a) Name and/or unique identifier – It is important for design and documentation purposes to be able to uniquely identify each zone or conduit.

b) Accountable organization(s) – The accountable organization is the person, group or groups who are responsible and accountable for the security of the zone or conduit.

NOTE The accountable and responsible organizations can be different. If so, they will both be identified.

c) Logical boundary – The logical boundary is important because it delineates the boundary between the zone or conduit and the rest of the system. It also helps identify the demarcation point for all communications entering or exiting the zone or conduit.

d) Physical boundary – It is important to document the physical boundary if the zone or conduit requires physical security to achieve its SL-T. If physical security could enhance (but is not required) the SL-T, it should preferably be documented.

e) Safety Designation – It is important to identify if the zone or conduit is safety related or contains safety related assets.

f) List of logical access points – Logical access points are any place where electronic information can cross the logical boundary of a zone or conduit. Logical access points need to be identified and documented as they may have vulnerabilities that can be exploited by threats.

g) List of physical access points – Physical access points (for example, fences, doors and enclosures) are any place where personnel can gain physical access to zone or conduit assets. Physical access points need to be identified and documented to determine appropriate means of monitoring and preventing unauthorized access.

h) List of data flows – In order to detect anomalies, it is important to identify and document the expected flow of data (for example, source, destination and protocol) throughout the system and, in particular, the flow of data in and out of a zone or conduit.

i) Connected zones or conduits – It is important to identify the connectivity between zones and conduits in order to identify all of the logical access points into and within the system. Typically, this is illustrated in a zone and conduit diagram.

j) List of assets and their classification, criticality and business value – It is important to identify the IACS assets contained within each zone or conduit and their classification, criticality and business value in order to develop an understanding of the consequences should that zone or conduit be compromised. When identifying consequences, it is important to consider the consequences to other zones/conduits as well as the zone/conduit in question.

k) SL-T – The SL-T communicates the level of protection required for a zone or conduit based upon the results of the risk assessment. Refer to 4.6.7 for further information.

l) Applicable security requirements – For each zone and conduit it is necessary to identify the applicable security requirements needed to achieve the SL-T. Some requirements may be common to all zones or conduits in the SUC while others may be specific.

NOTE Security requirements specification cannot be finalized until after completion of the detailed risk assessment (refer to 4.6).

m) Applicable security policies – For each zone and conduit, it is necessary to identify the applicable organizational security policies needed to achieve the SL-T. Some policies may be common to all zones or conduits in the SUC while others may be specific.

n) Assumptions and external dependencies – Oftentimes, the security of a zone or conduit is dependent upon factors outside of the zone or conduit, such as clean power and additional layers of physical and network security. These assumptions and interdependencies should be documented.

4.7.6 ZCR 6.5: Operating environment assumptions

4.7.6.1 Requirement

The CRS shall identify and document the physical and logical environment in which the SUC is located or planned to be located.