

Terminology

Reliability

Probability that a piece of equipment/component will perform its intended function satisfactorily for a prescribed time, under stipulated environmental conditions

Safety and Security

Safety is freedom from accidents and losses



Conclusion

Although a lot of work has been done in the field of safety and security, there is still a need for a more comprehensive approach to safety and security. This is especially true in the field of risk management, where the focus is on the identification and assessment of risks, and the development of strategies to manage them.

Failure

Occurs at failure
- Early
- Random



Risk

Hazard level combined with likelihood of an accident and exposure

Accidents, Incidents and Hazards



Terminology

Reliability

Probability that a piece of equipment/component will perform its intended function satisfactorily for a prescribed time, under stipulated environmental conditions

Safety and Security

Safety is freedom from accidents and losses



Conclusion

Although a lot of work has been done in the field of safety and security, there is still a need for a more comprehensive approach to safety and security. This is especially true in the context of the Internet of Things (IoT), where the number of devices and the amount of data are growing rapidly.

Failure

Occurs at failure
- Error
- Breakdown



Risk

Hazard level combined with likelihood of an accident and exposure

Accidents, Incidents and Hazards



Reliability

Probability that a piece of equipment/component will perform its intended function satisfactorily for a prescribed time, under stipulated environmental conditions

Failure

Opposite of Reliability

- Early
- Random

Systemic

- Design flaws
- Does not satisfy goal

Non-systemic

- Deviation from design
- Caused by environmental or structural changes

Error

- A design flaw or deviation from the intended state
- Failure is an instant; error is present until it is fixed
- Failure is an event; error is a state

Faults

- A high order event
- Primary
- Secondary
- Command

Systemic

- Design flaws
- Does not satisfy goal

- Dev
- Cau
- stru

Non-systemic

- Deviation from design
- Caused by environmental or structural changes

Error

- A design flaw or deviation from the intended state
- Failure is an instant; error is present until it is fixed
- Failure is an event; error is a state

Faults

- A high order event
- Primary
- Secondary
- Command

Accidents, Incidents and Hazards

Hazard

A state or set of conditions that will lead to an accident when combined with other environmental conditions

- Defined with respect to the system's environment
- Depends on where the boundaries are drawn
- Likelihood is evaluated qualitatively or quantitatively
- Level determined by severity and likelihood

Accident

An accident is an undesired and unplanned event that results in a specified level of loss

Incident

Undesired event which has little or no loss

Accident

An accident is an undesired and unplanned event that results in a specified level of loss

Incident

Undesired event which has little or no loss

Hazard

A state or set of conditions that will lead to an accident when combined with other environmental conditions

- Defined with respect to the system's environment
- Depends on where the boundaries are drawn
- Likelihood is evaluated qualitatively or quantitatively
- Level determined by severity and likelihood

Risk

Hazard level combined with likelihood of an accident and exposure

Safety and Security

Safety is freedom from accidents and losses

Differences

- Intent
- Emphasis

Similarities

- Threats or risks
- Protection against losses
- Important
- Regulated

Differences

- Intent
- Empahsis

Similarities

- Threats or risks
- Protection against losses
- Important
- Regulated

Terminology

Reliability

Probability that a piece of equipment/component will perform its intended function satisfactorily for a prescribed time, under stipulated environmental conditions

Safety and Security

Safety is freedom from accidents and losses



Conclusion

Although a lot of work has been done in the field of safety and security, there is still a need for a more comprehensive approach to safety and security. This is especially true in the case of complex systems where the failure of one component can lead to the failure of the entire system.

Failure

Occurs at failure
- Error
- Breakdown



Risk

Hazard level combined with likelihood of an accident and exposure

Accidents, Incidents and Hazards



Conclusion

Although a bit tedious terminology is necessary for good communication within the engineering field. As such it is important that students understand and effectively use correct terminology to enable progress towards solutions.

Reference

Leveson Chapter 9

Reference

Leveson Chapter 9