4.2 ZCR 1: Identify the SUC

4.2.1 ZCR 1.1: Identify the SUC perimeter and access points

4.2.1.1 Requirement

The organization shall clearly identify the SUC, including clear demarcation of the security perimeter and identification of all access points to the SUC.

4.2.1.2 Rationale and supplemental guidance

Organizations typically own and operate multiple control systems, especially larger organizations with multiple industrial facilities. Any of these control systems may be defined as a SUC. For example, there is generally at least one control system at an industrial facility, but oftentimes there are several systems that control various functions within the facility.

This requirement specifies that SUCs are identified for the purpose of performing cyber security analysis. The definition of a SUC is intended to include all IACS assets that are needed to provide a complete automation solution.

System inventory, architecture diagrams, network diagrams and dataflows can be used to determine and illustrate the IACS assets that are included in the SUC description.

NOTE The SUC can include multiple subsystems such as basic process control systems (BPCSs), distributed control systems (DCSs), safety instrumented systems (SISs), supervisory control and data acquisition (SCADA) and IACS product supplier's packages. This could also include emerging technologies such as the industrial Internet of Things (IIoT) or cloud-based solutions.

4.3 ZCR 2: Initial cyber security risk assessment

4.3.1 ZCR 2.1: Perform initial cyber security risk assessment

4.3.1.1 Requirement

The organization shall perform a cyber security risk assessment of the SUC or confirm a previous initial cyber security risk assessment is still applicable in order to identify the worst case unmitigated cyber security risk that could result from the interference with, breach or disruption of, or disablement of mission critical IACS operations.

4.3.1.2 Rationale and supplemental guidance

The purpose of the initial cyber security risk assessment is to gain an initial understanding of the worst-case risk the SUC presents to the organization should it be compromised. This is typically evaluated in terms of impacts to health, safety, environmental, business interruption, production loss, product quality, financial, legal, regulatory, reputation, etc. This assessment assists with the prioritization of detailed risk assessments and facilitates the grouping of assets into zones and conduits within the SUC.

For potentially hazardous processes, the results of the process hazard analysis (PHA) and functional safety assessments as defined in IEC 61511-2 [8] should be referenced as part of the initial cyber security risk assessment to identify worst-case impacts. Organizations should also take into consideration threat intelligence from governments, sector specific Information Sharing and Analysis Centers (ISACs) and other relevant sources.

Assessment of initial risk is often accomplished using a risk matrix that establishes the relationship between likelihood, impact and risk (such as, a corporate risk matrix). Examples of risk matrices can be found in Annex B.