4.4.4.2 Rationale and supplemental guidance

Safety related IACS assets usually have different security requirements than basic control system components or systems, and components interfaced to the control system components. Safety related zones typically require a higher-level of security protection due to the higher potential for health, safety and environmental consequences if the zone is compromised.

4.4.5 ZCR 3.4: Separate temporarily connected devices

4.4.5.1 Recommendation

Devices that are permitted to make temporary connections to the SUC should be grouped into a separate zone or zones from assets that are intended to be permanently connected to the IACS.

4.4.5.2 Rationale and supplemental guidance

Devices that are temporarily connected to the SUC (for example, maintenance portable computers, portable processing equipment, portable security appliances and universal serial bus [USB] devices) are more likely exposed to a different and wider variety of threats than devices that are permanently part of the zone. Therefore, these devices should be modelled in a separate zone or zones. The primary concern with these devices is that, because of the temporary nature of the connection, they may also be able to connect to other networks outside the zone. However, there are exceptions. For example, a hand-held device that is only used within a single zone and never leaves the physical boundary of the zone may be included in the zone.

4.4.6 ZCR 3.5: Separate wireless devices

4.4.6.1 Recommendation

Wireless devices should be in one or more zones that are separated from wired devices.

4.4.6.2 Rationale and supplemental guidance

Wireless signals are not controlled by fences or cabinets and are therefore more accessible than normal wired networks. Because of this increased access potential, they are more likely exposed to a different and wider variety of threats than devices that are wired.

Typically, a wireless access point is modelled as the conduit between a wireless zone and a wired zone. Depending upon the capabilities of the wireless access point additional security controls (for example, firewall) may be required to provide appropriate level of separation.

4.4.7 ZCR 3.6: Separate devices connected via external networks

4.4.7.1 Recommendation

Devices that are permitted to make connections to the SUC via networks external to the SUC should be grouped into a separate zone or zones.

4.4.7.2 Rationale and supplemental guidance

It is not uncommon for organizations to grant remote access to personnel such as employees, suppliers and other business partners for maintenance, optimization and reporting purposes. Because remote access is outside the physical boundary of the SUC, it should be modelled as a separate zone or zones with its own security requirements.