Chapter 9

Causal Analysis of a Pressure Tank

We have described the ontology of objects and behaviors, states and state predicates, which we use to describe systems and their behavior. We have also introduced intuitively the notion of nearness of behaviors and states, and a formal notion of causality, which can be used with this ontology and the notion of nearness. We claim that the notion of causality is central to system analysis and we demonstrate how by means of an example of a pressure tank in this section.

9.1 Basic Concepts: Object, Properties, Relations

The Pressure Tank The simple pressure tank is shown in Figure 9.1. It

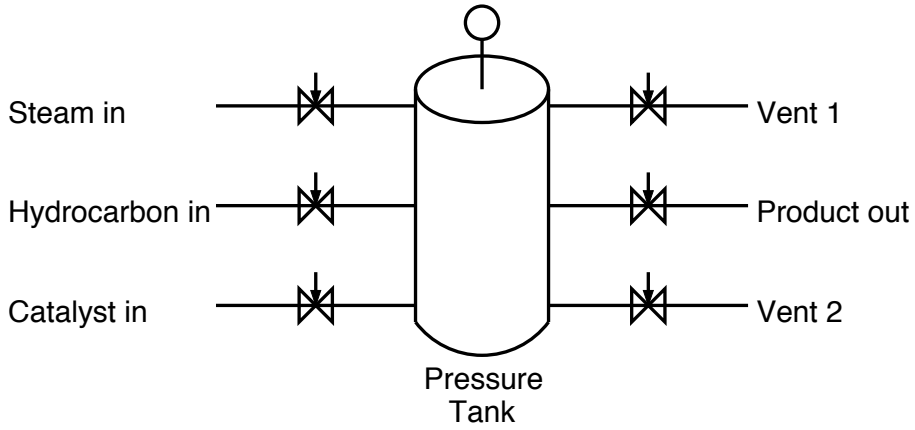

Figure 9.1: The Pressure Tank Without Safety Mechanisms

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 The accident for this analysis is defined to be an explosion of the tank due to overpressure.

Safety Analysis Levels On the level on which the design has been given to us, we can specify certain properties and predicates amongst the components of the system. Examples include 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. We cannot therefore assess the state or behavior of these components, although this might be a significant factor in any real accident behavior. This is why we speak of *levels of analysis*. One cannot infer anything about things one is not given, or properties one is not made aware of. It is essential, however, to determine precisely what one can know and what one cannot know, and assign the latter to a different stage of analysis.

Objects We have quite a few objects, even for so simple an example.

- *Tank*
- *SteamPipe*
- *HCPipe*
- *CatalystPipe*
- *ProductOutPipe*
- *VentPipe1*
- *VentPipe2*
- *TankPressureSensor*
- *SteamPipeValve*
- *HCPipeValve*
- *CatalystPipeValve*
- *ProductOutPipeValve*

- *VentPipe1Valve*
- *VentPipe2Valve*
- *Steam*
- *HC*
- *Catalyst*
- *Product*

Properties The following properties pertain to certain objects.

- *Intact* and its contrary *Ruptured*, to *Tank*, *SteamPipe*, *HCPipe*, *Catalyst-Pipe*, *ProductOutPipe*, *VentPipe1*, *VentPipe2*;
- *Open*, *Closed* and *Partopen*, to *SteamPipeValve HCPipeValve Catalyst-PipeValve 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.

9.2 Causal System Analysis (CSA)

Formal Definition of Accident The accident may then be defined as

$$Ruptured(Tank)$$

What Can Cause The Accident? In this case, we are lucky that the causal antecedents to the accident at this level of analysis are fairly resticted. Indeed, it is a goal of, and a criterion for, a hierarchical division into safety analysis levels that each analysis level allows one to delimit the causal antecedents to events and system states.

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. If we rule out the breach, and an accident occurs, then *the accident would not have happened had there not been overpressure for a particular time in the tank.*

We use the symbol "$\Rightarrow\!\!\!\!\!-$" to denote "*is a causal factor of*". The causal relation between accident and condition we can thus write:

$$Pressure(Tank) > N\,Units\ over\ time\ T \Rightarrow\!\!\!\!\!- Rupture(Tank)$$

In fact, it is much more reasonable to consider the certainty of occurrence of the accident 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, but much more likely is a sustained smaller overpressure. Nevertheless, in order to indicate how a condition may depend on time, without complicating the argument, we consider overpressure above a fixed value over a fixed time interval. The reader should keep in mind, however, that this is a simplification.

Hazard Condition We can thereby intuitively designate $Pressure(Tank) > N$ to be a hazard condition. An accident is not inevitable provided that the pressure is reduced inside a particular time. But that the pressure has been greater than N for some time increases the chances that an accident will occur. The argument is as follows. It rests on certain assumptions, called *stasis* and *temporal strengthening*, which are debatable and by no means universally true without conditions.

Suppose $T = t + s$, that both t and s are non-zero, and the pressure has already been greater than N for time s. Call this the precondition.

- Then the chances that the pressure will continue to be greater than N are equal to or greater than if the the pressure had not been greater than N in previous time. This we call *stasis*.

- The condition for an accident to occur, given the precondition, is that

  $$Pressure(Tank) > N \textit{ for time } t$$

  Since t is less than T it follows from temporal logic that

  $$Pressure(Tank) > N \textit{ for time } T$$

  tense-logically implies

  $$Pressure(Tank) > N \textit{ for time } t$$

  but not vice versa. If A tense-logically implies B but not vice versa, we assume that the a priori probability of B is higher than that of A. This assumption is called *temporal strengthening*.

The chances that an accident will occur given the precondition are thus at least the a priori probability that $Pressure(Tank) > N for\ time\ t$ (and possibly raised by stasis). Temporal strengthening says that this is greater than the a priori probability that $Pressure(Tank) > N for\ time\ T$, which is the a priori

probability that an accident will occur tout court, given the causal dependence of the accident on this condition.

It follows that the accident is more likely to occur, given the precondition. Therefore the precondition is a Hazard-3.

A simple argument that the precondition or some transformation of it fulfils one of the other hazard conditions seems difficult to obtain. But the assumptions of stasis and temporal strengthening are crucial even to the argument that the overpressure condition is a Hazard-3.

Causal Factors of the Hazard The hazard condition is unusual in that there is just one condition which leads to an accident. We now inquire about the causal factors of the hazard condition.

Knowledge of the gas laws tells 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 (which must be justified through chemical knowledge), that the pressure of the product rises as the hydrocarbon and steam convert into 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 F, just in knowing that it is monotone increasing with its arguments. We may summarise this causally as

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

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

The superscript indicates the monotonic increasing dependency of values, as well as the *hysteresis*, the lag in time of the effect.

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.

We have moved from a simple counterfactual definition of causality to describing a causal tendency:

- not only that one extensively-measurable state predicate (or fluent, as we have called it) 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:

- that these specific four features may be brought within the counterfactual definition in a straightforward way, for example
- we have shown by example how time-triggering may be handled in our discussion of the condition *Pressure*(*Tank*) > *N for time T* above, and
- these qualitative features of quantitative causal regularities are (with maybe some others) all that is needed for an adequate causal analysis for safety purposes.

This last point can be taken to suggest that so-called Qualitative Physics, as studied for example under "Common-Sense Physics" by AI researchers, can have a role to play in the future in adequate causal analyses for safety. This field is still quite young, however.

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

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

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

From now on, we shall 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 shall 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

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

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

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

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

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

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

9.3 The Causal Influence Diagram

The Causal Influence Diagram (CID) We can represent the causal influences we have derived so far as a graph, which we call a *Causal Influence Diagram* (CID).

9.3.1 Generating the CID from CI-Script

Software cid2dot We have software *cid2dot* which automatically builds a CID from a specification in *CI-Script*, using the *dot* graph-layout tool from AT&T Research. Figure 9.2 shows the CI-Script for the analysis we have performed so far.

```
[0] /* Ruptured(Tank) */
    [1] /* Pressure(Tank) > N // +, TIME */
[1] /\ [-.1] /* Quantity(Product) // +, TIME */
    /\ [-.2] /* Temperature(Product)  // +, TIME */
    /\ [-.3] /* Fixed Volume V units */

  [1.1] /\ [-.1] /* Quantity(Steam) // +, TIME */
        /\ [-.2] /* Quantity(HC) // +, TIME */

  [1.2] [-.1] /* Quantity(Steam) // +, TIME */
  [1.2] [-.2] /* Quantity(HC) // +, TIME */
  [1.2] [-.3] /* Temperature(Steam) // + */
  [1.2] [-.4] /* Temperature(HC) // + */
  [1.2] [-.5] /* Temperature(Catalyst) // + */
```

Figure 9.2: The CI-Script for the Pressure Tank CID

The resulting CID is shown in Figure 9.6. Because the labels are somewhat obscured (we have not finished modifying the code from its use for generating WB-Graphs yet), we include another version generated by *dot* from hand-prepared

input. This version, which is intended to be identical, but with the labels drawn felicitously on the causal relations (arros) instead of obscurely in the nodes, is shown in Figure 9.7.

9.3.2 Analysing the CID

Conditions Derived From the Meaning of Causal Factor The CID shows the causal influences on the processes in the pressure tank at this System Level 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, because 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 presence (of discrete factors) of other factors. In this case, one may 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 can ameliorate the immediate causal factors of an accident is the most direct form of avoiding the accident that presents itself.

The Obvious Top Condition We proceed therefore by considering whether we can 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 by changing the value of V. But by Boyle's Law, volume is a value-influence factor of pressure, so we cannot ameliorate the accident simply by picking any old value of V.

Changing Volume According to Boyle's Law, the volume V is a negative value-influence factor. Accordingly, we can consider increasing V appropriately. We can do this, for example, by opening either *Vent1* or *Vent2*. Let us build in 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 ensure that this measure *by itself* is sufficient to increase the volume enough to remove the factor $Pressure(Tank) > N$.

We have then designed the system in Figure 9.3.

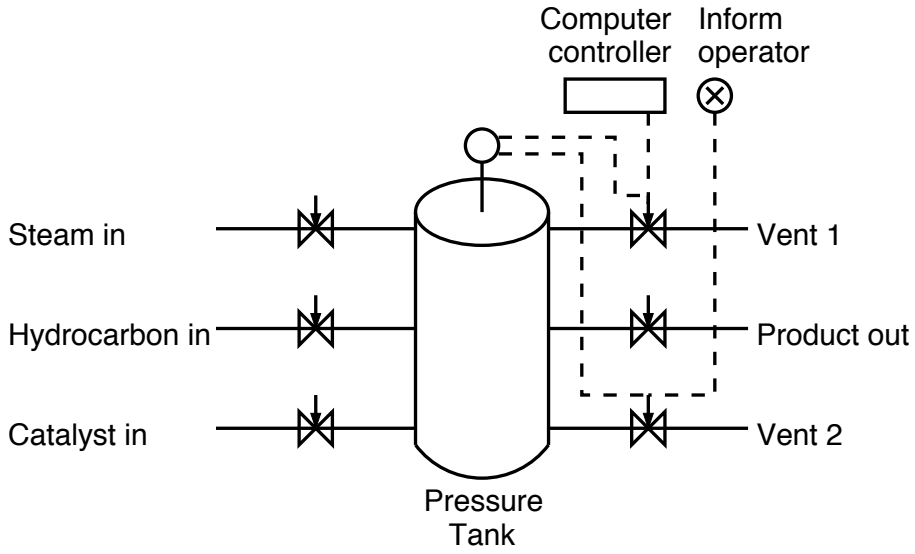

Figure 9.3: The Modified Pressure Tank

9.3.3 Analysing The Modified System

The CID The CI-Script for the modified system is shown in Figure 9.4, and the CID thereby generated in Figure 9.8. Again, a *dot* version from hand input is shown in Figure 9.9.

```
[0] /* Ruptured(Tank) */
    [1] /* Pressure(Tank) > N // +, TIME */
[1] /\ [-.1] /* Quantity(Product) // +, TIME */
    /\ [-.2] /* Temperature(Product)  // +, TIME */
    /\ [-.3] /* Fixed Volume V units */

  [1.1] /\ [-.1] /* Quantity(Steam) // +, TIME */
        /\ [-.2] /* Quantity(HC) // +, TIME */

  [1.2] [-.1] /* Quantity(Steam) // +, TIME */
  [1.2] [-.2] /* Quantity(HC) // +, TIME */
  [1.2] [-.3] /* Temperature(Steam) // + */
  [1.2] [-.4] /* Temperature(HC) // + */
  [1.2] [-.5] /* Temperature(Catalyst) // + */

  [1.3] [-.1] /* Closed(Vent1) */
  [1.3] [-.2] /* Closed(Vent2) */
```

Figure 9.4: The CI-Script for the Modified Pressure Tank

Ameliorating the Factors Reconsidered We have introduced two new discrete factors into the CID, namely *Closed(Vent1)* and *Closed(Vent2)*. So, concentrating on the discrete factors leads us to remove these factors as a way of ameliorating the hazard condition. This will work, but leads us to a new accident analysis.

Causal Analysis of the Valves We have modified the accident scenario, but have not yet performed a full causal influence analysis of the new system. The analysis is specified in CI-Script in Figure 9.5, and the CID generated is shown in Figure 9.10. A hand-prepared-input *dot* version is shown in Figure 9.11.

The vent-subsystem causal analysis shown in the Causal Influence Diagram is not a causal analysis of an accident, as the other diagrams were. It shows the normal causal operation of the vent subsystem, which is a safety subsystem.

The Safety Subsystem Function Fulfils Its Purpose It may be seen directly by comparing the CIDs in Figures 9.9 and 9.11 that the vent subsystem fulfils its intended safety function. Place similarly-labelled nodes on top of each other, namely the *Pressure*(*Tank*) $> N$ and *Volume* nodes, and look at the precursors of the volume nodes. Both of them, in both diagrams, involve the objects *Vent*1 and *Vent*2. However, the predicates in the accident CID are contraries of those in the vent-subsystem CID ("contrary" means that it is not possible for them both to be true at the same time of the same object). That means

```
[0] /* Volume */
    /\ [1] /* Open(Vent1) // +, TIME */
    /\ [2] /* Open(Vent1) // +, TIME */

[1] /\ [-.1] /* Command(Open(Vent1)) */

  [1.1] /\ [-.1] /* On(Sensor)  */

    [1.1.1] /\ [-.1] /* Pressure(Tank) > N  */

         [1.1.1.1] [0]

[2] /\ [-.1] /* Operator commands Open(Vent2)  */

  [2.1] /\ [-.1] /* Operator perceives On(WarnLight)  */

    [2.1.1] /\ [-.1] /* On(WarnLight)  */

      [2.1.1.1]  [1.1.1]
```

Figure 9.5: The CI-Script for the CID of the Vents

simply that the intended operation of the vent subsystem precludes the situation described in the accident CID; they are incompatible. Since the relevant state predicates are discrete predicates, their falsity ensures that the accident cannot happen, as explained above. Hence the vent-subsystem CID demonstrates visually and directly that the discrete state predicates of the vents, required for an accident to happen, do not pertain when the vent subsystem operates as designs. Ergo, the accident cannot happen.

9.3.4 Causal System Analysis of the Vent Subsystem

From Normal Operation to Failure We have not yet identified improper operation of the vent subsystem. The vent-subsystem CID is a CID of normal operation. The system does not function properly, it fails, precisely when one of the causal arrows is "broken", that is, it is not there in the case of a discrete factor, or it has null or opposite influence if it is a value-influence factor. These may be considered one at a time from the CID, and their causal influence traced, 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 CID "over" the accident CID as before and see if they are consistent;
- if they are not consistent, the failure does not result in an accident; if they are consistent, this failure allows the accident

For example, if the arrow between node `[2.1.1.1] On(WarnLight)` and node `[2.1.1]: Operator perceives On(WarnLight)` is "broken", then the chain from here forwards to the next joint with another chain, at the `Volume` node, must be removed. This chain is indicated by the dashed lines in Figure 9.12. After removal, the CID is shown in Figure 9.13. Note that the other chain remains: `Vent1` will still open, volume will be increased, pressure reduced. When this modified CID in Figure 9.13 is placed "over" the accident CID, the nodes `Open(Vent1)` and `Closed(Vent1)` still contradict. The causal link we removed represents the case in which an operator did not perceive the warning light. Heshe did not thereby act to open `Vent2`.

It is easy to see that removing any single arrow from `Volume` backwards renders the vent-subsystem CID still incompatible with the accident CID. Hence the modified pressure tank system is immune to single-point failures of the vent subsystem.

One Must Consider Multiple "Breaks" The previous operation only dealt exhaustively with single failures 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. Any pair of arrows removed, one from each parallel chain, will remove both `Open(Vent1)` and `Open(Vent2)` and the resulting diagram will be compatible with the accident CID.

It is easy to see that a pair of arrows removed from both chains is both necessary and sufficient to render the vent subsystem compatible with the accident CID, by the "placing over" test.

The safety analysis thereby explicitly produces a general condition both necesary 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 easy to see how to perform an exhaustive analysis, even though the combinatorics might not always be so felicitous;
- it is easy to check that one's analysis has been exhaustive; since this is merely a graph-theoretic counting exercise;

- it is visually much easier to check one's reasoning than, say, to check a fault tree.

A Comparison With Fault Tree Analysis For comparison, to substantiate especially the last point above, a fault tree from [Lev95, Figure 14.5, p331] for this system is shown in Figure 9.14.

Fault Tree Analysis (FTA) is not based upon a formal notion of cause. So there is no means of checking its correctness except through informal inspection by experienced practioners. The advantage of FTA seems to be threefold:

- to perform an FTA, one has to inspect a system and its components thoroughly. Any thorough inspection is bound to help highlight inadequacies in system design, including safety inadequancies.
- FTA has developed graphical methods of handling system decompositions into components, which enables one to combine FTAs performed independently over an adequate decomposition.
- There is long experience with FTA, and its strengths and weaknesses are known, as well as a "library" of individual ways of handling specific cases which can be drawn on by other users

These advantages are not to be sneezed at. However, the advantages of basing an analysis method on a formal notion of causal factor are also important:

- one has a formal criterion for correctness;
- it is in principle possible to develop criteria for completeness;
- although CIDs have to be constructed by hand by analysts, in principle checking them against each other can be automated, since it is based on logical consistency methods

That is, the use of the formal notion of cause means that correctness checking and analysis of safety mechanisms such as we have described can be automated. This cannot be done with FTA.

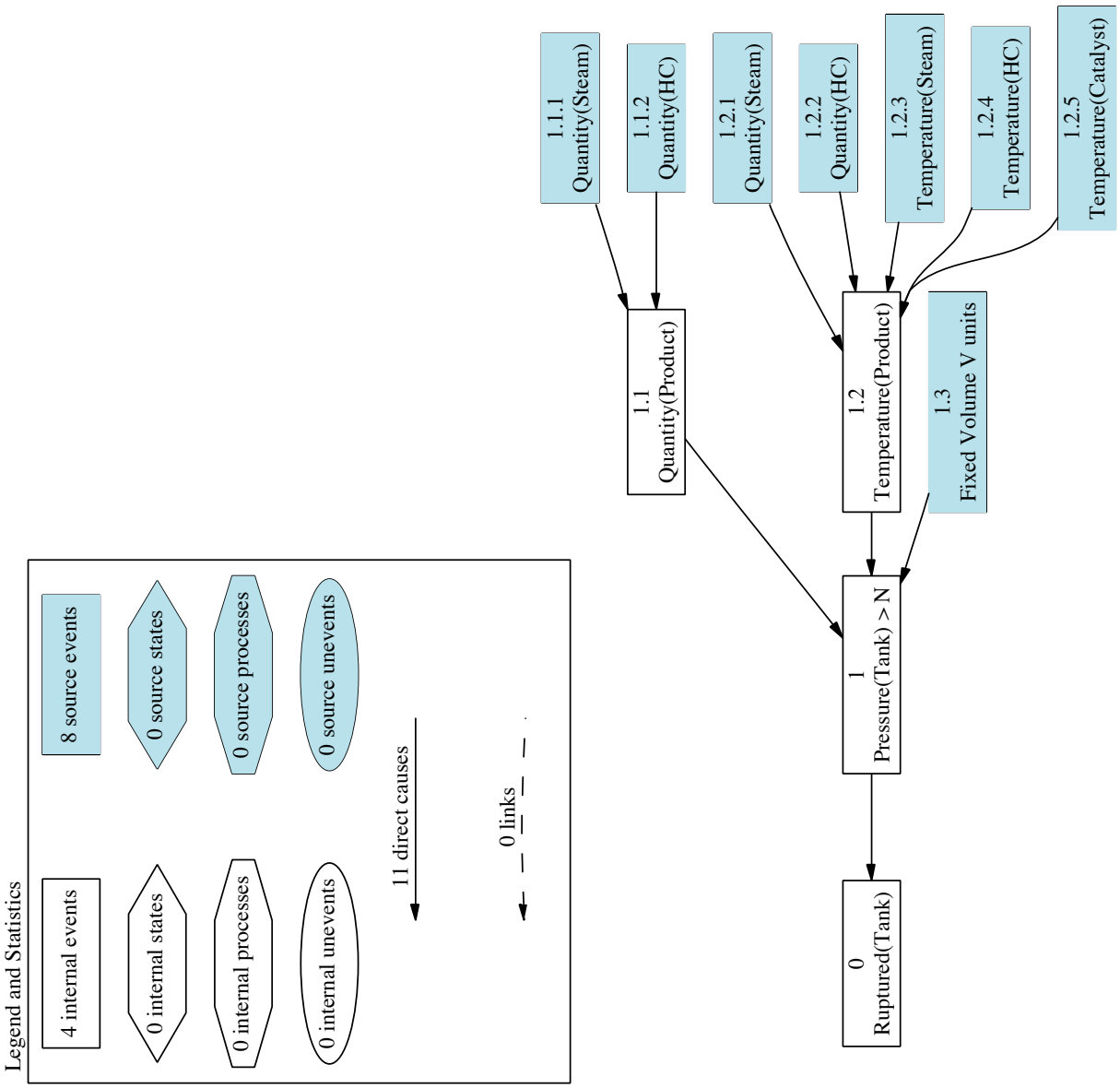

Figure 9.6: The CID for the Pressure Tank

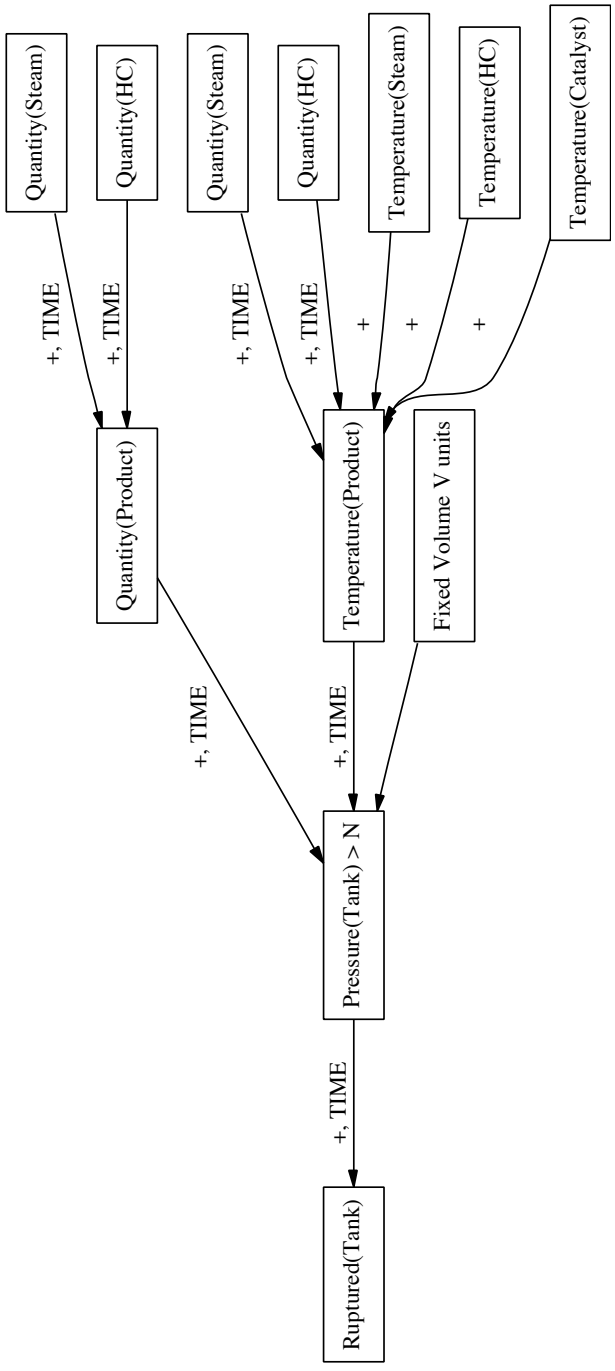

Figure 9.7: The CID for the Pressure Tank: Version 2

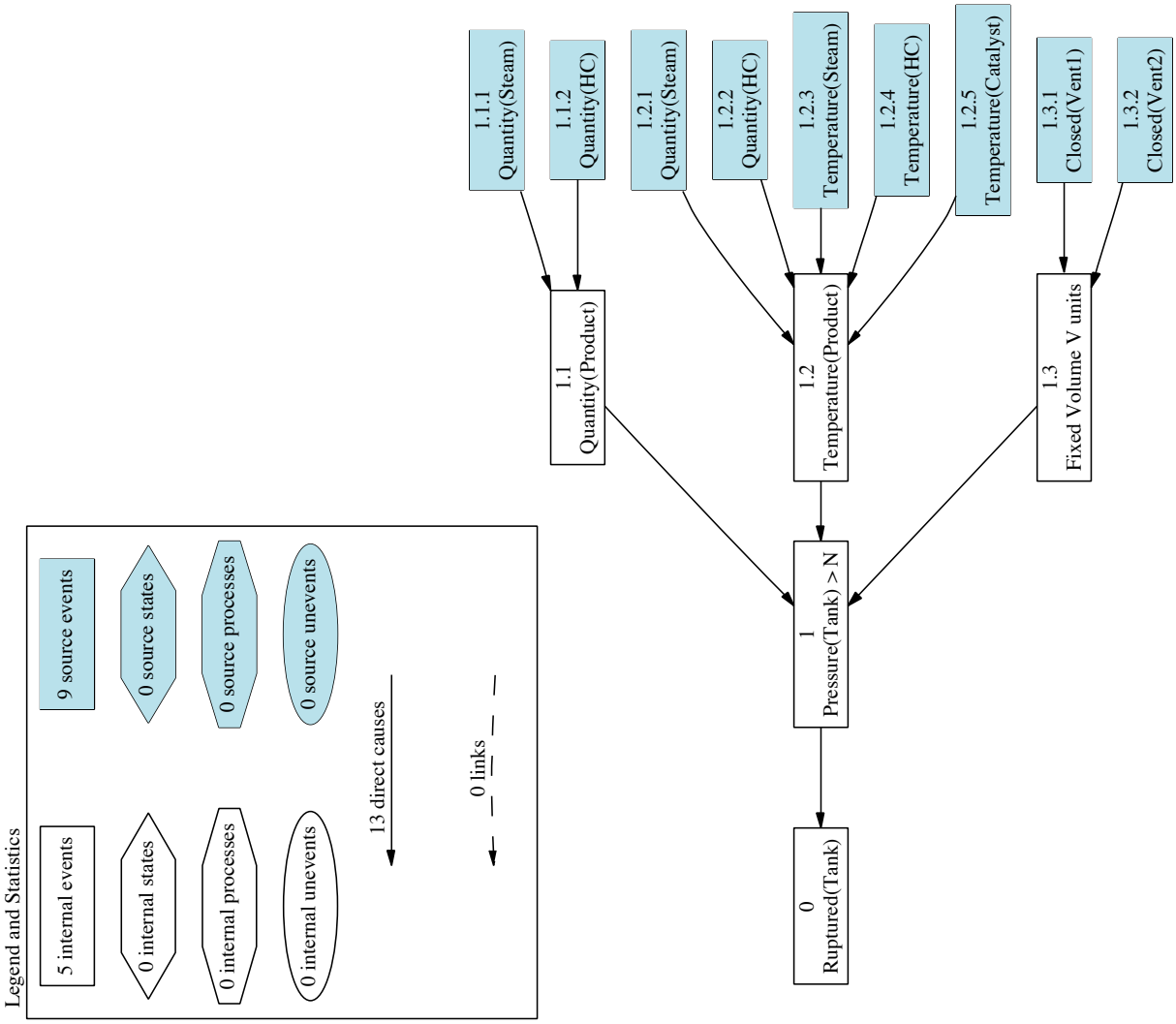

Figure 9.8: The CID for the Modified Pressure Tank

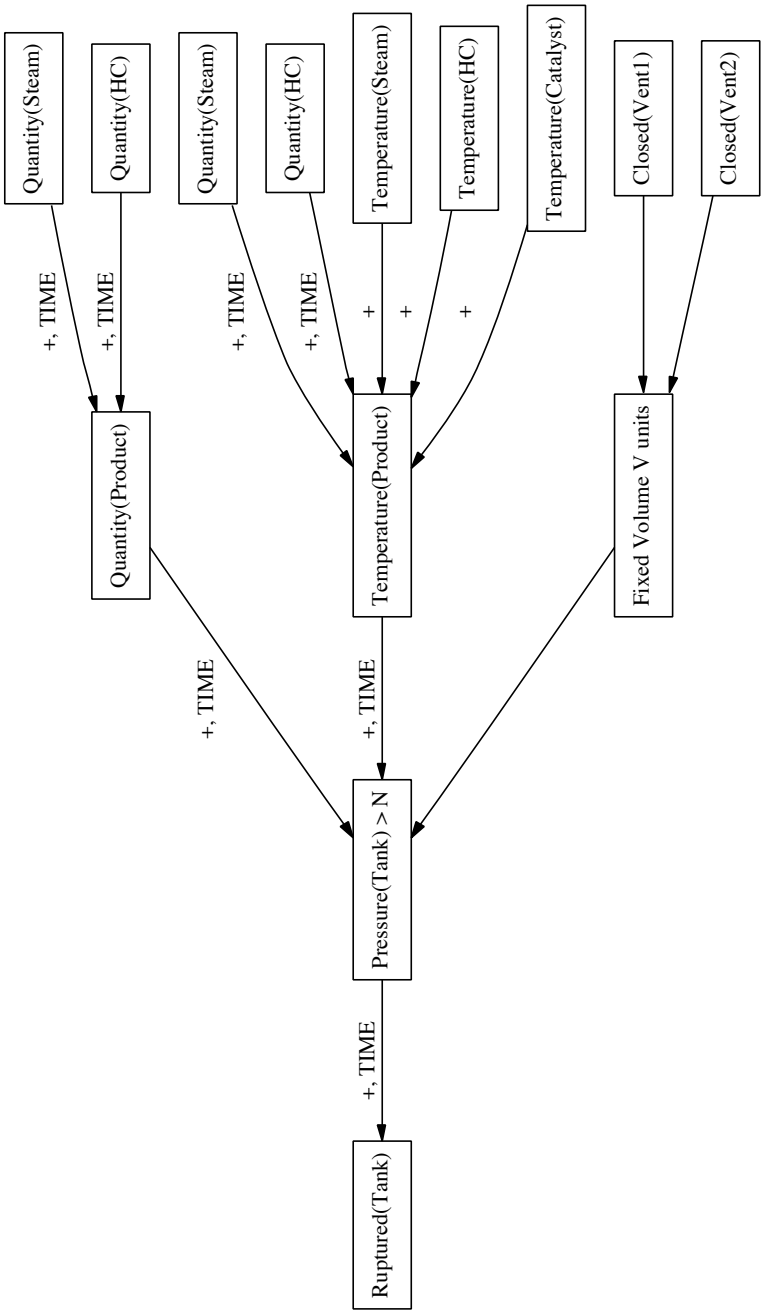

Figure 9.9: The CID for the Modified Pressure Tank: Version 2

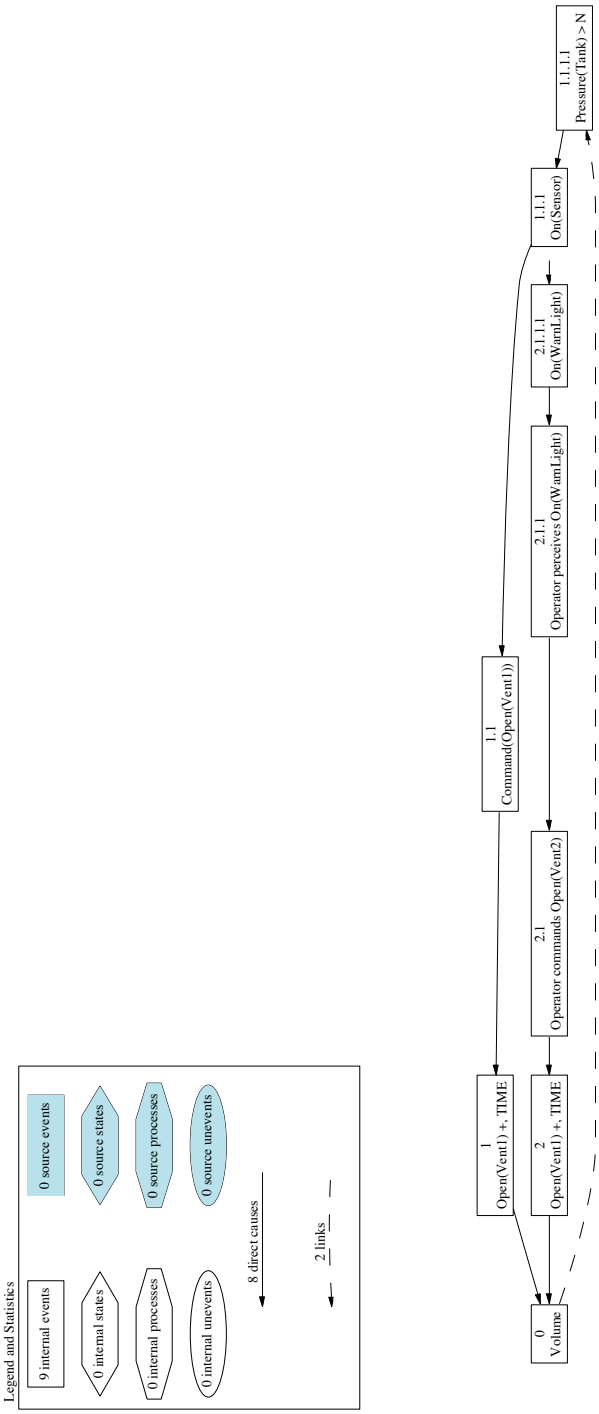

Figure 9.10: The CID for the Vents

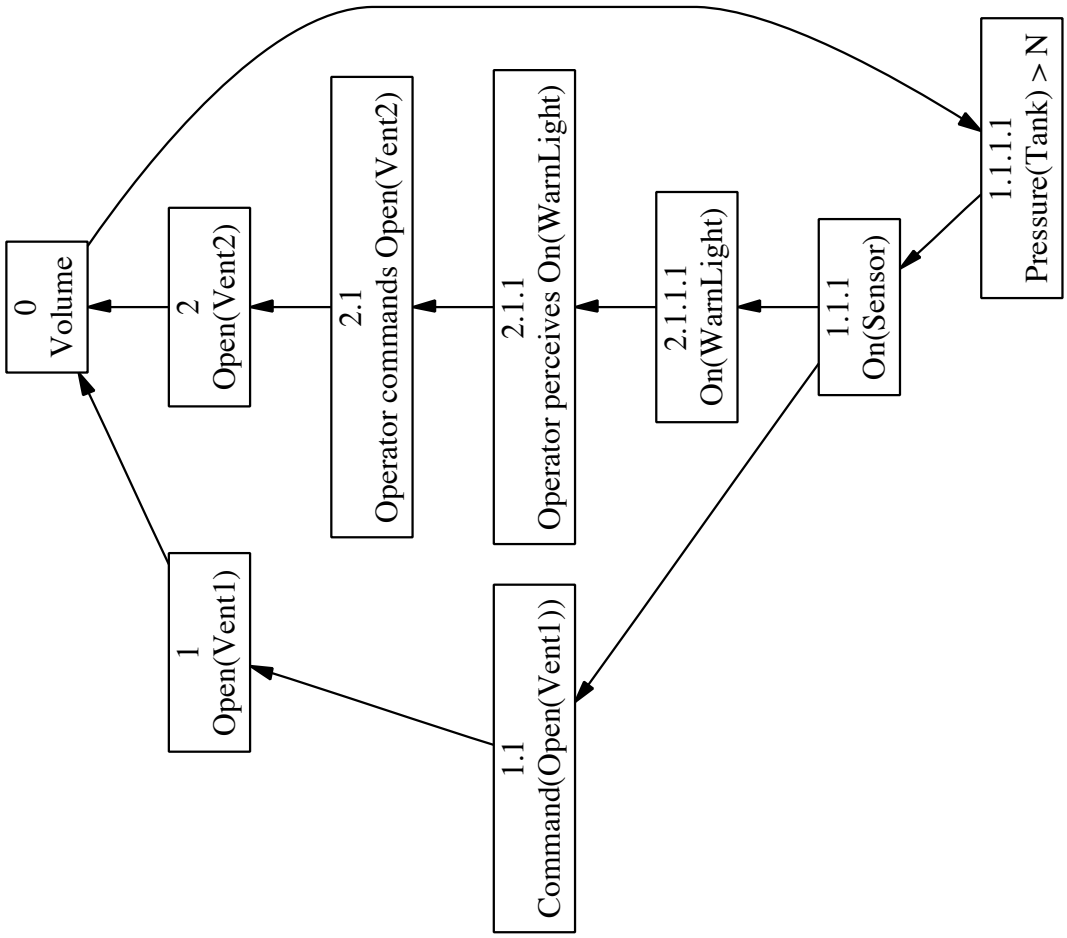

Figure 9.11: The CID for the Vents: Version 2

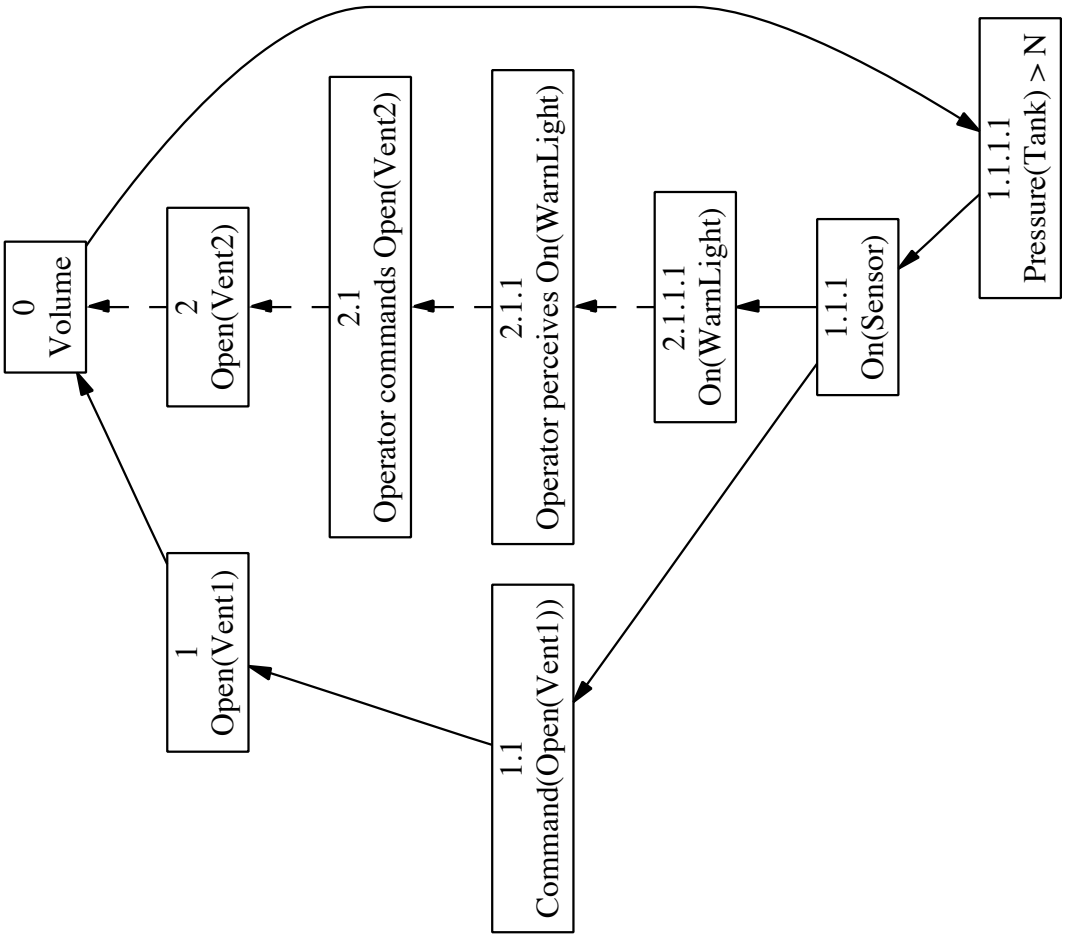

Figure 9.12: Removing a Causal Chain After Breaking a Link

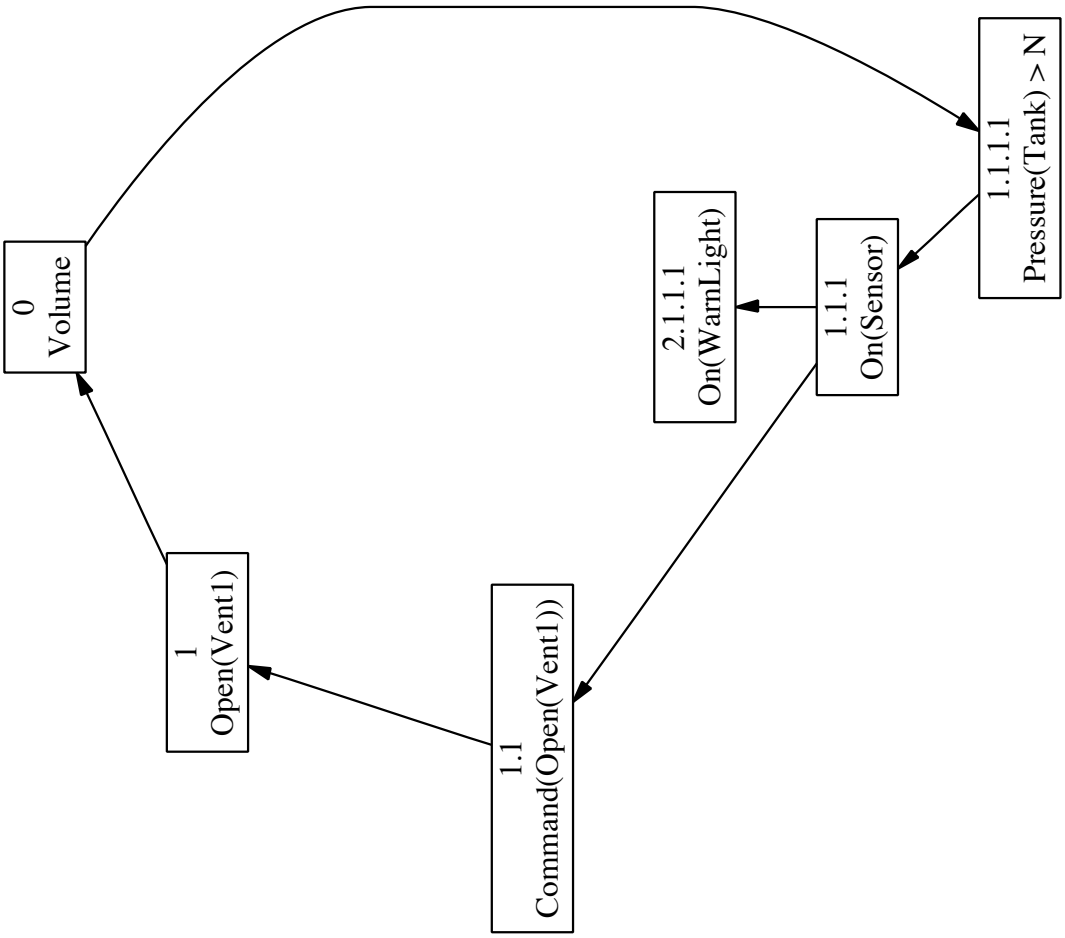

Figure 9.13: The CID of the Vent Subsystem After Breaking a Link

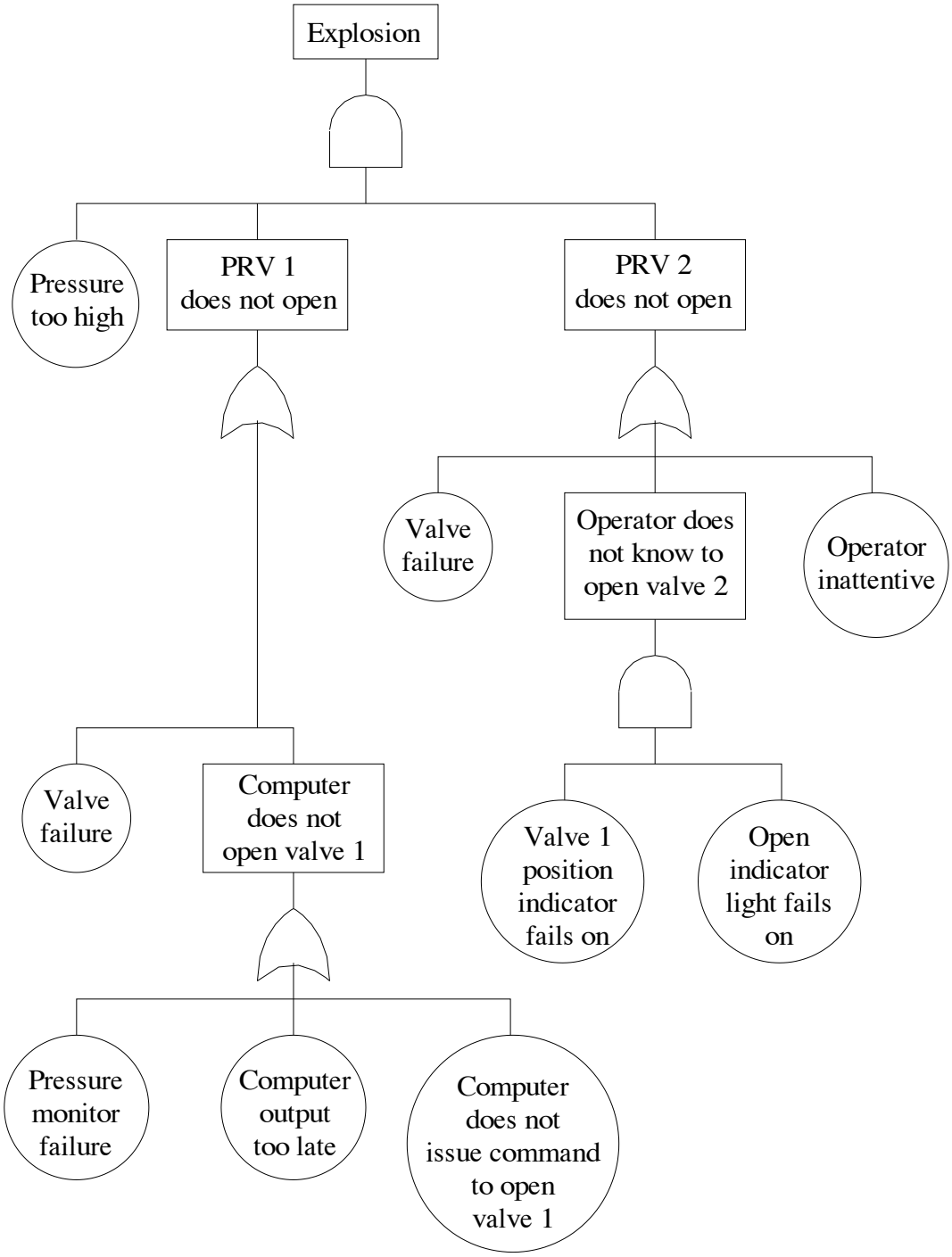

Figure 9.14: The Fault Tree for the Pressure Tank