GAS SECURE

SAFE WIRELESS™

Wireless communication in safety systems

Wireless sensors have been around for some time. The motivating factors for installing wireless equipment are easy to identify; simplicity of installation and flexibility in operation.

Just as the benefits are easy to see, so are the potential challenges. The main challenges with safe wireless communication are to guarantee a short response time and to immediately detect loss of contact with sensors.

Wireless instruments are most often battery powered and are hence energy constrained. This limits the rate at which the instruments can report process values. For most process monitoring applications, this is not a major obstacle as the process values in question tend to change relatively slowly. For safety applications, the picture is somewhat different. For most safety applications continuous monitoring is necessary and a short latency (response time) needs to be guaranteed if a safety critical situation arises. However, the average bandwidth requirement is modest. Thus the primary difficulty in designing a wireless safety system is having a guaranteed short latency while not depleting the batteries. In addition, full control of all network message traffic is required, and loss of contact with a device must be identified immediately.

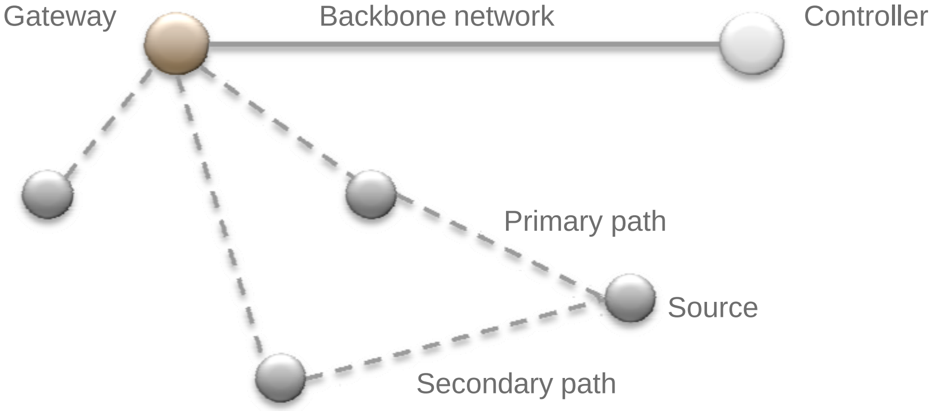
Wireless gas detection

GasSecure has developed an optical gas detector, the GS01, that operates with significantly lower power consumption than today’s state of the art detector units. This allows for wireless operation with battery life exceeding two years. In addition, GS01 will not need recalibration and performs equally or better than state of the art detectors.

The detector is intended for monitoring applications as well as for safety applications. For safety applications, the communication with the controller needs to meet reliability requirements according to SIL2 (Safety Integrity Level) guidelines as described in IEC 61508 Ed2.0. GasSecure’s patent pending wireless communication system meets the requirements of fast response time, power efficiency and full control of network traffic. The detector itself is also developed according to IEC 61508 Ed2.0 and meets the performance requirements of IEC 60079-29-1.

Wireless mesh networks

Simple wireless networks, like WLAN, rely on adequate radio connection between the information source and receiver. In the general industrial case this cannot be assumed, and additional wireless nodes are installed to act as relays. These nodes may also have sensing capability and they may, or may not, be battery powered. Having relay nodes in the network has the benefit of creating secondary paths. If the normal path used by a node is obstructed or becomes unavailable, the information source may choose to transmit its data along the secondary path. This leads to immensely stable and predictable networks.



The deployment of a wireless sensor network is simple. The nodes are placed in their desired locations and powered on. Subsequently, each node will spend some initial time conferring with its neighbors, obtaining an image of the network and the available paths to the network gateway. The network information will include not only what neighbors are available for communication, but also the associated quality of each individual link. The aggregated information is stored in the gateway, which is responsible for scheduling communication opportunities.

Once the network has stabilized, the traffic intensity drops. However, the nodes will continue to update their neighbor link information, including the possible removal or addition of nodes. In this way the network becomes adaptable to changes in the topology or of the environment.

Wireless sensor network standards

There are several communication protocols to choose from in the wireless sensor network area. In the process industry wirelessHART and ISA100.11a are the two most promising contenders. The gas detector and gateway from GasSecure has therefore been designed to be able to handle both these standards.

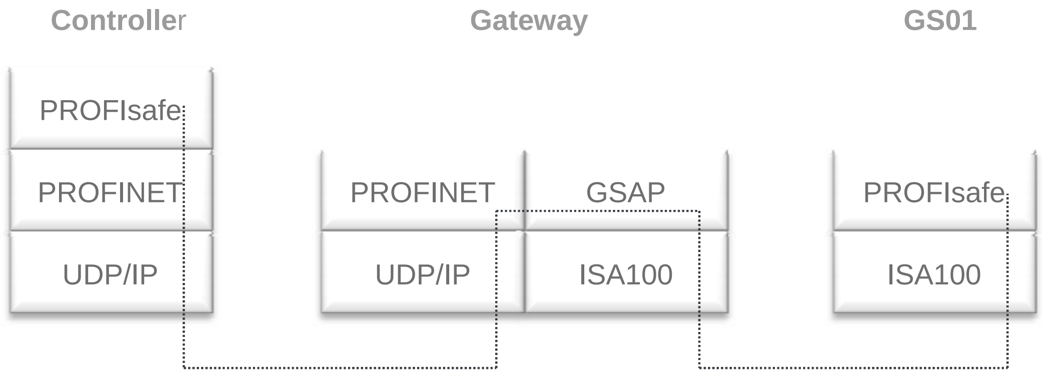
While standards ensure interoperability between different vendors of equipment, it is still possible to tailor the gateway to obtain a performance that is optimized for a particular application. One typical parameter to optimize is the number of allowed radio hops in the network. Increasing the number of hops allows networks spanning a large geographical area whilst increasing both latency of the packets and the processing load on the relay nodes. Similarly, the maximum number of children associated with any node may be configured. A large number enables the formation of dense networks. The flip side is the increased bandwidth demand on the relay node catering for the routing needs of a large number of devices.

Fulfilling the SIL2 requirements with SafeWireless^{TM}

For safe communication at SIL2, four error handling mechanisms must be supported: sequence numbering, timeout in the absence of response, device code name, and data consistency checking. The purpose of these mechanisms is to detect failures of the safety device in terms of packet loss, unacceptable network delay, bit errors, replay attacks, etc.

A safety controller will send a packet equipped with the four above mechanisms. The safety device needs to respond to that packet within the process safety time. If the device does not respond before the safety time elapses, the device is marked as unavailable in the control system. It is fundamental to the operation of all safety systems that the exchange of safe packets is initiated by the controller and that there is a one-to-one correspondence between the packet sent and the packet received. Once the controller receives a response, a new request can be issued.

Several options exist for implementing the four required safety features. One approach, chosen by GasSecure, is to base the product on a certified implementation of an open safety protocol. GasSecure has chosen PROFIsafe over PROFINET, due to the widespread use of the latter in process control applications. Other safety protocols may be implemented following the same principles of operation. The communication stack in the three entities can be viewed as follows:



The gateway has PROFINET implemented in order to communicate with the controller. It does not need PROFIsafe as this is relevant only to the controller and the device.

Setup of gateway and detectors

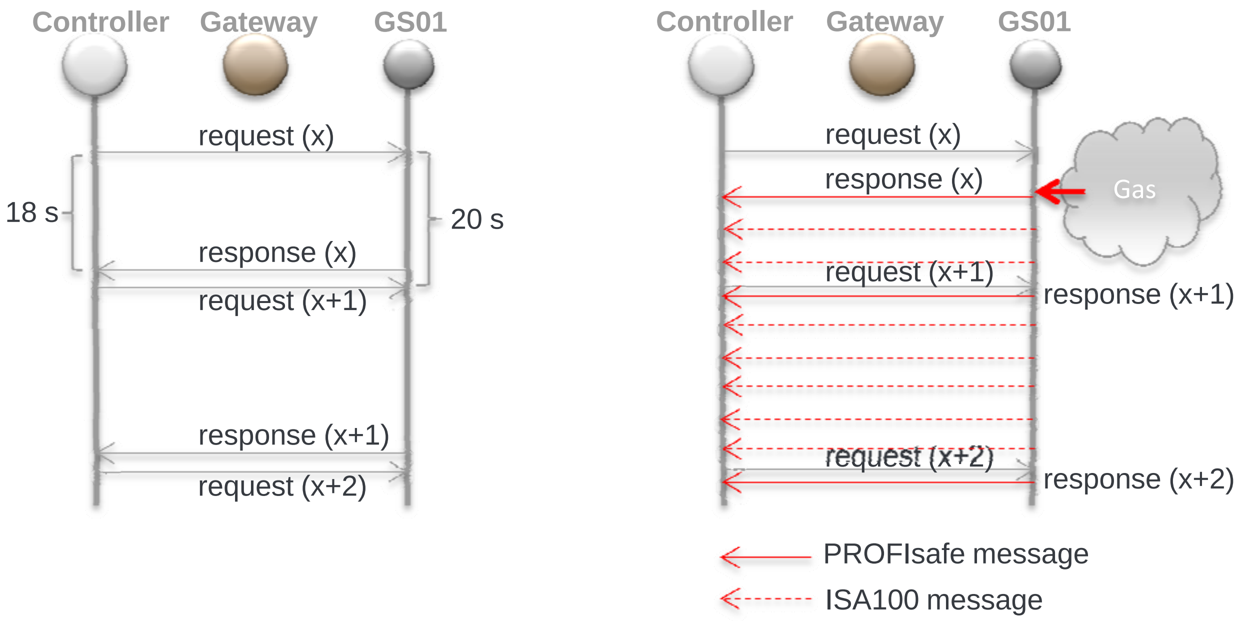
The process safety time for hydrocarbon gas detection as defined by IEC60079-29-1 is 60 seconds. In order for the device to be defined as safe by the control system it needs to respond to safe request packets within this time. Given that wireless packets may get lost in transmission, it is prudent to make several attempts at transmitting the packet within the process safety time. There is an obvious trade-off here. Frequent downlink transmissions will deplete batteries quickly but have a high probability of getting the message through, while rare transmissions save the batteries and reduce the success probability and thus the availability of the device. A reasonable balance between energy consumption and probability of success is to have three attempts within the process safety time, i.e. one downlink transmission every 20 seconds.

GasSecure will provide a response time of five seconds from gas enters the detector to the information about the event is received at the controller. In order to fulfill this requirement, and with three seconds for analysis at the detector, there needs to be opportunities to send uplink packets once every two seconds. The gas detector will therefore, during setup, request that bandwidth is set aside for this uplink transmission rate. The transmit opportunity is most often not used by the gas detector, and will hence result in only minimum extra power consumption. However, the fact that bandwidth has been reserved ensures that the latency requirement is met.

To further optimize the network for the gas detection application, GasSecure has decided to limit the number of hops to two and the number of devices per gateway to 25. This gives good geographical coverage and will support reasonably dense networks. At the same time, it will not adversely affect the energy consumption of the devices. It is important to note that although the gateway now has been optimized for the gas detection application, it will still be a regular ISA100.11a gateway able to serve other ISA100.11a devices.

Modes of operation

When gas is detected by the device, it needs to report the event at the earliest opportunity. However, downlink safe request packets arrive only once every 20 seconds and there is a one-to-one mapping between request and response. In other words, once the detector has responded to a safe request it is unable to report gas until a new request has been received. It will be "blind". This apparent dilemma is solved by delaying the safe response until just before a new request is expected. This way, the "blind" time is kept to two seconds and the detector is always ready to report gas should it be necessary. Thus, most uplink packets will be safe responses sent once every 20 seconds, only containing status information in the detector. It will serve primarily as an "alive" signal, indicating to the control system that the detector is operating as it should and that the communication link is open. This sequence of packets is shown in the figure below. If gas is detected, the detector will transmit messages every two seconds. These intermediate messages between safe messages are in the regular ISA100.11a monitoring format, not PROFIsafe messages.



GasSecure estimates that the battery will last for two years of continuous operation under normal conditions. If longer battery life is required there are two possibilities. One can either increase the time between uplink transmission opportunities from two to say four seconds. This will increase the total detector response time from five to seven seconds. Alternatively, and under the assumption that all GS01s are in close proximity, one could limit the topology to a star network. In such a configuration no GS01 will be called upon to route for others, and can hence spend more time in low power mode.

For non-safety applications, the GS01 may be used in other ISA100.11a networks in parallel with devices from other vendors. In this case the restrictions regarding maximum hop count and number of devices no longer apply.

Redundancy

Safety systems are designed to avoid single points of failure. There are several ways to implement redundancy in a wireless sensor network. The multiplicity of wireless nodes constitutes redundancy at the detector level. But redundant operation uplink may also be required in certain applications, preferably both at the gateway and at the controller. Several options exist:

Internal gateway redundancy: A gateway consists of a number of functional roles. Using the ISA100.11a nomenclature they can be identified as backbone router (handles the physical interface), system manager (handles the setup and real time control of the network), and gateway (higher level protocol conversions). Normally these logical entities are contained within the same box, but it is conceivable to split the backbone router as a separate physical entity. Having done so, it becomes possible to have two or more backbone routers controlled by the same system manager. This will eliminate single points of error that occur on the physical interfaces.

Multiple gateways: The ISA100.11a specification supports having multiple gateways complete with backbone routers and system managers. Each gateway will address a unique subset of the installed gas detectors. In case one of the gateways experiences a failure, its load will be partitioned among the remaining gateways. After a transition period used for this network reconfiguration, the operation will continue as before.

Multiple controllers: Having two or more controllers introduces redundancy at the highest level in the control architecture. This is supported by the ISA100.11a standard, but will need additional integration with control system vendors.

The GS01 represents a totally new concept in hydrocarbon gas detection. Its unique low power detection principle has paved the way for wireless communication. Furthermore, the implementation of SafeWireless™ enables its use in safety critical applications. GasSecure's patent pending wireless communication system meets the requirements of fast response time, power efficiency and full control of network traffic.