2 Hidden Functions

2.1 Introduction

Having established the critical importance of hidden functions and failures in real-world incidents in the previous chapter, this section goes on to define the general concepts used in the analysis of hidden functions and failures.

It also looks at some of the subtleties of hidden and evident functions and tries to answer an apparently simple question: when is a function evident, and when is it hidden?

2.2 When is a Function or Failure Hidden?

Hidden functions are conditional

A hidden function is *conditional*: it only comes into play on condition that a second event occurs. For this reason, typical hidden function statements can be recognised by words similar in meaning to those in the list below.

if	To shut down the turbine **if** its rotational speed exceeds 15000 rpm
capable of	To be **capable of** sounding an audible alarm if the storage tank liquid level rises above 2.5m from the tank base
in the event that	To bring the train to a safe stop **in the event that** the driver fails to respond to the audible and visual alarms

A protective device carries out its hidden function if a second event occurs; this is the *trigger event* or *initiating event*. The most obvious trigger is the failure of other components or equipment, but it could be the result of anything that does not occur during normal operation, including the following.

- Human error
- Loss of an external service such as electrical power, gas, cooling or heating services
- Failure of a control system
- External factors such as vehicle impact, severe weather, earthquakes and so on

The table below lists a number of typical protective systems, their associated functions and the trigger events that cause the protective system to operate. The final column is the overall function statement for the protective device; the trigger event is shown in *italics*.

Protective System	Carries out this function	...if this trigger event occurs	Function statement
Emergency stop switch	To stop the can filling line	*Any one of 10 emergency stop buttons is pressed*	To stop the can filling line if *any one of 10 emergency stop buttons is pressed*
Carbon monoxide gas alarm	To raise an audible and visible alarm	*The carbon monoxide concentration exceeds 400 ppm for 10 minutes*	To raise an audible and visible alarm if *the carbon monoxide concentration exceeds 400 ppm for 10 minutes*
Boiler pressure relief valve	To relieve excess boiler pressure	*Boiler pressure exceeds 10 bar*	To be capable of relieving excess boiler pressure if *it exceeds 10 bar*
Residual current device (RCD) or ground fault circuit interrupter (GFCI)	To interrupt the power supply within 40 milliseconds	*The imbalance between live and neutral line currents exceeds 10mA*	To interrupt the power supply within 40 ms if *the imbalance between live and neutral line currents exceeds 10mA*

Failure of the hidden function by itself has no consequences

First we need to be clear what "consequences" are. In this context, consequences include anything that could be observed by the equipment operators, not just the failure's direct effects on production output or safety.

Because the trigger event is not expected to occur during normal operation, the hidden function can never be activated unless something unusual happens. As a result the hidden function is never triggered in normal circumstances, and the hidden failure *by itself* has absolutely no consequences at all.

If a protective device is in a failed state when an initiating event occurs, then of course the outcome is very different. The resulting consequence is a *multiple failure*, the event that the protective device was intended to prevent.

No one will notice the effects of a hidden failure

It follows from the last section that when a hidden function fails, no one who is involved in operating the equipment notices any effects. As we have already said, these are not only effects on production or safety; they include any effects, including "fail safe" features that may have been designed to make the hidden failure evident.

This part of the definition can be confusing if you think about it hard enough. How can a device or system that has failed have absolutely no effects at all? How would we ever be able to diagnose a problem? To take a real example, could the failure of a pressure relief valve really be considered hidden if I could just walk past and see solidified product around it that would prevent it from operating correctly?

This is where the definition needs to be more precise. Of course, hidden failures do have some consequences: at very least, some part of the protective device has failed, and perhaps we could work out that the failure had occurred by inspection, by shaking the device or by dismantling it. But we are not talking about whether the failure can be found through maintenance intervention: the question is whether the failure would be noticed during normal operation, without equipment maintenance and without an engineer specifically looking for the problem. If there would be no effects under normal conditions, the failure is hidden.

The importance of time

There is one last factor to take into account: time.

Failure effects do no have to appear immediately for a failure to be classified as evident.

For example, if the filter in a cooling water supply is blocked, its effects may not become evident until there is a demand on the cooling system. It could take some time for the process that uses cooling water to overheat; in fact, it could be hours or even days before the problem comes to light. Is the filter blockage hidden? No, because its effects become evident *eventually*, even if the immediate effects are negligible or non-existent.

This rule may seem contrived, but it is not difficult to remember: a failure is evident if the operating staff *eventually* become aware of its effects when *everything else is operating normally*. So the filter blockage is evident, because eventually it causes the downstream process to overheat. On the other hand, failure of a fire alarm to detect fires is hidden because fires are not part of normal operating conditions.

2.3 Hidden Failures: a Definition for RCM Users

The previous sections have laid down these principles for defining a hidden failure.

1 A hidden failure by itself has no effects

2 The effects of a hidden failure only become evident if a trigger event occurs which would normally cause the hidden function to operate

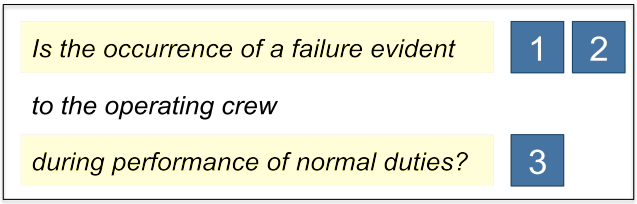
3 The only failure effects that count are those observed by the operations staff carrying out their normal duties

4 Even if it is not possible to diagnose exactly which failure has occurred from its effects, the failure is still evident. To be hidden, a failure must have no effects at all when it occurs on its own.

5 A failure whose effects appear eventually under normal circumstances is evident, not hidden

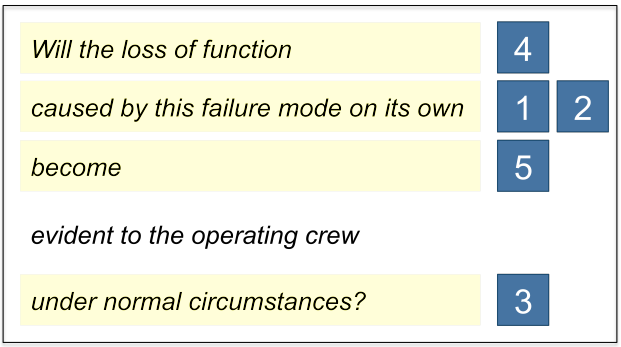
Every Reliability-centred Maintenance decision diagram includes a flowchart that identifies hidden failure modes. Finding the question is easy: it is usually the longest and most complex because it tries to embody all five of the principles above in a single sentence.

First, here is the original question from the Nowlan and Heap[1] decision diagram.



This embodies principles 1, 2 and 3, but it does not capture them all, and it does not capture principles 1 and 2 as well as it could.

The most complete and carefully considered definition of an evident failure in RCM is probably that in the RCM 2 Decision Diagram[2].



The RCM 2 definition introduces the idea of time ("*become* evident…") and focuses on the loss of function rather than the failure itself; it is the effects of failure that have to be evident, not the ability to diagnose the failure. Even so, it is probably impossible to compress all the subtleties of hidden failures into one sentence. Whichever definition you use, most failures are easy to categorise as either hidden or evident; you will only need to use the whole checklist for a tiny proportion of failure modes.

2.4 Failure Modes

So far this chapter has considered only one aspect of protective device failure: the loss of the primary protective function. However, even the simplest device can usually fail in at least two ways. One failure mode causes loss of the protective function (and is therefore hidden), while the second failure mode incorrectly triggers the protective action in normal circumstances, usually resulting in evident consequences.

The list below shows some simple examples.

Protective System	Failure Mode	What happens if the failure occurs
Emergency stop switch	Is incapable of stopping the canning line when an emergency stop switch is pressed	No effects in normal circumstances. Someone could be seriously injured if the emergency stop were needed to protect someone from running equipment
	Shuts down the canning line when no one has pressed an emergency stop button	Interrupts production and may result in significant product loss.
Carbon monoxide (CO) gas alarm	Cannot raise an audible alarm when CO concentration exceeds 400 ppm for 10 minutes	No effects if the CO concentration is normal. People could be injured or killed by high undetected CO levels if a burner or flue malfunctioned.
	Raises an audible alarm when CO concentration is normal	A spurious alarm could cause evacuation of personnel and a shut down of equipment until it has been inspected.
Boiler pressure relief valve	Is incapable of relieving boiler pressure above 10 bar	No effects unless the boiler pressure rises to abnormal levels, when it could explode
	Relieves at normal boiler pressure, allowing steam to escape	Allows steam to escape at normal boiler pressure, affecting production
Residual current device (RCD/ GFCI)	Is incapable of interrupting the power supply within 40 milliseconds if live and neutral currents are out of balance	No effects under normal conditions. If an unintended short to earth occurs, personnel could be seriously injured or equipment damaged.
	Interrupts the power supply when the live and neutral currents are balanced	Cuts power and shuts down production equipment

These are only simple examples; in practice, protective devices can fail in many ways. Some of those failure modes will be hidden, and some will be evident. Properly designed protective systems take into account the level of protection required and the impact that spurious alarms and trips may have on normal operation. The analysis of maintenance requirements—including periodic testing—also needs to take into account both hidden and evident failure modes.

The following chapters deal with these different failure modes in more detail, including methods for evaluating the availability of protective systems and the expected rate of spurious operation. They also cover techniques for combining failure modes by "black boxing" to reduce the analysis overhead.

2.5 Making a Hidden Function Evident

Hidden failures are potentially dangerous because there is no indication that the failure has happened unless the protective device is checked or a multiple failure occurs. So designers sometimes add features that monitor the protective device and take action (usually raising an alarm) if the protective function is disabled for some reason.

For example, failure of a car's traction control or anti-lock braking system could be hidden, because under normal circumstances the system does not need to operate to prevent skidding. However, manufacturers have recognised for some time that drivers need to be aware when the system is not working, and so modern units incorporate sophisticated monitoring of the control unit and its sensors to make the driver aware of most failures.

Two further examples are shown in the table below, with a description of failure effects for the unmodified and modified protective devices.

Protective System	What happens when it fails?	Hidden?
Smoke detector connected to a simple alarm system	Nothing happens under normal circumstances. If a fire occurred in the area covered by the sensor, no alarm would sound	Yes
Smoke detector connected to a more complex alarm system	Under normal circumstances, the alarm polls the sensors every 60 seconds to ensure that they are capable of sending an alarm signal. Most sensor failures would cause a "fault" light to illuminate on the alarm panel and a signal would be sent to the remote monitoring station. If a fire occurred in the area covered by the failed sensor, no alarm would sound	No
12000 rpm overspeed alarm warning lamp	Nothing would happen under normal circumstances. If the turbine entered an overspeed condition, no alarm would be displayed and an uncontrolled shutdown would be initiated at 15000 rpm. If the alarm had worked, the operator could have taken measures to reduce turbine speed or to initiate a "soft" equipment shutdown.	Yes
12000 rpm overspeed alarm warning lamp with intelligent monitoring system	Under normal circumstances, the control system detects an open circuit lamp and displays a warning on the operators' main control screen. The operator schedules lamp replacement. If the warning lamp were non-operational and the turbine entered an overspeed condition, no alarm would be displayed and an uncontrolled shutdown would be initiated at 15000 rpm. If the alarm had worked, the operator could have taken measures to reduce turbine speed or to initiate a "soft" equipment shutdown.	No

While the designer of the protective device has made the hidden function evident, it is important to remember that the new layer of protection has introduced an additional hidden function. So in the examples above, the smoke detector monitor would need to be checked to ensure that it can identify a failed detector, and similarly we need to ensure that the function of the lamp monitor is properly maintained. Both of these are hidden functions.

2.6 Into the Grey: Hidden or not?

Before starting this section, let me say first that it is easy to classify almost all failures as hidden or evident. A very small proportion—well under one percent—cause any difficulty, and only a very few of those are genuinely ambiguous.

A very small decrease in performance or increase in operating costs

Most ambiguities arise because the effects of a failure are small and, under normal circumstances, almost unobservable.

For example, a very slow leak of water from a pipe joint would obviously result in higher utility bills. If the leak were into a drain, and the loss was automatically made up by the feed water system, would the leak be hidden or evident?

Would the leak become evident eventually? If the leak is likely to grow and become evident, perhaps because of pools of water or increasing water usage, then the failure is evident; otherwise it is genuinely hidden.

Frequent activation of a protective device

A hoist includes a protection system to stop the motion of the load if it is lifted too high. Investigation shows that the protective device is tripped on average about once per shift, or three times per day.

Given the high rate of usage, tripping the overhoist protection appears to be part of "normal operations", so the failure appears to be evident. In any case, testing the device more than once a shift would be impractical, so failure-finding does not really seem appropriate. However it is very unlikely that the designers intended the switch to be operated so frequently; they almost certainly intended it to be a rarely used protective function. Rather than meekly accepting the current state of affairs, this example suggests that design and operation of the hoist should be reviewed. Classifying the failure as hidden or evident is probably irrelevant.

Extended period between the failure and its consequences

A sunken oil storage tank develops a leak. Over time, oil percolates through the soil, but the rate of loss is not enough to alert operations staff. Remember that the analysis is zero-based, so we assume for the moment that no maintenance is being carried out; no one is going around looking for leaks. After a period of years, the oil reaches a river that is used as a local source of fresh water, and its presence is detected by analysis of samples. Is the leak hidden or evident?

A theoretical approach says that the leak is evident, because it becomes evident eventually. If you want to stir up an argument, you could say that the period between a leak starting and anyone noticing the consequences is so long that the plant could have closed down by then. So isn't the failure hidden after all?

Dealing with ambiguity

For the very few failures that are genuinely difficult to classify, it is helpful to take a step back and ask the question: "*What difference will it make if the failure is classified as hidden or evident?*"

The objective of RCM is to manage failures appropriately, and classifying them as hidden or evident is just part of that process. The ultimate goal is to put in place maintenance tasks that are effective or to identify where redesign is necessary.

The table below takes the three examples above and lists the likely maintenance task selection assuming the failure is treated either has hidden or evident.

Failure	Possible maintenance task selection if hidden	Possible maintenance task selection if evident
Slow water leak from pipe joint into drain	Visually check joint for leaks once per day	Visually check joint for leaks once per day
Overhoist protection switch fails	Change operating procedures or redesign system	Change operating procedures or redesign system
Slow oil leak from underground tank	Take soil samples from area around tank at an appropriate interval	Take soil samples from area around tank at an appropriate interval

In this case it makes no difference: the responses are the same whether the failures are classified as hidden or evident.

2.7 Key Points and Review

A hidden failure has no observable effects unless another event occurs, usually a second failure.

The only failure effects that count are those observed by the operations staff carrying out their normal duties

A failure is evident even if it is not possible to diagnose exactly which failure has occurred from its effects.

The effects of an evident failure appear eventually under normal circumstances

Typical protective devices can fail in at least two ways. Failure to provide the protective function is generally hidden, but unintended operation of the protective device is usually evident.

In a real world analysis, most failures can easily be classified as hidden or evident. Ambiguous failures are rare.

If you find a failure that is difficult to classify, focus on the maintenance outcome: does it make any difference if the failure is classified as hidden or evident?

---

[1] *Reliability-centered Maintenance*, FS Nowlan and HF Heap, Dolby Access Press, 1978

[2] Moubray, John. Reliability-Centered Maintenance. Industrial Press. New York, NY. 1997