

HYDROCARBON ENGINEERING

July 2014

The number one
global leader in
hydroprocessing
catalysts and the
complete range
of catalysts


artcatalysts.com

ART
Advanced Refining Technologies

The page features a decorative, ornate frame in a golden-brown color, resembling a laurel wreath, which encircles the main title. Below the frame, at the bottom of the page, is a dark silhouette of a castle with multiple towers and battlements. A red flag is visible on the left side of the castle. The background is a textured, aged parchment-like surface.

SECURED AGAINST **SABOTAGE**

Ton Beems and Mark Hellinghuizer,
Yokogawa Europe, The Netherlands,
discuss refinery safety systems and
network security.



During system realisation, all involved parties do their utmost best to deliver a correctly functioning and properly documented safety system. This means the use of well proven state of the art latest technology, all safety integrated functions (SIFs) calculated and validated, and all loops checked. But is the overall validation (step 13 of the IEC61508 lifecycle) carried out in sufficient detail? What happens after two or three years? Are the safety integrity levels (SIL) of the plant still OK?

What if one looks at network security aspects; can they represent a threat to a carefully engineered safety system and render it unsafe?

This article will show how apparently carefully considered safety procedures can be undermined, leaving process plants vulnerable to attack in a number of ways. By presenting the situation from the viewpoints of a plant owner and a hypothetical hacker, the authors show how safety and security can no longer be considered as separate issues.

For any process plant during the operational phase of the safety lifecycle, there are multiple things that need to be done to maintain the safety integrity levels of the installation. A plant owner may be under the impression that all is taken care of and the correct procedures have been carried out to keep the plant compliant with the IEC standards. A 'hacker', however, sees opportunities to create dangerous process situations by using any gap they can find in the plant's network security.



Figure 1. The five key elements generally regarded as necessary for full IEC61508/IEC61511 compliance in a process plant.

If one considers the safety lifecycle according to the second edition of IEC61508, then one can say that until step 12 (overall safety validation) all is done to deliver a project that operates in the best possible way. The SIFs are designed; every SIF will get a safety integrity level (SIL); and during engineering it must be proved that the hardware is compliant in terms of the average probability of a failure on demand (PFDavg) and tolerance of hardware faults (HFT). In addition, the engineering should be performed in such a manner that the systematic safety integrity is also compliant with the required SIL.

For this last item, companies typically have functional safety management systems that cover areas such as competence, procedures, templates, testing and reviewing. Engineering is reviewed; what is built is internally tested and corrected where required; and then the end user does a factory acceptance test, corrections are carried out, and the customer signs a certificate for acceptance.

It might now be considered that after site acceptance and commissioning the best possible situation has been attained. The safety system is 100% documented and ready for operation. All procedures and documentation are in place and 'as built'. After overall site validation, the end user may start production.

However, functional safety, as specified in the IEC61508 and IEC61511 standards, only considers dangerous situations from the viewpoint of the process itself: i.e. when the process runs out of control. What it does not consider are deliberate attacks such as sabotage, hacking and terrorism!

During the operational phase, it is more difficult to maintain full compliance with the standards because of factors such as production pressure, forecasts and penalty clauses in contracts, so that sometimes safety is compromised to keep production promises. People that have to make changes in the safety system also suffer from these pressures, and tend to be prone to human error. Production takes priority: a failure during implementation of an online change can result in a shutdown, resulting in more stress. Paperwork may be prepared, but sometimes a prepared change has to be modified on the spot, and the paper updates can then be forgotten.

Figure 1 is a diagram in which the five key elements that are generally regarded as necessary for full IEC61508/IEC61511 compliance are represented as coloured segments of a 3D 'ball' diagram. Only if all five pieces of the diagram are in place will the ball roll smoothly and full compliance be achieved during the operational phase. These five elements are:

- Competence: Everybody involved in the safety lifecycle must be proven competent.
- Auditable trail: The auditable trail must be obvious.

- Modifications: To be carried out with impact analysis and must be well documented and tested.
- Maintenance: To be done properly, in time and well documented and (if applicable) tested.
- Proof testing: To be implemented within the agreed proof test interval (PTI), and to be well documented. Proof test results must be analysed and compared with previous proof tests.

Competence in the standards

With the second edition of IEC61508, the competence of all involved in the safety lifecycle of a project has changed from informative to normative, and must be clearly specified (by the management), written down in procedures, documented, proven and monitored. Company managements should be aware of the potential dangers in their process environment as a social responsibility, and internal safety training, for personnel at all levels from engineering to site service, must be carried out with the long term in mind. At Yokogawa, for example, all safety training has a validity of three years, and now has to be completed with an assessment to prove that the engineer really has understood what they are being told.

Now let us look at the situation of competence in the standards from the hacker's point of view. In particular, one must consider 'social engineering', which can be defined as the art of interposing oneself as a different person in order to obtain information. To do this, no technical skills are needed: the skills required are more on a communication level.

Reconnaissance: The first step in any hack is reconnaissance; i.e. the hacker tries to get information to find out what the best way to attack is.

In social engineering, the hacker tries to find the names and functions of key people in order to find the best way to enter the plant. Google is a very helpful tool in this: it will provide much information in this first step. Using Google, the hacker can, for example, first look for members of the fire fighting department, and can then find more information about these people using social media.

For the purposes of this article, assume that the hacker has found Mr. Smith, who is the head of the fire fighting department. In order to enter the plant, the hacker will need to look like a fire fighter. Using internet retail sites, the hacker can procure real fire fighting gear. He also needs an ID to prove himself as a fire fighter; on the internet he can find many examples of companies who will make these IDs.

For the final step, the hacker travels to the plant wearing the fire fighting gear, shows the fake ID and says that he is here to do an unscheduled fire inspection. He will show a faked signed letter from Mr. Smith proving that he is allowed to do this and will ask somebody to show him around the plant.



Figure 2. Five additional elements need to be added to the diagram shown in Figure 1 to create a complete security model.

The hacker will then wait for a brief moment when he is unaccompanied, and will insert a USB stick into a computer that will install a 'back door' which will grant remote access to the plant.

So there goes the diagram part for competency.

Auditable trail

Typically, a company's quality and FSM system forces companies to provide an auditable trail from the start of the project to the end, ensuring that all engineering reviews, internal testing, acceptance testing and site testing evidence is kept, along with maintenance and proof test records. But what really happens after handover to site? Will the maintenance of the trail get forgotten?

Who can follow the auditable trail of the plant's safety system? Can a technician who is known to work on, for example, the ESD system show his manager the SIL classification of the system, the HAZOP report, maybe the SIL calculations?

In the control room, the operators might be looking at the process. It is very likely that they know which parts on the screen are connected to the safety system. But do they know the safety functions?

In this context, hackers define a hack in five steps to achieve their aim:

- Reconnaissance: Gather information about the system.
- Scanning: Scan the system for vulnerabilities.
- Gaining access: If a vulnerability is found, exploit it and get access to the system.
- Maintaining access: If the hacker is inside, he might be detected and disconnected, so now he has to take measures to maintain access.
- Covering tracks: After the hack, the hacker deletes every log and every trace so that nobody ever knows the system has been hacked.

Now the diagram part for the auditable trail has been lost.

Maintenance

In the process industries, there are two types of maintenance: scheduled maintenance and corrective maintenance.

Scheduled maintenance is maintenance that has to be done on a regular basis; otherwise known problems arise that prevent certain safety functions from working. This kind of maintenance can be regarded as preventive, and can be scheduled in such a way that production can be maintained. For this to happen, the installation has to be equipped with extra devices to make sure that the work can be carried out safely. The sections that require maintenance must be completely isolated from the process, emptied, purged and so on. For scheduled maintenance the paperwork can be

prepared in advance; risk analysis can be done; procedures can be prepared; work orders and instructions can be prepared; and permits to work can be requested. With scheduled maintenance there is time to properly prepare the work.

Corrective maintenance is maintenance that is carried out on an interrupt basis. Diagnostics or tests show that something is not working properly anymore, and replacement/repair/maintenance is needed to correct this. Unlike scheduled maintenance, there is pressure from the operations and production departments to correct the situation. Procedures and permits are written with more time pressure: hence there is a greater chance of overlooking things and introducing human error. The work itself is also needed more urgently.

What is important is that, as previously mentioned, the people are competent, an auditable trail is kept, and an impact analysis is carried out.

The hacker's response to the maintenance scenario is, assuming that the plant security is not OK, to remotely attack the plant and gain control over the DCS. By using, for example, remote desktop protocol (RDP), a standard Microsoft tool, the hacker can gain full control of the keyboard, mouse and monitor from anywhere on the planet, and can activate a maintenance override switch (MOS) from the safety system. He will, of course, need a master MOS key before he can do this, but in many cases this key is already enabled. Once the MOS is set, the hacker can trigger an action on the DCS that may result in an unsafe situation.

And yet another part of the diagram is gone . . .

Trips and failures

Plants will inevitably encounter trips, false trips or occasional system failures, but what is the procedure when they happen? Are they all registered, or does the user register even more? Are trips and failures studied properly? It may be, for example, that a certain safety loop trips more than expected during hazardous operation; in other words, the demand rate is higher than expected.

Proof testing

Proof testing is something that every user knows they have to do, probably during a planned shutdown. But does it need to happen every year, and can anyone prove it? Can the plant really be tested pipe to pipe; what needs to be simulated; does the user write down what is simulated?

So managers really sometimes need to act as the devil's advocate; people may not like what is asked for in the first place, but everyone has a responsibility. This responsibility should be emphasised by the management.

Now consider the hacker response to the proof testing scenario. Assume again that the security is not OK, so that the

hacker can again remotely access the plant. Proof testing information can be deleted or, even worse, fake proof test evidence can be generated which may result in an unsafe situation.

Whichever is the case, another diagram part bites the dust.

Modifications

If a modification needs to be done on a plant that is in the operational phase of the safety lifecycle, the following needs to be considered:

- Where does the request from the modification come from: operations, process, maintenance?
- Is the modification approved by the appropriate level/department in the organisation, and who did it?
- Has an impact analysis of the modification been done? Who did it, what was considered, and where is it documented?
- Is site testing done; who did it; is it documented? Was it possible to perform a complete (pipe to pipe) test of the changed safety function?
- Is there evidence of the full trail above, including an auditable trail?

Now consider the hacker response to modifications. Again, assuming that the network security on the plant is suspect, the hacker gets into the asset management system.

Most plants have an asset management system to monitor the status of transmitters and make changes by using a communications protocol such as HART.

The hacker again installs a key logger under Microsoft. He then waits for a privileged engineer to log in. The asset management password is acquired, providing full access to the hacker, who then searches for a pressure transmitter that is connected to the safety system.

A pressure transmitter is located whose current range is 0 - 10 bar. The pressure transmitter will convert this to 4 - 20 mA, and the safety system will convert this internally back to 0 - 10 bar.

Now assume that this transmitter is on a vessel that will explode at 15 bar, with a high pressure trip at 9 bar (14.4 mA), even though the safety system will accept any value in the 4 - 20 mA range.

The hacker now remotely changes the pressure range of the transmitter to 0 - 30 bar. Usually, safety transmitters have a write protection switch, but they are often not activated because of the inconvenience caused.

The hacker can now switch the DCS controller to manual operation, and set the controller to maximum burner power. The pressure will rise in the furnace vessel, but the high pressure trip level at 14.4 mA will now never be reached. With the new range (0 - 30 bar), the furnace will explode at 12 mA.

So, when the security protection is not in place, the hacker has totally fooled the good working safety system. The last part of the compliance diagram has gone.

Building solid security

So, despite all the effort put into the safety system as it comes to compliance with the IEC61508 and IEC61511

standards, the original five criteria from our diagram have proved insufficient.

In fact, in order to create an appropriate security model, the diagram needs to be augmented with five extra pieces to create 10 in all (Figure 2). The new elements are:

- Physical security.
- Network security.
- Host based security.
- Disaster recovery.
- Lifecycle maintenance.

The Yokogawa security model is based on the ISA 99 standard, which covers these areas as follows:

- Physical security: The first layer of protection is to physically protect access to the PC and the network equipment. This will involve doors with locks, locked cabinets, keycards etc., but also plant access, proper security guards, and procedures for authorising access.
- Network security: The second layer is the network protection. There should be a properly configured and well maintained firewall between the process control network and the office network. All unused ports on network equipment should be disabled, and use should be made of VLANs and access control lists.
- Host based security: Host based security is a key part of security on the actual PCs and servers in the system. Every PC should have a virus scanner and all the latest Microsoft security patches provided via the Windows security update server (WSUS). PCs should all be hardened, and all unused programs and unused services should be disabled. Users should pay special attention to USB ports and other disk drives.
- Good user management should be in place.

Disaster recovery

100% security does not exist. That is why good backup management is of vital importance. In an emergency, the user should be able to restore the system to a fully working condition.

Security lifecycle maintenance

Security without maintenance gives a false sense of security.

It is of vital importance to maintain security. Users can either adopt a 'do it yourself' approach, or ask their DCS vendor for a security maintenance contract.

Conclusion

Any plant operator that imagines that their safety system is foolproof needs to consider their security as much as their safety. The diagram needs to be shared into ten pieces instead of five.

The world can only turn if one has all pieces of the diagram in place. Any missing piece will make the world both vulnerable and unable to rotate.

If the reader is a plant owner, manufacturer, SIS integrator or supplier of any equipment included in any safety instrumented function one needs to consider all elements of the diagram.

If the reader is an inspector, look outside the boundaries: disaster can come from an unexpected angle. 