NOPSA

NATIONAL OFFSHORE PETROLEUM SAFETY AUTHORITY

SAFETY ALERT 45

Functional Safety of Control Systems

What happened?

NOPSA has encountered a number of instances, in a diverse range of applications, where Operators have introduced equipment or systems that have potential weaknesses in the design of their safety-related control systems.

In some cases, Operators have been unaware of the significance of control systems as control measures against Major Accident Events and Dangerous Occurrences, and have consequently not used appropriate safety management techniques in their design and operation.

What could go wrong?

Inadequate design of safety-related control functions can cause death or injury when they do not perform in the intended manner. Examples include unsolicited movements of machinery, failures of interlocks, or excursion of processes beyond safe limits.

Since the source of harm results from the incorrect functioning of the control system, and not directly from the physical implementation of the control system itself, the term 'functional safety' is used to describe the subject.

The use of programmable control devices is increasingly prevalent throughout industry due to their inherent flexibility and relatively low cost. While this flexibility can result in risk reduction unachievable by other means, without adequate precautions it can also introduce other risk factors. These other risks may not be as visible, and can remain undetected for long periods, until manifesting themselves as a Dangerous Occurrence or an accident event.

Key Lessons:

If the failure of a control system could create a hazard which may result in an accident or Dangerous Occurrence, then it is safety related. Systems include: crane control; automated pipe handling; diving control; process control; emergency shut-down; gas detection; high integrity protection systems (HIPS); dynamic positioning; drilling table control; and well control.

Operators should carry out an audit of their control systems to identify those that are safety related, and reassure themselves that such systems are adequately designed, constructed and maintained to reduce risks arising from their use to as low as reasonably practicable.

In particular, NOPSA draws Operators' attention to control systems where programmable devices are used. These devices include programmable logic controllers, smart instruments, computer-based safety management systems, motor drives and any other devices containing microprocessors.

Contact

For further information email alerts@nopsa.gov.au and quote Alert 45.