IH Ref: IH-050-Prov

Intrusion Detection for Destruction and Contamination Activation

TECHNICAL AREA:

This disclosure relates generally to preventing or thwarting reverse engineering, and more specifically to safety measures that are configured to detect intrusion and activate destruction and/or contamination.

BACKGROUND:

If someone attempts to reverse engineer the technology, the trace left behind after activating the destruction mechanism has to be so little that it would be hard to deduce anything. This is similar to playing a game where we have the first move, therefore we are able to dictate the initial stages; anticipating what reverse engineers would do and responding with an effective way to block their methods. It is highly likely that the technology would be reverse engineered because our strategy does not change, however, we hope to generate enough obstacles that we would already be a dominant force in the market.

EXISTING TECHNOLOGIES:

The technologies involved are related to intrusion detection, destruction, and contamination. These technologies would be installed into the device. There is a lot of existing technologies that can be used to prevent reverse engineering. Most of the technologies will be used to protect the cold fusion technology. The technologies discussed are most likely the ones that will be used.

Intrusion detection technologies include Performance Monitoring and Fault Location (PMFL), sensors, and encryption codes. With PMFL, the device can be monitored remotely. Sensors will help detect an intrusion. Some sensors that can be used are light and proximity. The encryption method will be some form of a code that needs to be entered in.

As for the destruction of the reactor, thermite is a possibility. Thermite would be made by mixing iron oxide with aluminum powder, followed by the addition of sulfur to make the ignition process easier.

As for contamination, the contaminants would need to be properly contained. The contaminants can be placed inside separate chambers, refer to *Figure 3* for example, and released when it detects an intrusion. Some strategies include the use of dummy variables to confuse reverse engineers, destruction by mixing certain chemicals, or introducing contaminants.

PROBLEMS WITH EXISTING TECHNOLOGIES:

There are ways to stop these technologies from working, especially when only one piece of technology is used. This section will discuss the ways to bypass independent technologies.

The problem of PMFL is if the communications gets blocked, then the device would not be able to send or receive the destruction command. For the light sensor, they could either remove the light sensor in the dark before turning on the light or work outside the detection range of the light sensor. For the proximity sensor it would be hard to implement because the device would be in the product. There will be many objects inside the product that can cause the proximity sensor to malfunction. These sensors might not work well after a long time under hot conditions and not charged, however, we can assume that reverse engineers would open the device before the sensors stop working.

The problem of encryption is that maintenance people would have to know the key to fix the devices, which can be stolen. For example, the maintenance person might help get the code for the reverse engineer. Another problem is that the cost of attaining this technology could be very expensive.

For the destruction of the reactor, it would require some sort of spark and ultimately, it would be difficult justifying using thermite, especially when it is remotely controlled.

For the contamination of the reactor, there are many possible contaminants that could be placed in separate chambers, refer to *Figure 3*. However, the contaminants cannot leak into the reactor until the valves leading to the reactor are opened. This would require proper storage and a good seal at various pressures. Preparing these contaminants would take some time as well because each chamber would need to be filled separately during assembly. With more valves, it gives rise to potential leaks within the reactor. Finally, if

the contaminant are liquid or solid form, it might not mix well inside the reactor and there could be remnants of it in the chamber, allowing reverse engineers to find out what contaminant it was.

SUMMARY OF THE PROPOSED SOLUTION AND THE ADVANTAGES THE PROPOSED SOLUTION PROVIDES:

In this document, product refers to the commercial good, device refers to the intrusion detection method, and reactor refers to where exothermic reactions occur. See *Figure 1*. In order to prevent reverse engineering, we have to consider the ways one can reverse engineer, then attempt to eliminate as many possibilities as possible with the most cost effective solution. This method concerns the initial intrusion of opening the device, which would trigger a destruction or contamination of the reactor so that no useful information can be obtained. Even though safety could be an issue upon destruction of the system, the risks only exists when the device is opened.

There are various ways and use of technology to prevent reverse engineering. The technologies discussed here uses certain technologies, in particular, the possible combination of the technologies listed. Since every technology equipment used to prevent reverse engineering has a way to be countered, the combination of technologies will make reverse engineering much more difficult. It is important to remember that even though the purpose of these technologies is to prevent reverse engineering, cold fusion is revolutionary and given enough time, someone else will figure out cold fusion. These preventive measures will prolong the time taken for reverse engineers.

The steps to prevent reverse engineering are intrusion detection, followed by destruction and or contamination. For intrusion detection, the solutions are PMFL, sensors, and encryption. The destruction and contamination are a mixture of chemicals. These proposed solutions will be in the device. See Figure 1.

With PMFL, a specific list of criteria would have to be fulfilled to prevent the triggering the reactor's destruction. This method requires a remote activation for the destruction of the reactor, so it will require communication to and from the product. PMFL gives the opportunity to daily monitor the product to ensure nothing wrong happens. The easiest sensors to use are light and or proximity sensors. The activation for

the light sensor would be light, which would be triggered if the device is exposed to light. Likewise, the proximity sensor would activate when it notices something being detached from the system, leading to the destruction of the reactor.

The encryption key would take a while to figure out since there are many ways to create an encryption key. This would be a big hurdle for reverse engineers because they would need to know the key to decipher the code. If they input the wrong code a certain number of times in a row then the device would automatically self-destruct.

The destruction solutions are cheap and easy to implement. Most importantly, it will destroy the reactor, resulting in no useful information remaining. With the intrusion detection system, it will be hard to even look inside the device without destroying it.

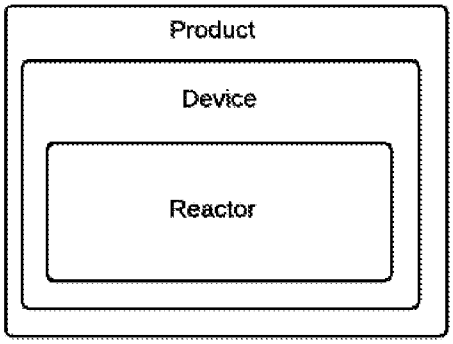
For the contamination option, there are many possible contaminants we could choose to confuse the reverse engineers. The contaminants can react with each other also to cause different kinds of results. Choosing contaminants carefully can result in a lot of permutations in what the starting material could be. In addition, reverse engineers also need to know the starting conditions to start the reaction. This could buy us a lot of time to dominate the market.

For the destruction and contamination, we could combine both methods since their operation are independent of each other and provides more protection for the LENR technology.

DETAILED DESCRIPTIONS OF THE PROPOSED SOLUTION AND FIGURES:

The exothermic reaction will occur inside the reactor. The proposed solutions will be located in the device area, which will be connected to the reactor. Finally, the product is the outer shell and encapsulates both the device and reactor, referring to Figure 1.

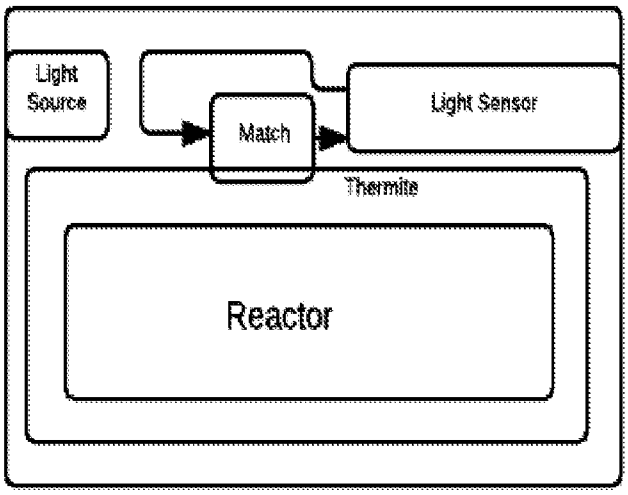
Figure 1: Product



For PMFL, some of the criteria would be is the device on, is the device and reactor at its home base, is the device within a predetermined physical range of other devices, is the device working properly, is the walls of the device being penetrated, and so on. The signal will be sent every *x* amounts of time and triggered for destruction upon failure to communicate *y* times or not fulfilling majority of the criteria. The third criterion listed refers to a device's distance to another device. Since the device is in the product, devices should have a minimum distance between them. So if that distance is breached, we can assume that the devices are out of the product shell, ready to be opened. There are many conditions to check, the ones listed are a few examples.

For the light sensor, it would be near the top of the device as shown in *Figure 2*. The light sensor would detect visible light since people work under these conditions. This will be the one way of activating the destruction of the reactor. The PMFL can be connected to the light bulb to trigger the light sensor or some other way to create a spark. The diagram only shows one light sensor, however, we can put more to ensure that there would be a spark created. This option will not require a power source since it is activated by light.

Figure 2: Light Sensor



The proximity sensor will detect if anything is disconnected. It will be connected to the important parts of the product such as the device, reactor, and other things that are considered valuable. Therefore, if one of these parts are removed, it would emit a signal to destroy the reactor. The proximity sensors' data will be relative to each respective part of the product to minimize the reading error. However, if the device is being removed from the reactor, it will automatically trigger the destruction. This could also be used for the device that is close to another device mentioned in PMFL.

The encryption key could be similar to the banking system where a code is generated and an appropriate response is required within a certain period of time. There are two ways to implement this. The first method is for the code to be generated remotely and there would be a choice to relay the code to the person opening the device (maintenance worker). A method to ensure safety would be that even though the code is randomly generated, there cannot be similar codes generated at the same time. So one device's code will never be the same as another. Another possibility is that our people will know the key, so they can decode it either by their knowledge or by a device that can help them do that. The first option is better since less people will know the key of how to decode it. If the input code is incorrect for x number of times, it would activate the destruction of the reactor.

For the destruction of the reactor, thermite would be placed around the outer walls of the reactor. The ignition could be a match connected to a power source that turns on.

When a trigger is sent to destroy the reactor, the power source turns on, creating a spark on the match, which in turn will ignite the thermite. There are many ways to ignite the thermite and the match is just one possibility.

For contaminating the reactor, the contaminants would be stored in separate chambers as shown in *Figure 3*. The number of contaminants shown in the figure can be varied. The valves would be opened when potential breach of the device is detected. If reverse engineers try to remove the contaminants first, the device would have a mechanism to detect what is happening, which would lead to the release of the other contaminants into the reactor. An example of contaminants would be glycerol and potassium permanganate in another chamber. These contaminants can combine to react with each other, creating a large flame, destroying everything inside the reactor. Other potential contaminants are corrosive chemicals and oxidants. The amount of the contaminants used can be calculated by using mole calculations. It is important that the contaminants has to be in excess compared to the reactant to ensure that the ingredients in the original reactant gets destroyed. The corrosive chemicals can destroy surfaces of the cold fusion reactant due to its nature. Oxidants would oxidize the reactants, which would stop the reactor if electrochemical reactions are involved. Examples of corrosive chemicals are strong acids and bases, aqua regia, hydrochloric acid, sodium hydroxide, etc. Examples of oxidants are potassium permanganate, oxygen, etc. Exposure to open air or dirt can also be considered as contaminants and could render the reactor useless. There are many more possibilities for choosing contaminants, the ones listed above are just a few. It is essential that the contaminants are stored properly and react quickly so that the important parts in the cold fusion reaction will be destroyed. All the stored contaminants can be released into the reactor so that it would be harder to determine the cold fusion reaction.

Another method to confuse reverse engineers would be the use of dummy variables. The dummy variables can either do nothing, or be part of the original reactants. The dummy variables that do not do anything can be placed together in one of the contaminant chambers, it will give the reverse engineers more things to think about. The dummy variable that is one of the original reactants that starts the exothermic reaction will disguise the real amount of material needed. The dummy variables are stalling techniques.

Figure 3: Contamination Design