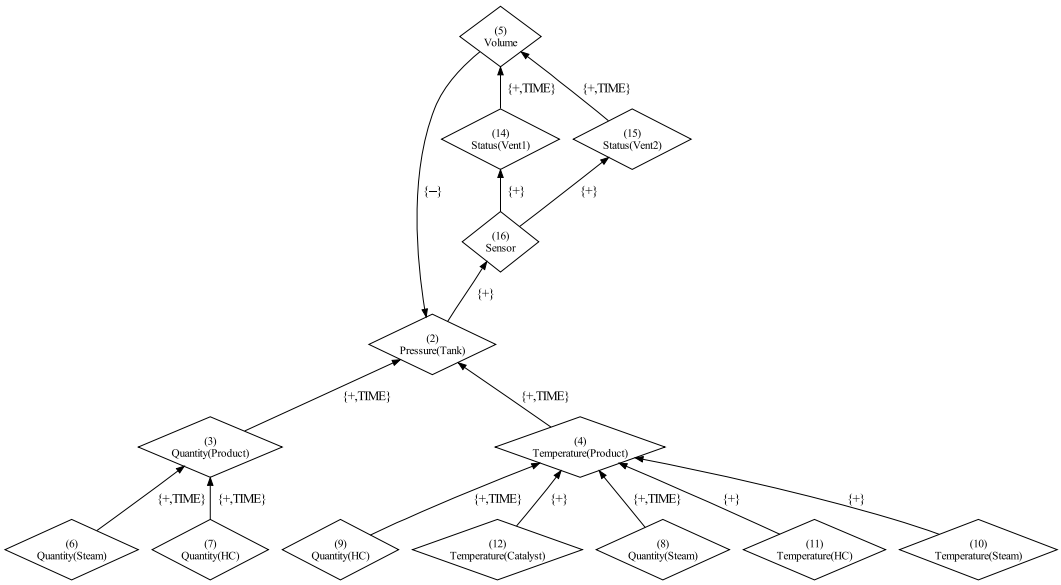

Figure 5.8: CCFD for the Modified Pressure Tank at SDL 1

Open, for this is the property the valves must have if not *Closed* at SDL 1 (we can imagine that further refinements might consider a third state of valves: namely, stuck half-way).

Causal Analysis of the Valves We have modified the system based on an accident scenario, but have not yet performed a full causal influence analysis of the new system. In what follows, for simplicity, we show only part of the CCFD as in Figure 5.12, restricted to the "pertinent" causal subgraph. We also leave out the annotations. The vent-subsystem Causal Control Flow Diagram shows the normal causal operation of the vent subsystem, which is a safety subsystem. And it contains loops (a loop is a sequence of arrows which leads back to itself), denoting what is known in control-system terminology as feedback.

We causally analyse the partial CCFD by considering how the factors influence each other through the form of the partial CCFD. We assign specific values to some of the factors, so technically these factors in the CCFD turn from value-influence factors into discrete factors. We also leave out the arrow-annotations from now on, since they

won't figure further in our reasoning.

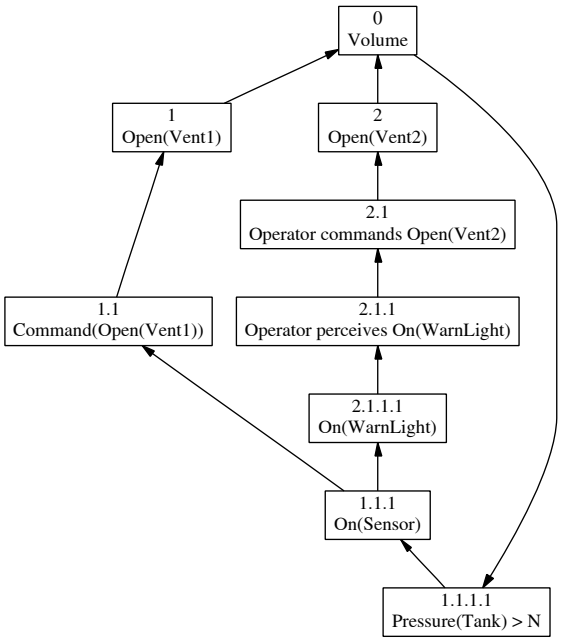

Figure 5.9: The CSD for the Vents in Normal Operation

The Safety Subsystem Function Fulfils Its Purpose Figure 5.9 shows what happens now when the *Pressure(Tank)* becomes larger than N (or larger than A, for that matter, as in the annotation. Also, the node numberings are somewhat different; we may ignore them. I felt it more advantageous to use the prettier picture). The *Sensor* becomes *On*, which turns the *Warnlight On*, which leads to operator action to *Open Vent2*. The *Sensor* becoming *On* also triggers a The *Command* to the automatic system to *Open Vent1*. The *Volume* is increased and, looking back to the annotation of monotone-decreasing value influence, the pressure is thereby reduced. The CCFD in Figure 5.9 thus shows that the vent subsystem fulfils its intended safety function when everything functions correctly.

5.4.2 Causal System Analysis of the Vent Subsystem

From Normal Operation to Failure However, the vent subsystems may themselves fail. We must identify and analyse improper operation of the vent subsystem. The vent-subsystem CCFD is one of normal operation. The system does not function properly, that is, it fails, precisely when one of the causal arrows is "broken", that is, the causal influence is missing, in the case of a discrete factor, or it has null or opposite influence if it is a value-influence factor.

We may completely causally analyse the various failure modes of the event subsystem by removing causal connections (the arrows) one by one from the CCFD, and tracing the causal result, as follows:

- remove the chosen causal link;
- remove all successors of that link up to the point at which another path combines (i.e., up to the first point at which there are two or more in-arrows to a node;
- place the resulting CCFD "over" the accident CCFD (Figure 5.6; that is, match them node-for-node where nodes are the same) and see if they are consistent;
- if they are not consistent with each other, the failure does not result in an accident; if they are consistent with each other, this failure allows the accident to happen

For example, if the arrow between node *On(WarnLight)* and node *Operator perceives On(WarnLight)* is "broken", then the chain from here forwards to the next joint with another chain, which occurs at the *Volume* node, must be removed. This removal is indicated by the dashed lines in Figure 5.10.

After removal, the CID is shown in Figure 5.11. Note that the other chain remains: *Vent1* will still open, volume will be increased, pressure reduced. When this modified CID in Figure 5.11 is placed "over" the accident CID, the nodes *Open(Vent1)* in Figure 5.11 and *Closed(Vent1)* in Figure 5.6, representing the *Status* of *Vent1* contradict. We conclude that the accident is not possible in this scenario, in which the operator does not perceive the warning light and thereby fails to open *Vent2*, but the automatic system for *Vent1* still works.

It is easy to see that removing any single arrow from *Volume* backwards renders the vent-subsystem CCFD still incompatible in this way with the accident CCFD. Hence the modified pressure tank system is immune to failures of the vent subsystem at a single point (removing a single causal arrow, and then subsequent ones up to a join,

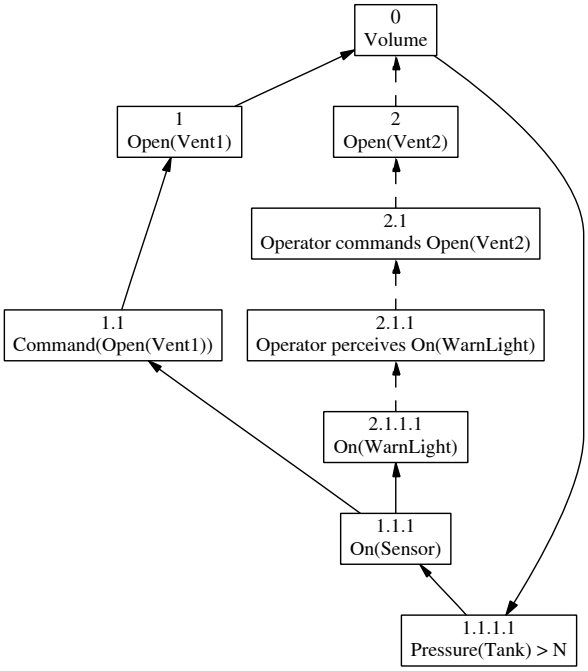

Figure 5.10: Removing a Causal Chain After Breaking a Link

as above). The system we have conceived is thus tolerant of single points of failure.

One Must Consider Multiple "Breaks" The previous operation only dealt with single points of failure of the vent subsystem. One must remove arrows two at a time, three at a time, and so forth in general to obtain a complete analysis. However, from the form of the graph, it is easy to see what those consequences will be. Removing one causal arrow from each parallel chain, will remove both *Open(Vent1)* and *Open(Vent2)*. The resulting diagram will thus be compatible with Figure 5.6, since these are the two nodes in Figure 5.11 which are incompatible with their equivalents in Figure 5.6, and they are now gone. Since the resultant is compatible with Figure 5.6, the hazard condition and thus the accident can happen. It follows that this design is not tolerant of failures in both chains. This much is intuitively evident, of course, but it helps to have a simple formal method as above which allows this analysis even in cases which are not intuitively obvious.

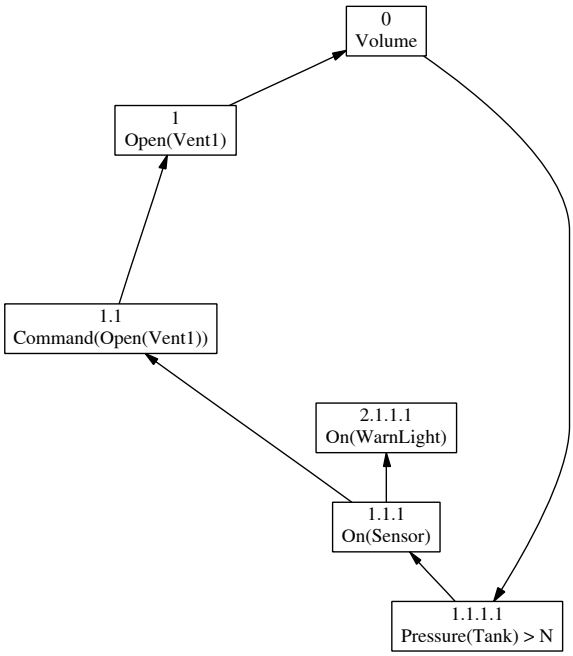

Figure 5.11: The CSD of the Vent Subsystem After Breaking a Link

The safety analysis has thereby produced a general condition both necessary and sufficient for the vent subsystem to be compatible with an accident. One cannot always expect such an analysis to be so clean - this is an example, after all. But certain features stand out:

- it is straightforward to perform an exhaustive analysis like this, even though the combinatorics might be more complex;
- it is easy to check that one's analysis has been exhaustive; since the analysis has been reduced to a formal graph-theoretic counting exercise;
- it is visually much easier to check one's reasoning than, say, to check a fault tree. (We consider fault trees in the subsequent chapter.)

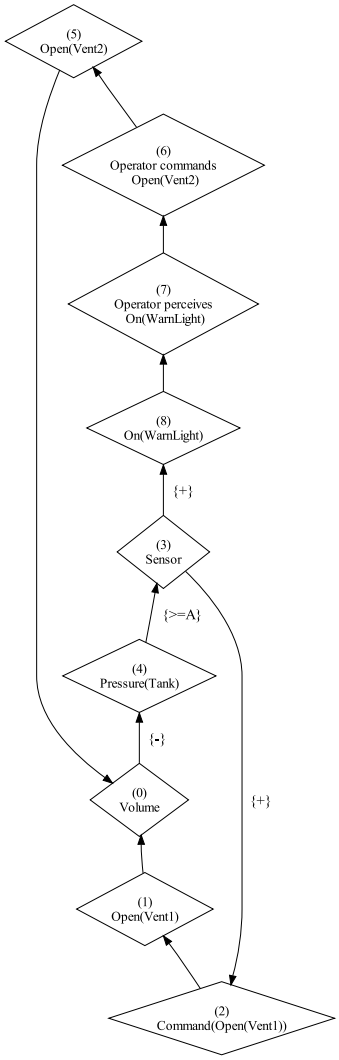

Figure 5.12: Sub-CCFD for the Factors affecting the Status of Vents and the Result on Pressure(Tank)

5.5 Exercises

1. Derive the objects in the preliminary OPR list (Level 0) from the diagram of the pressure tank as given
2. Explain the derivation of the properties and relations of these objects using intuitive physical reasoning
3. Consider a possible refinement of OPR Level 0. Let us call it OPR Level 1.
   - Pipes must connect to the pressure vessel at *joints*.
   - Valves must be installed in pipes at joints.

   Consider the properties and relations now induced by the inclusion of more objects. What would they be? What additional accident events can be defined at Level 1?
4. We have observed that Figure 5.4 is not a general CCFD for SDL 0. Define a general CCFD for SDL 1.
5. We have observed that Figure 5.4 is not a complete CCFD for SDL 0, in the sense that there are causally-related OPRA items at SDL 0 which are not included. Define a complete CCFD, in the sense that as many causal relations amongst SDL 0 OPRA items are included.
6. Is Figure 5.8 a general CCFD for SDL 1? If yes, give your reasons. If no, devise a general CCFD for SDL 1.
7. Provide arguments that the precondition $Pressure(Tank) > NUnits$ *over time* $s < T$ is a hazard condition for the concepts Hazard-1, Hazard-2 and Hazard-4 of hazard also.
8. Show that monotonically-increasing or -decreasing value-influence factors, as well as threshold-triggered and time-triggered value-influence factors can be brought within the counterfactual definition of causal factor.
9. Suppose the OHA is to proceed. What is reasonable to introduce at SDL 2 as a refinement of the abstract pressure tank construction at SDL 0 and SDL 1? How does the causal analysis of the hazard condition at SDL 2 proceed? (That is, perform it!)

Bibliography

[1] Tim Bedford and Roger Cooke, *Probabilistic Risk Analysis: Foundations and Methods*. Cambridge University Press, 2001

[2] Kevin Driscoll, *Murphy Was an Optimist*, ongoing lecture series. Version 19 of the lecture (circa 2010) is available from https://rvs-bi.de/publications/DriscollMurphyv19.pdf, no date.

[3] Kevin Driscoll, Brendan Hall, Håkan Sivenkrona and Phil Zumsteg, *Byzantine Fault Tolerance, from Theory to Reality*, in Computer Safety, Reliability and Security, Proceedings of the 22nd International Conference, SAFECOMP 2003, Lecture Notes in Computer Science volume 2788, Springer-Verlag, 2003. Available from https://www.cs.indiana.edu/classes/p545-sjoh/post/lec/fault-tolerance/Driscoll-Hall-Sivencrona-Xumsteg-03.pdf , accessed 2017-06-14.

[4] R.W. Hazell, G.V. McHattie and I. Wrightson, *Note on Hazard and Operability Studies [HAZOP]*, Royal Society of Chemistry, London, 2001.

[5] Daniel M. Kammen and David M. Hassenzahl, *Should We Risk It?*, Princeton University Press, 1999.

[6] Hiromitsu Kumamoto and Ernest J. Henley, *Probabilistic Risk Assessment and Management for Scientists and Engineers*, Second Edition. IEEE Press, 1996.

[7] Peter Bernard Ladkin, *Causal System Analysis*, ebook, RVS Group, University of Bielefeld, 2001. Available at https://rvs-bi.de/publications/books/CausalSystemAnalysis/index.html , accessed 2016-07-26.

[8] Peter Bernard Ladkin, *Ontological Analysis*, Safety Systems 14(3), Safety-Critical Systems Club, 2005.

[9] Peter Bernard Ladkin, *Causal System Analysis*, electronic edition, RVS 2001.

Available from https://rvs-bi.de/publications/books/CausalSystemAnalysis/index.html , accessed 2017-06-14.

[10] Peter Bernard and Stefan Leue, *Interpreting Message Flow Graphs*, Formal Aspects of Computing 7(5):473–509, 1995. Available from https://rvs-bi.de/publications/abstracts.html#FAC-MSC .

[11] Leslie Lamport, *TLA in Pictures*, IEEE Transactions on Software Engineering SE-21:768-775, 1995. Available at http://lamport.azurewebsites.net/pubs/pubs.html#lamport-pictures , accessed 2017-06-14.

[12] J. L. Mackie, *The Cement of the Universe: A Study of Causation*, Oxford University Press, 1974.

[13] RVS Group, *Train Crash Near Warngau, Germany*, course material, RVS Group, University of Bielefeld, 2008. Available from http://wwwhomes.uni-bielefeld.de/cgoeker/SysSafe/WiSe%2011-12/Cases/TrainHeadOnCollisionWarngau.pdf

[14] Andrew S. Tanenbaum and David J. Weatherall, Computer Networks, 5th edition, Prentice-Hall, 2011.

[15] W.E. Vesely, F.F. Goldberg, N.H. Roberts and D.F. Haasl, *Fault Tree Handbook*, NUREG 0492, U.S. Nuclear Regulatory Commission, 1981. Available from https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0492/

[16] Felix Redmill, Morris Chudleigh and James Catmur J, *System Safety: HAZOP and Software HAZOP*, John Wiley & Sons, 1999.

[17] Bernd Sieker, Systemanforderungsanalyse von Bahnbetriebsverfahren mit Hilfe der Ontological Hazard Analysis am Beispiel des Zugleitbetriebs nach FV-NE, Doctoral Dissertation (in German), RVS Group TechFak and CITEC, Uni Bielefeld, April 2010. Available from https://rvs-bi.de/publications/Theses/Dissertation_Bernd_Sieker.pdf , accessed 2017-06-14.

[18] VDV (2004), *Fahrdienstvorschrift für Nicht-bundeseigene Eisenbahnen (FV-NE)*, (english: *Operating Regulations for Non-Federal Railways*), Verband Deutscher Verkehrsunternehmen (VDV) Ausgabe (edition) 1984.