TÜVRheinland®
Risktec

RISKworld / The Newsletter of Risktec Solutions / Spring 2018 p10-11

Wireless communication in major hazard sectors: Challenges and solutions

Many major hazard sectors deploy control and instrumentation (C&I) based safety systems to provide the necessary level of risk reduction for operational plant that would otherwise be unacceptably hazardous. Wireless communication for such systems is more easily installed and maintained than cabling, but what challenges are introduced and can they be solved?

A C&I safety system comprises a number of separate elements which must communicate in order to perform its intended safety function. This communication is traditionally enabled using tried and tested technology based on copper or fibre optic cabling (Figure 1).

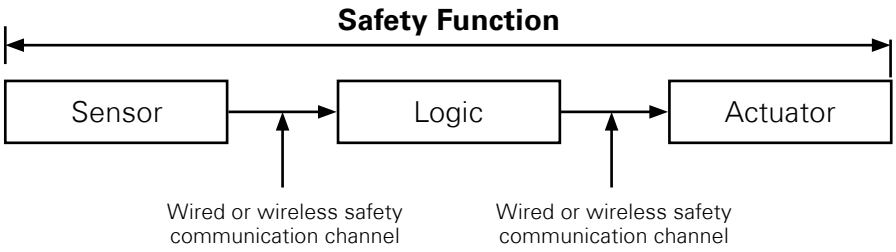

Figure 1 – Safety system elements

The time, trouble and cost of buying and installing communications cabling may be significant and, if disproportionate to the safety benefit, might preclude deployment of risk reduction measures. This is more likely to be the case where the distance between sensors, logic and actuators is significant, or where, as often happens on legacy sites, the installation of additional cabling is potentially hazardous to existing plant.

The continuing advances in commercial off-the-shelf (COTS) wireless communications equipment and the batteries that enable truly wireless operation, has led to use of this technology in non-safety related industrial applications. So far, there has been limited uptake of COTS wireless communications for safety-related systems, except for applications such as crane control and basic data and alarm communications systems.

More widespread use of COTS wireless communications for general safety-related applications is anticipated where the required level of risk reduction is low, as evidenced by the increasing availability of suitable equipment from major C&I equipment vendors, and the development of international standards to facilitate deployment in some major hazard sectors.

NEW CHALLENGES

COTS wireless communication introduces a number of important considerations which are not applicable to safety-related systems using wired communications.

Safety: Wireless communication utilises complex programmable electronic equipment; and demonstrating compliance with functional safety standards such as BS EN 61508 may be challenging.

Security: Wireless communication provides a new attack vector (e.g. eavesdropping, denial of service, hijacking) since it does not require the attacker to gain physical access to the safety related system.

Design: Predicting the reliability of wireless communications during the design phase may be more difficult than for wired communications, as the topology of the site and the presence of temporary obstructions such as scaffolding or vehicles could have a significant detrimental effect.

Maintenance: Routine maintenance of wireless communications equipment could cause spurious data to be sent to the safety-related system, leading to unintended actuation or failure.

Decommissioning: Off-site disposal of a 'failed' wireless device may provide an attacker with the configuration data necessary to mount an attack on the safety-related system from a location external to the site.

SOME SOLUTIONS

There is a broad range of solutions to these challenges.

White channel / black channel communications: Communications must either be designated as 'white channel' or 'black channel'. White channel communication is characterised by the need to provide a functional safety justification for the associated equipment against standards such as BS EN 61508. However, functional safety justification of communications equipment is not required if the remaining elements of the safety-related system have been designed to detect and appropriately respond to all credible communications failures. In this case, communication may be designated as black channel.

Security measures: A security risk assessment should be completed, with identified threats countered using a defence-in-depth approach where reasonably practicable, to avoid reliance on individual security measures that may be overcome should a threat evolve over time.

Reliability and coexistence: A site specific survey should be completed to correctly locate and configure the COTS wireless equipment in order to ensure adequate communications reliability is achieved, and to ensure adequate separation from any existing equipment that is either sensitive to or emits electromagnetic energy.

Latency: The time taken for the wireless transmission and reception of data may suffer increased latency (i.e. a longer delay) than for equivalent wired communication. The overall system latency is dependent upon the wireless communications system design, which must ensure that the overall safety system achieves its required speed of response.

Network topology: The location of each wireless device and how they are wirelessly interconnected, in either a mesh or star network for example, will generally improve reliability or reduce latency respectively.

Wireless protocol: The standard, policies, procedures and formats which define communication between two or more devices over a network is known as the wireless protocol. Selection of an appropriate protocol is a significant decision, influencing the ability to deliver a number of important factors including security and safety.

Procedural controls: Operating and maintenance procedures must ensure the safety-related system is not compromised by any permitted maintenance activities on the wireless communications equipment. Decommissioning procedures must maintain the security of the system by ensuring the permanent removal of all wireless configuration data when components of the system are decommissioned.

CONCLUSION

When the time, trouble and cost precludes deployment of a safety-related system using wired communications, COTS wireless communications may provide an acceptable alternative if the level of risk reduction required from the system is low. However, the design, safety and security justification of such a system must acknowledge and adequately address the specific challenges that the use of COTS wireless technology introduces.

Contact: Kevin Charnock
kevin.charnock@risktec.tuv.com