Secure Remote Monitoring
Technical Note

Options and Security Considerations for Remote Monitoring

Remote monitoring capabilities are implemented in a range of different physical and logical configurations. The available configurations allow partners and customers to select from the most appropriate combination of cost, ease of deployment and security.

Air Gap Deployment

Overview	All sensing is undertaken using duplicate physical sensors that are physically separated from sensors that are involved in the operation of the plant (e.g., PLC connected sensors).
Pros	Most secure, complete physical (and logical) isolation from plant control systems.
Cons	Higher costs - duplication of sensing devices and installation requirements.

The “Air Gap” deployment is completely physically separated from any existing or new control systems, sensors, and devices. It exists as a completely independent monitoring system that replicates key sensor inputs. A separate communications network is used that does not touch any on-site communications infrastructure.

It is the most secure deployment since there are no physical connections between the control and monitoring systems. There is no way to attack the control systems via the remote monitoring system as no paths are available between the two. It is immune from stepping-stone attacks and provides no pathway for an attacker to transition to any other part of the system being monitored.

This deployment topology is the least efficient in terms of use of resources. Sensors must be duplicated and while DCO’s wireless and energy harvesting sensor solutions reduce installation requirements they are not fully eliminated. Care must also be taken to ensure that any new sensing accurately replicates the physical configuration of existing sensors – e.g., if replicating a thermowell sensor then either another thermowell is implemented or a surface probe must be configured to adjust readings to reflect the installation method.

Fire Break Deployment

Overview	All sensing is undertaken using duplicate physical sensors that are physically separated from sensors that are involved in the operation of the plant (e.g., PLC connected sensors).
Pros	High security with safe and efficient re-use of existing sensor resources.
Cons	Elevated complexity of integration and installation versus an integrated deployment.

The “Fire Break” deployment is completely logically separated from any existing or new control systems, sensors, and devices. It utilises very specific physical connections to existing sensors that cannot physically provide a route for attack into the control systems. Most often it is integrated with existing 4-20mA (or similar simplified comms protocols) to provide a duplicate view of the sensor data in a way that does not provide any stepping-stones from monitoring to control system.

It would be typical for the deployment to utilise a separate communications network – most often a dedicated 3/4/5G mobile network uplink – that does not touch any on-site communications infrastructure.

This deployment is highly secure since the physical links between systems provide no usable route between those systems for an attacker. Where, as is very common, the integration is provided through routes such as 4-20mA current loops the monitoring system has no physical mechanism to affect the loops – the electronics provided is not physically cable of driving the loop, only of monitoring the loop (alongside the existing monitoring equipment).

This deployment topology is more efficient than full air gap in use of resources. Duplication of sensors can be reduced. If there are gaps in the existing sensor coverage, then DCO's wireless and energy harvesting sensor solutions simplify the deployment of new sensors into those gaps.

Integrated Deployment

Overview	Sensing is a mix of new physical sensors, integration with existing sensors and integration with control systems for the process (e.g., PLCs).
Pros	Maximises available data, reduced installation costs, duplication avoided.
Cons	Increased security risk profile – network level (or similar) touchpoints between remote monitoring system and control systems.

The "Integrated" deployment makes use of shared sensors and devices to achieve the greatest sensor coverage and co-existence. It is generally a combination of new and existing sensing where existing PLC level information can be integrated into the remote monitoring solution alongside new sensor solutions that plug existing coverage gaps.

While it is still possible for a separate communications network to be used by the remote monitoring system it is also likely that a customer may choose to route monitoring traffic through their existing network topology. This permits the customer to manage PLC and monitoring traffic in a similar way using the same network infrastructure.

The security of this solution is reduced versus other options, it presents similar security risks to general purposes computing devices shared common communications infrastructure. With physical and logical connections between systems there is the possibility of routes being provided that enable stepping-stone type attacks. This can be greatly reduced by limiting the types of connections to the least capable technology that enables communications between the PLC and the remote monitoring installation – e.g., functionality restricted protocols. However, it is very common that physical integration is in the form of network level links (e.g., shared Ethernet) and so the risks inherent in such inter-system links cannot be completely avoided.

This deployment topology is the most efficient in terms of use of resources. Duplication of sensors can largely be avoided and in some cases may be completed eliminated. If there are gaps in the existing sensor coverage, then DCO's wireless and energy harvesting sensor solutions simplify the deployment of new sensors into those gaps.

© DCO Systems Ltd 2021
Errors and omissions excepted; alterations possible without prior notice. Revision: 1.1.1