**Safety-Critical Systems: Open Assessment 2018-19**

**Supporting Competent Authorities in the Implementation**

**of the NIS Directive for Safety-Critical Industries (Level M)**

**student name: xiangrui xu**

**metric number:2367947x**

**email:** [**2367947x@student.gla.ac.uk**](mailto:2367947x@student.gla.ac.uk)

Index

[Introduction 3](#_Toc1987166)

[Method 3](#_Toc1987167)

[Fault tree 3](#_Toc1987168)

[Criticality analysis 5](#_Toc1987169)

[Case analysis 7](#_Toc1987170)

[Evaluation 9](#_Toc1987171)

[Conclusion 10](#_Toc1987172)

[Appendices 10](#_Toc1987173)

# Introduction

According to the document of NIS directive, the Network and Information Systems Directive has been integrated into UK law. Therefore, the Operators of Essential Services (OES) are expected to be guided and assessed by Competent Authorities (CAs). For example, the Civil Aviation Authority will support airlines operating UK flights acting as the Competent Authority. In UK energy distribution, the Competent Authority is the Health and Safety Executive (HSE).

The aim of the directive is to increase the resilience of critical infrastructures and, in particular, improve the robustness of systems that rely on the exchange of digital information. In most cases, the loss of these infrastructures can have an impact on safety-related applications. This has resulted in many CAs being drawn from the regulatory agencies that protected the safety of complex systems and they have had to extend their competence to consider the cyber security of critical infrastructures.

In order to address this problem, we utilize an approach of the combination of fault tree and criticality analysis to assist CAs. The method section would explain the details of the method and a case would be analyzed by the method in following section. In the end. The conclusion would be discussed.

# Method

## Fault tree

Fault tree is a top-down failure analysis in which an undesired state of a system is analyzed using Boolean logic to combine a series of lower-level events. Fault tree can be used in multiple situations. For example, it can be applied to monitor and control the safety performance of the complex system or function as a diagnostic tool to identify and correct causes of the top event.

Fault tree method contains some basic symbols including events, gates and transfer symbols. The event symbols are used for primary events and intermediate events. The figure 1 shows the details of events symbols as following.

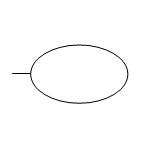
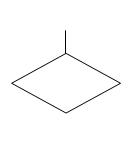
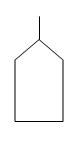
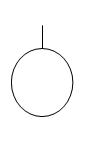


Figure 1. basic, external, undeveloped events and conditional events

The basic events are the failure or error in the system and the external events are normally expected to happen while itself is not an error. The undeveloped events are usually the events about which insufficient information is available.

Fault tree method also includes gate symbols to describe the relationship between input and output events. The figure 2 shows the details of events symbols as following.

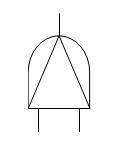
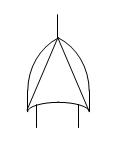
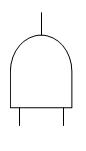
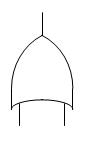


Figure 2: OR gate, AND gate, Exclusive OR gate and Priority OR gate

The OR gate would perform output when any input occurs. The AND gate would perform output when all inputs occur. The Exclusive OR gate would perform the output when exactly one input happens. The priority AND gate would perform output when the input happens in specific sequence by a conditional event.

The basic mathematical foundation of fault tree is associated with statistical probabilities and failure probabilities depends on the constant failure rate λ and the exposure time t. The equations of fault tree are shown below.

A fault tree is often normalized to a given time interval, such as a flight hour or an average mission time. Event probabilities depend on the relationship of the event hazard function to this interval.

The fault tree method involves five steps:

1. define the undesired event to study.
2. Obtain an understanding of the system.
3. Construct the fault tree
4. Evaluate the fault tree
5. Control the hazards identified

## Criticality analysis

The method contains 8 steps to analyze the failure mode and rate:

1. Functional Block Diagram. Establish scope of the analysis and break system into subcomponents.
2. Identify Failure Modes
3. Assess Criticality

|  |  |  |
| --- | --- | --- |
| 10 | Hazardous without warning | Very high severity ranking when a potential failure mode affects safe operation or  involves non-compliance with a government regulation without warning. |
| 9 | Hazardous with warning | Failure affects safe product operation or involves noncompliance with government  regulation with warning. |
| 8 | Very High | Product is inoperable with loss of primary Function. |
| 7 | High: | Product is operable, but at reduced level of performance |
| 6 | Moderate | Product is operable, but comfort or convenience item(s) are inoperable. |
| 5 | Low | Product is operable, but comfort or convenience item(s) operate at a reduced level of performance. |
| 4 | Very Low | Fit & finish or squeak & rattle item does not conform. Most customers notice defect. |
| 3 | Minor | Fit & finish or squeak & rattle item does not conform. Average customers notice defect. |
| 2 | Very Minor | Fit & finish or squeak & rattle item does not conform. Discriminating customers notice defect. |
| 1 | None | No effect |

1. Repeat for potential consequences
2. Identify Cause and Occurrences Rates, risk = frequency x cost
3. Determine detection factors.
4. Calculate Risk Priority Numbers:

RPN = S x O x D, where:

– S - severity index;

– O - occurence index;

– D - detection index.

1. Finalise Hazard Analysis.

# Case analysis

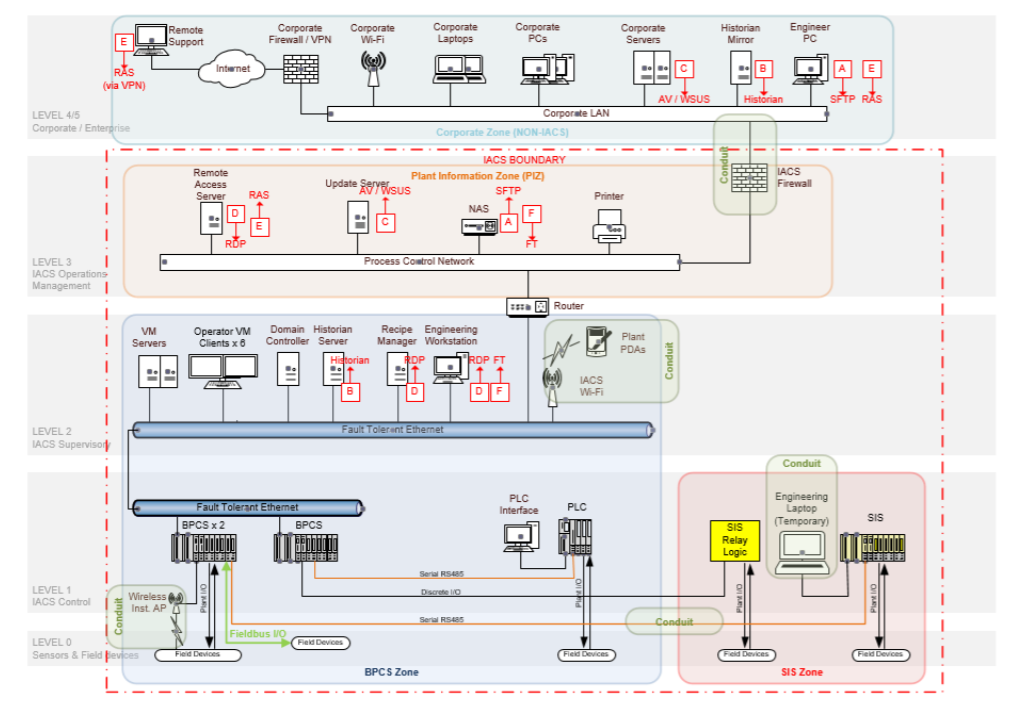


Figure 3 Medium sized Site

The figure 3 shows the medium sized site of SIS zone, a BPCS zone and a plant information zone. As shown in the figure, the devices are in the scope of IACS system, which means it may need some countermeasures. In addition, the BPCS zone is connected to SiS zone by a conduit to provide data. While the engineering laptop is an external conduit when it is used to transfer data.

There is a router between plant information zone and BPCS zone and this would allow the necessary connections between the BPCS and plant information zone. A firewall could also be considered for this duty depending upon the necessary data access etc. Network Access Controls are in place to permit file transfer via the NAS between the corporate zone and the BPCS and to gather anti-virus operating system updates via the Update server.

The engineering laptop can be provided a short-time connection in the SIS zone scope. The laptop and connection need to prevent unauthorized access.

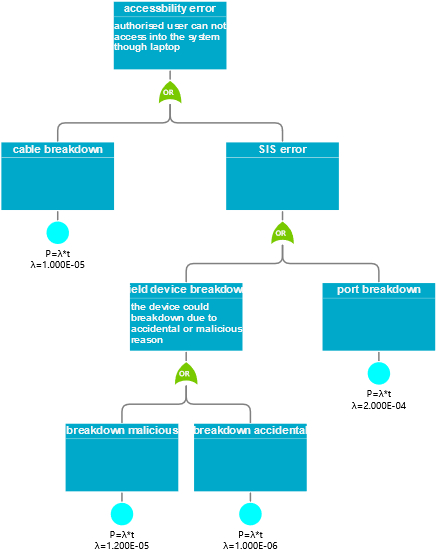


Figure 4 inaccessibility fault tree

To analyze the SIS zone, fault tree method is used to analyze the potential failure in SiS zone. As the figure 4 shows, the SiS zone could meet the failure of inaccessibility issue. This issue could be triggered by multiple faults. The fault could emerge in cable breakdown, which could cut out the connection between login authentication and account database. In addition, the SiS system also could occur some errors, such as the interface breakdown and field devices like sensors breakdown. The leaf events carry the possibility of unwanted events happening. Each event would contribute to the root event(the failure) based on probability theory. Therefore, we could calculate the possibility of the unwanted event by the fault tree method.

To assess the criticality of the system, the possibility of the failure event would be applied to determine the occurrence degree of the event. Even though the possibility of event could be high but sometimes the severity of each event could be low. In that way, the system could set a low priority of that failure, which could be more reasonable for the system. In order to assess the priority of each event, the risk priority number is introduced to this scheme. The occurrence, detection and severity are contributed to the risk priority number based on the equation of RPN.

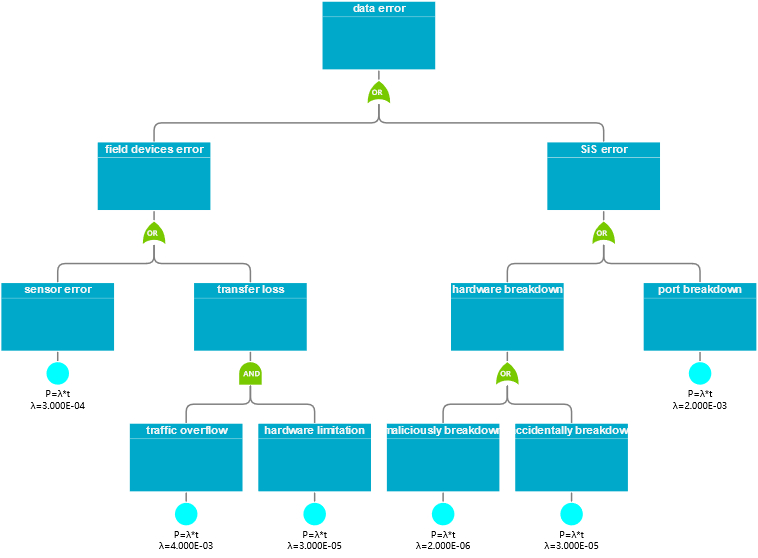


Figure 5 data error fault tree

As the figure 5 shows, the SiS zone could meet the failure of data showing. This issue also could be triggered by multiple faults. The fault could emerge in field devices error which could originate from the sensor failure or data transfer loss. The transfer loss could be triggered by traffic overflow or limited infrastructure. In addition, the SiS system also could occur some errors, such as the interface breakdown.

The potential failure mode and effect analysis table is shown in appendices.

# Evaluation

Thanks to Junpeng Lu for evaluating the method. The feedback of evaluation of the method is stated as follows: the overall method framework is reasonable and it can sense the potential faults in candidate system. In addition, the countermeasures could be applied to prevent the potential risk by calculating possibility. However, there might be some ambiguity on how to construct the fault and the feasibility of speculating the potential risk and fault mode.

# Conclusion

By applying the fault tree and failure mode & criticality anaylsis method, the competent authority could roughly infer the potential failure mode though fault tree. In addition, the priority and occurrence of system’s potential error could be roughly calculated, so some countermeasures could be done to prevent or lower the risk of failure.

# Appendices