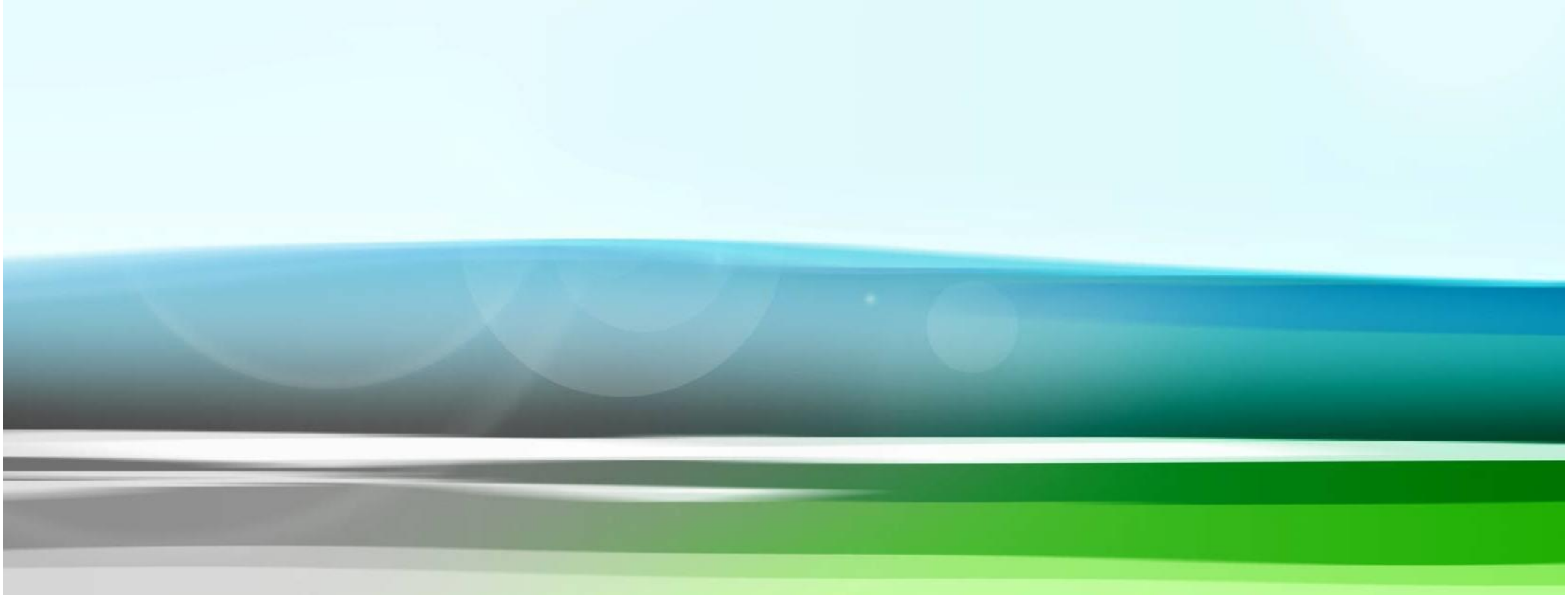


The Use of an Operator as a SIL 1 component in a Tank Overfill Protection System

By Andrew Derbyshire IEng MIET
Senior Safety Consultant
Det Norske Veritas

MANAGING RISK

In the beginning

- Hazard XXIII held in Southport between 12th – 15th November 2012
  - David Embrey and Jamie Henderson – *Human Reliability Associates, UK*

An independent evaluation of the UK Process Industry Association Gap Analysis tool for addressing the use of an operator as a SIL 1 component in tank overfill protection systems.

The UK Process Industry Association (UKPIA) has developed a minimum set of requirements for an operator to be considered part of a SIL1 safety function in relation to tank overfill protection systems at refineries and terminals. The requirements address areas such as systems architecture, human factors, communication and alarm management. This set of requirements was used by the UKPIA to develop a self assessment tool (the SIL 1 human factors self assessment tool) for organisations to assess an actual or proposed Safety Instrumented System (SIS) that incorporates a human operator

In the beginning

- Hazard XXIII held in Southport between 12th – 15th November 2012
  - David Embrey and Jamie Henderson – *Human Reliability Associates, UK*

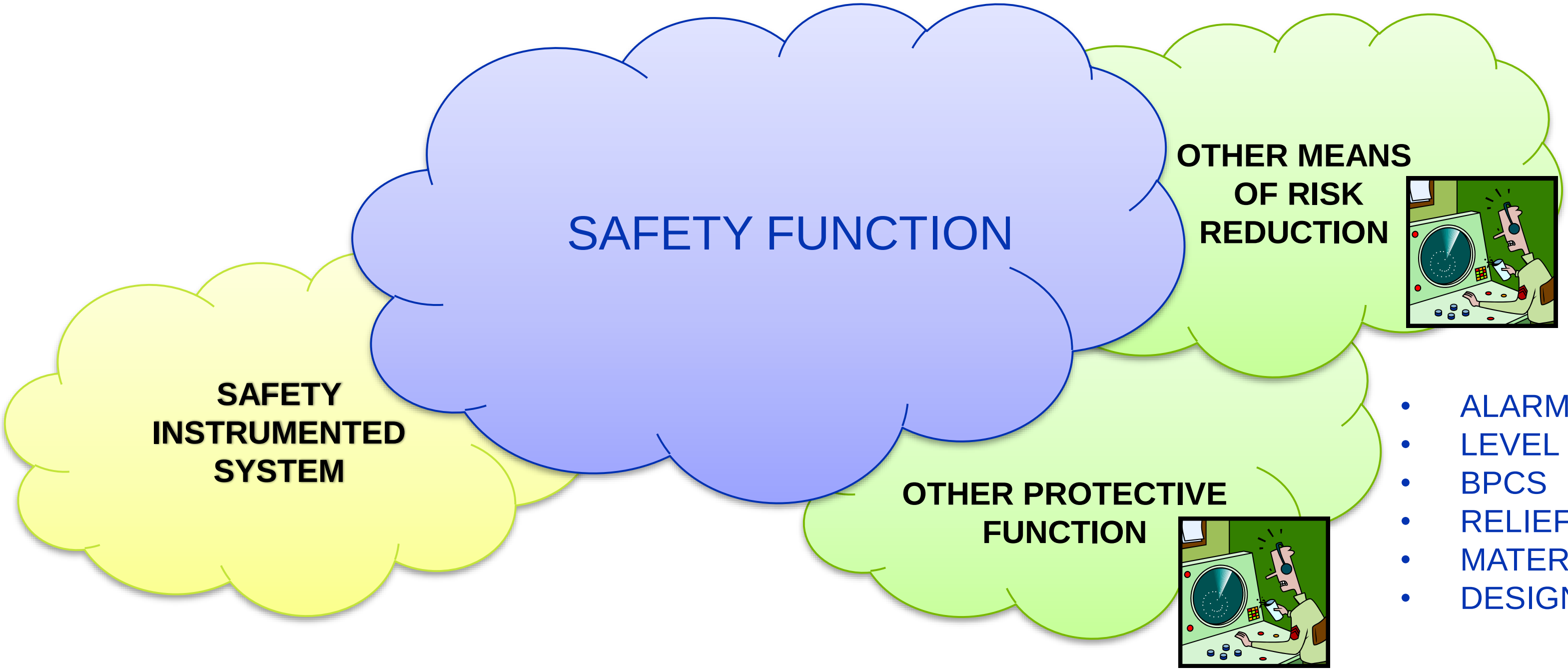
An independent evaluation of the UK Process Industry Association Gap Analysis tool for addressing the use of an operator as a SIL 1 component in tank overfill protection systems.

The UK Process Industry Association (UKPIA) has developed a minimum set of requirements for an **operator to be considered part of a SIL1 safety function** in relation to tank overfill protection systems at refineries and terminals. The requirements address areas such as systems architecture, human factors, communication and alarm management. This set of requirements was used by the UKPIA to develop a self assessment tool (the SIL 1 human factors self assessment tool) for organisations to assess an actual or proposed **Safety Instrumented System (SIS) that incorporates a human operator**

Operator to be considered part of a SIL 1 **Safety Function**

What is a Safety Function…??

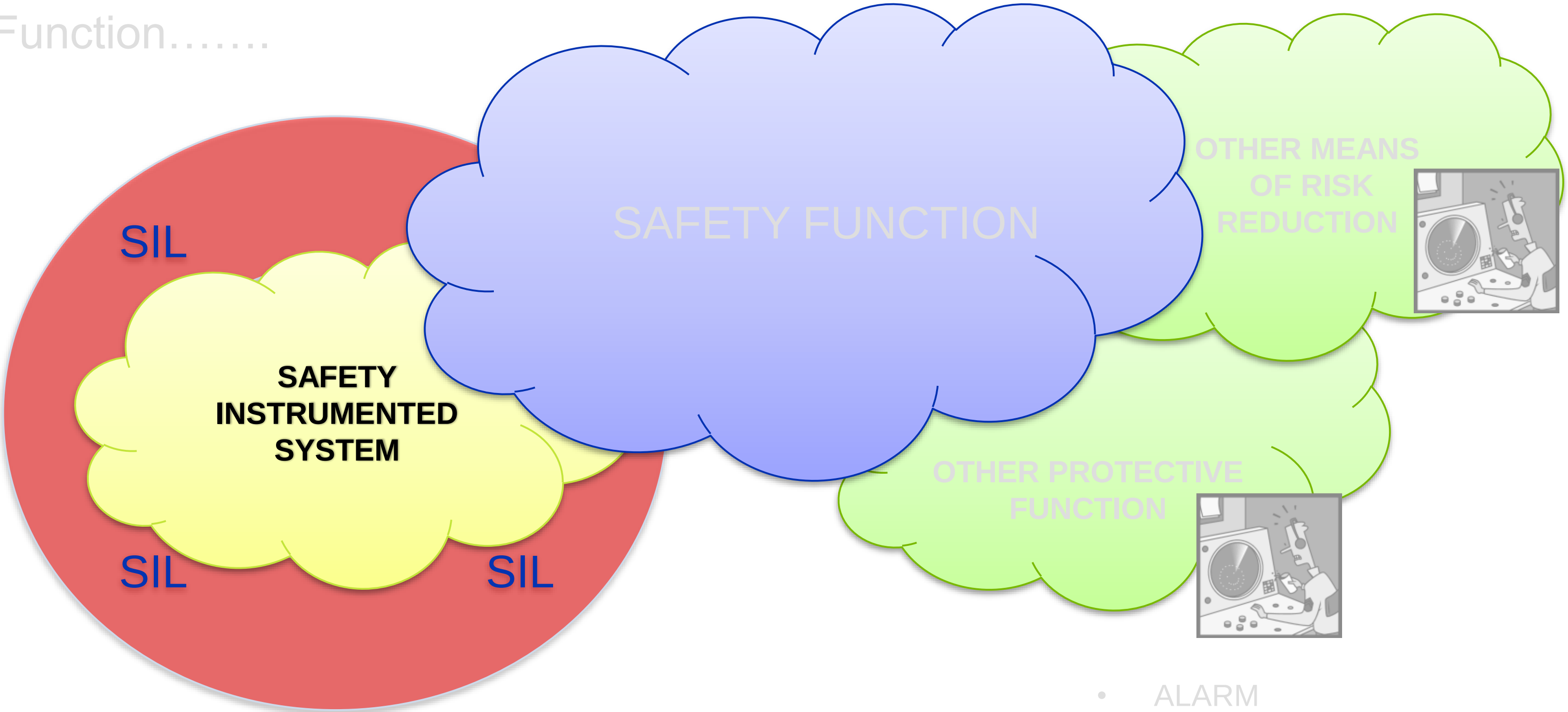
Function to be implemented by an SIS, other technology safety related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event.
IEC 61511:2004 Part 1 Clause 3.2.68


SAFETY FUNCTION
OTHER MEANS OF RISK REDUCTION
SAFETY INSTRUMENTED SYSTEM
OTHER PROTECTIVE FUNCTION

- ALARM
- LEVEL GAUGE
- BPCS
- RELIEF VALVE
- MATERIAL SELECTION
- DESIGN PHILOSOPHY

Operator to be considered part of a **SIL 1** Safety Function

Safety Function…….


SIL
SAFETY INSTRUMENTED SYSTEM
SIL
SIL
SAFETY FUNCTION
OTHER MEANS OF RISK REDUCTION
OTHER PROTECTIVE FUNCTION

- ALARM
- LEVEL GAUGE
- BPCS
- RELIEF VALVE
- MATERIAL SELECTION
- DESIGN PHILOSOPHY

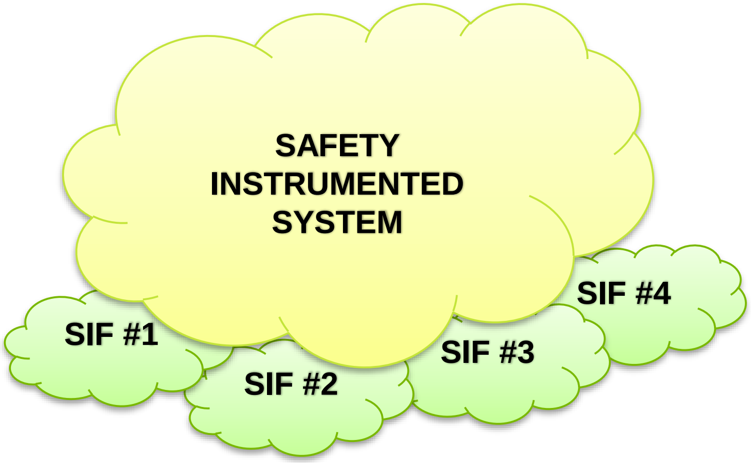
What is SIL…??

discrete level for specifying the safety Integrity requirements of the SIFs to be allocated To the SISs
IEC 61511:2004 Part 1 Clause 3.2.74

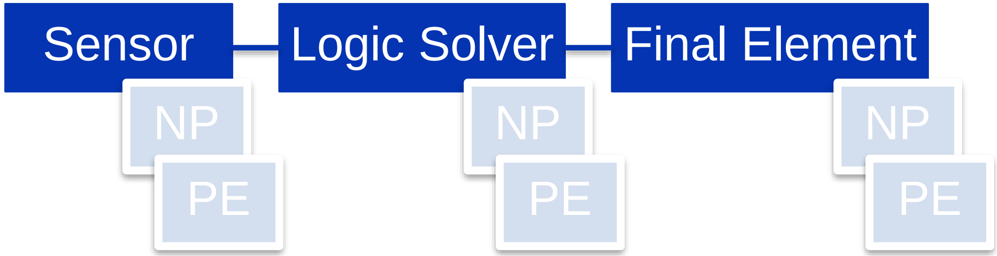
Safety Instrumented System that incorporates a Human Operator

Safety Instrumented System…….

Instrumented System used to implement one or more safety instrumented functions. An SIS is composed of any combination of Sensor(s), Logic solver(s), and Final element(s) .
IEC 61511:2004 Part 1 Clause 3.2.72



e.g.



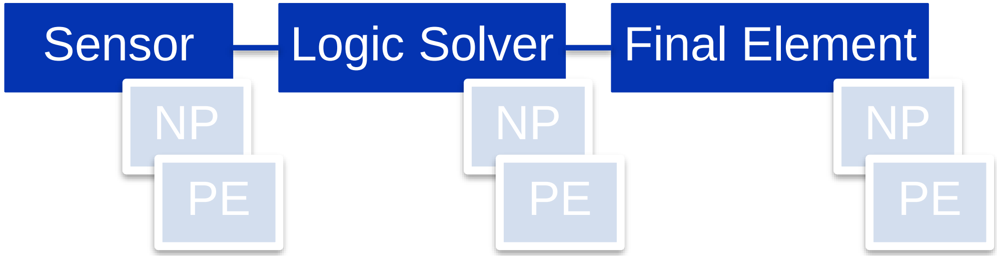
Safety Instrumented System that incorporates a Human Operator

Safety Instrumented System…….

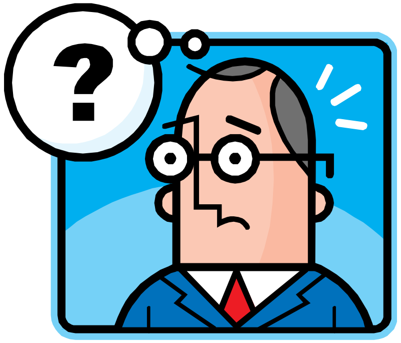
Instrumented System used to implement one or more safety instrumented functions. An SIS is composed of any combination of Sensor(s), Logic solver(s), and Final element(s) .
IEC 61511:2004 Part 1 Clause 3.2.72

SAFETY INSTRUMENTED SYSTEM

e.g.



NOTE 5 When a Human action is a part of an SIS, the availability and reliability of the operator action must be specified in the SRS and included in the performance calculations for the SIS. See IEC 61511-2 for guidance on how to include operator availability and reliability in SIL calculations.
IEC 61511:2004 Part 1 Clause 3.2.72

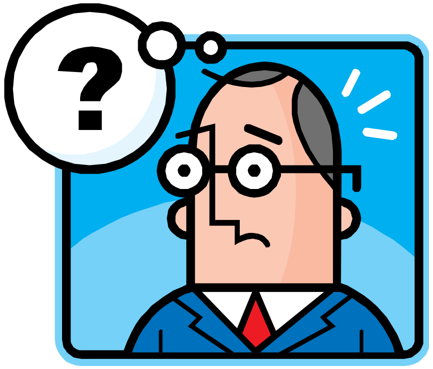


IEC 61511:2004 Vs IEC 61511:2012 (Draft)

Safety Instrumented System…….

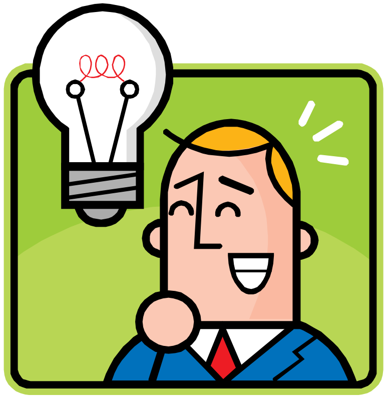
2004:
Instrumented System used to implement one or more safety instrumented functions. An SIS is composed of any combination of Sensor(s), Logic solver(s), and Final element(s) .

NOTE 5 When a Human action is a part of an SIS, the availability and reliability of the operator action must be specified in the SRS and included in the performance calculations for the SIS. See IEC 61511-2 for guidance on how to include operator availability and reliability in SIL calculations.
IEC 61511:2004 Part 1 Clause 3.2.72



2012:
Instrumented system used to implement one or more SIF

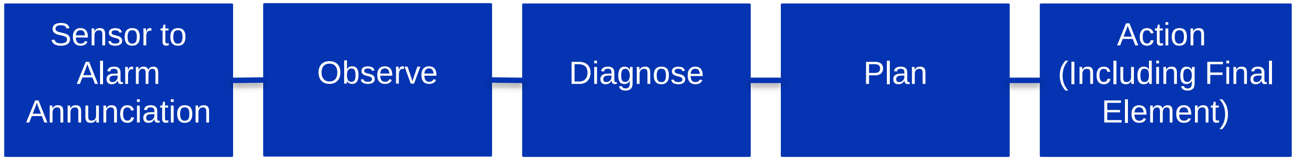
NOTE 3 When a Human **interaction** is a part of an SIS, the availability and reliability of the operator action must be specified in the SRS and included in the performance calculations for the SIS. See IEC 61511-2 for guidance on how to include operator availability and reliability in SIL calculations.
IEC 61511:2012 Part 1 Clause 3.2.71



Consideration..??

1. **Operator** to be considered part of a **SIL 1** Safety Function

2. Safety **Instrumented** System that incorporates a **Human** Operator



Sensor to Alarm Annunciation

Observe

Diagnose

Plan

Action (Including Final Element)

What if they are only Considering a Human Operator as interacting with the SIS

The evidence in the paper to suggest contrary to this:

1. Introduction

‘The terms of reference of the review were that, in accordance with IEC 61511, operators may form a part of a SIL 1 safety function’

‘inclusion of an operator within a SIL1 safety function as part of the end to end safety function’

‘factors necessary to justify the use of an operator as a SIL 1 component in a Safety Instrumented System (SIS)’

2. Review of the Content of the Tool

‘ factors or conditions necessary for an operator to act as part of a SIL 1 safety function. This was interpreted as confirming that all variables that might affect operator response to an alarm in an overfill scenario were included in the tool’

3. Restructuring the Tool

‘which allows the focused evaluation of the most relevant factors necessary to justify the use of an operator as a SIL 1 component in a SIS.’

‘Operators and Safety Systems for Overfill Protection of Tanks’

‘The analysis should be concerned solely with the probability of the operator responding in a timely fashion to a SIL 1 alarm’

When would you consider a Human Operator interacting with a SIS

λ_{DD} Failure modes in a SIL Capable Element

MTTR calculations

Notify operator of SIS actions

Notify operator of reduced HFT

Bypassing of the SIS

The Human may interact with a part of the SIS but must NOT be considered a part of implementing the Safety Instrumented Function.

The important issue with any interaction between the SIS and the operator is That the means of interaction must not prevent the SIS from performing its SIF.

Conclusion

Functional Safety is about implementing risk reduction within a defined level of integrity in the form of an autonomous system capable of placing or maintaining a process in a safe state. In order to achieve this a Safety Instrumented System, as defined by IEC 61511, does not place any direct requirements on the individual operators or maintenance person. Neither IEC 61511 or any other Functional safety related standard allows the substitution of one of the fundamental 3 elements, Sensor(s), Logic Solver(s) or Final element(s) with a human operator.

As defined in IEC 61511 a human operator maybe used within other means of risk reduction and this maybe considered in a LoPA study so long as there is sufficient independence. A human operator may interact with part of a SIS however this is not to say they form part of the Safety Instrumented Function being achieved by the SIS. Functional Safety and IEC 61511 in particular does not allow the use of a human operator to act as the logic solver in a SIS responding to an alarm in order to action the final element. A Human decision to respond to an alarm can be considered the case for other protective means but not for Functional Safety.

The paper presented at the Hazard XXIII on the use of an operator as a component in a SIL 1 level tank overfill protection system is not in compliance with IEC set of Functional Safety standards and specifically IEC 61511. The use of terms such as SIL and SIS in the paper have been misinterpreted by the author and used out of their perceived context. The paper is in jeopardy of placing the process industry into a false sense of security by adopting these practices and I recommend that the IEC 61508 Association respond to UKPIA with a committee backed letter of disapproval of this practice.

Safeguarding life, property and the environment

www.dnv.com

MANAGING RISK

DNV