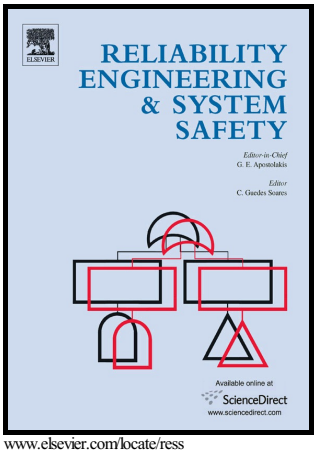
How to interpret safety critical failures in risk and reliability assessments

Jon Tømmerås Selvik, Jean-Pierre Signoret



www.elsevier.com/locate/ress

PII: S0951-8320(16)30524-5
DOI: http://dx.doi.org/10.1016/j.ress.2017.01.003
Reference: RESS5725

To appear in: *Reliability Engineering and System Safety*

Received date: 20 September 2016
Revised date: 23 November 2016
Accepted date: 4 January 2017

Cite this article as: Jon Tømmerås Selvik and Jean-Pierre Signoret, How t interpret safety critical failures in risk and reliability assessments, *Reliabilit Engineering and System Safety,* http://dx.doi.org/10.1016/j.ress.2017.01.003

How to interpret safety critical failures in risk and reliability assessments

Jon Tømmerås Selvik[a], Jean-Pierre Signoret[b]

[a]University of Stavanger and IRIS

[b]Reliability expert, ISO/TR 12489 project leader

Abstract

Management of safety systems often receives high attention due to the potential for industrial accidents. In risk and reliability literature concerning such systems, and particularly concerning safety-instrumented systems, one frequently comes across the term 'safety critical failure'. It is a term associated with the term 'critical failure', and it is often deduced that a safety critical failure refers to a failure occurring in a safety critical system. Although this is correct in some situations, it is not matching with for example the mathematical definition given in ISO/TR 12489:2013 on reliability modeling, where a clear distinction is made between 'safe failures' and 'dangerous failures'. In this article, we show that different interpretations of the term 'safety critical failure' exist, and there is room for misinterpretations and misunderstandings regarding risk and reliability assessments where failure information linked to safety systems are used, and which could influence decision-making. The article gives some examples from the oil and gas industry, showing different possible interpretations of the term. In particular we discuss the link between criticality and failure. The article points in general to the importance of adequate risk communication when using the term, and gives some clarification on interpretation in risk and reliability assessments.

1. Introduction

Industrial failure events occurring in safety systems could, depending on the system, lead to severe consequences. However, in many situations we find the terminology referring to such events to be rather vague. For example, the term 'safety critical failure' could have different meanings. It depend on what 'critical' refers to. It could refer to an undetected unsafe state with possibility for severe consequences, or simply express that a part of the safety system has lost its functionality, i.e. the failure in itself is categorized as critical (cf. ISO 14224:2016). There are also other interpretations.

In this article we will focus on what is the meaning of the term 'safety critical failure' as a subset of the failures occurring in 'safety critical systems'. Currently, in literature and practice within the risk and reliability area, both of these two terms are open for interpretation. And there is a need for clarification.

Nevertheless, there is a common understanding that failures occurring in 'safety critical systems' may have safety concerns, including possible harm to humans or the environment. It thus intuitively makes sense to label the failures that could cause severe consequences as 'safety critical'. Many publications establish such a link, although with different levels of specificity. For example, Isaksen et al. (1996) associate the term with failure events that can contribute to accidents. The definition could be further extended by including system states that produce the possibility for accidents (i.e. dangerous failures). Consider a redundant system with two components A and B; for example, two emergency shutdown valves. If a failure occurs on Components A, then the impact could be very different according to the state of component B. The state of Component B could matter for whether or not the system is conditioned for severe consequences, and thus matters for the criticality.

Vinnem (2010), as another example to link failure events and criticality, refer to failure events on safety-related equipment by the term 'safety critical failures'; such as for example, if an emergency shutdown valve does not close on demand, this is considered a 'safety critical failure'. Such a link works fine for a single component system, but is not necessarily applicable for example for the redundant system considered above. There is then a need to address the relevant system in more detail and understand how the critical and dangerous failures might occur. Such a definition is provided in Hauge and Lundteigen (2008), where the term is defined as "a failure that prevents the component to perform its safety function, i.e. to bring the process to a predefined safe state".