Licensed copy: National Library of Scotland , National Library of Scotland, Version correct as of 16/11/2020

4.4 ZCR 3: Partition the SUC into zones and conduits

4.4.1 Overview

Subclauses 4.4.2 through 4.8.1 describe the ZCRs for partitioning the SUC into zones and conduits and provide rationale and supplemental guidance for each requirement. Subclause 4.4.2, sets out the base requirement for establishing zones and conduits within the SUC. Subclauses 4.4.3 through 4.4.7 are intended to provide guidance on assignment of assets to zones based upon industry best practices. This is not intended to be an exhaustive list.

4.4.2 ZCR 3.1: Establish zones and conduits

4.4.2.1 Requirement

The organization shall group IACS and related assets into zones or conduits as determined by risk. Grouping shall be based upon the results of the initial cyber security risk assessment or other criteria, such as criticality of assets, operational function, physical or logical location, required access (for example, least privilege principles) or responsible organization.

4.4.2.2 Rationale and supplemental guidance

The intention of grouping assets into zones and conduits is to identify those assets which share common security requirements and to permit the identification of common security measures required to mitigate risk. The assignment of IACS assets to zones and conduits may be adjusted based upon the results of the detailed risk assessment. This is a general requirement, but special attention should be given to the safety related systems including safety instrumented systems, wireless systems, systems directly connected to Internet endpoints, systems that interface to the IACS but are managed by other entities (including external systems) and mobile devices.

For example, a facility might first be divided into operational areas, such as materials storage, processing, finishing, etc. Operational areas can often be further divided into functional layers, such as manufacturing execution systems (MESs), supervisory systems (for example, human machine interfaces [HMIs]), primary control systems (for example, BPCS, DCS, remote terminal units [RTUs] and programmable logic controllers [PLCs]) and safety systems. Models such as the Purdue reference model as defined in IEC 62264-1 [9] are often used as a basis for this division. IACS product supplier reference architectures can also be helpful.

4.4.3 ZCR 3.2: Separate business and IACS assets

4.4.3.1 Requirement

IACS assets shall be grouped into zones that are logically or physically separated from business or enterprise system assets.

4.4.3.2 Rationale and supplemental guidance

Business and IACS are two different types of systems that need to be divided into separate zones as their functionality, responsible organization, results of initial risk assessment and location are often fundamentally different. It is important to understand the basic difference between business and IACS, and the ability of IACS to impact health, safety and environment (HSE).

4.4.4 ZCR 3.3: Separate safety related assets

4.4.4.1 Requirement

Safety related IACS assets shall be grouped into zones that are logically or physically separated from zones with non-safety related IACS assets. However, if they cannot be separated, the entire zone shall be identified as a safety related zone.