4.6.7.2 Rationale and supplemental guidance

SL-T is the desired level of security for a particular IACS, zone or conduit. It is established to clearly communicate this information to those responsible for designing, implementing, operating and maintaining cyber security.

SL-T may be expressed as a single value or a vector. Refer to IEC 62443-3-3:2013, Annex A for a discussion of the SL vector approach.

There is no prescribed method for establishing SL-T. Some organizations chose to establish SL-T based upon the difference between the unmitigated cyber security risk and tolerable risk. Whereas others elect to establish SL-T based on the SL definitions provided in Annex A of this document and IEC 62443-3-3:2013. Another approach, if a risk matrix is used (see Annex B for examples), is to qualitatively establish the SL. Starting from a reasonable estimate of SL (can also be none) the cyber security risk is evaluated by the risk matrix taking into account the countermeasures implied by the SL. If the risk is not acceptable, then the SL is raised (this means additional countermeasures are added) until the cyber security risk is acceptable. The SL derived from this analysis becomes SL-T.

4.6.8 ZCR 5.7: Compare unmitigated risk with tolerable risk

4.6.8.1 Requirement

The unmitigated risk determined for each threat identified in 4.6.6, shall be compared to the organization’s tolerable risk. If the unmitigated risk exceeds the tolerable risk, the organization shall determine whether to accept, transfer or mitigate the risk. To mitigate the risk, continue to evaluate the threat by completing 4.6.9 through 4.6.13. Otherwise, the organization may document the results in 4.6.14 and proceed to the next threat.

4.6.8.2 Rationale and supplemental guidance

The purpose of this step is to determine if the unmitigated risk is tolerable or requires further evaluation.

4.6.9 ZCR 5.8: Identify and evaluate existing countermeasures

4.6.9.1 Requirement

Existing countermeasures in the SUC shall be identified and evaluated to determine the effectiveness of the countermeasures to reduce the likelihood or impact.

4.6.9.2 Rationale and supplemental guidance

In order to determine residual risk, the likelihood and impact should be evaluated taking into account the presence and effectiveness of existing countermeasures. This step in the process focuses on identifying and evaluating existing countermeasures.

IEC 62443-3-3 provides guidance on types of countermeasures and their effectiveness by assigning a capability SL (SL-C) to each system requirement.

4.6.10 ZCR 5.9: Reevaluate likelihood and impact

4.6.10.1 Requirement

The likelihood and impact shall be re-evaluated considering the countermeasures and their effectiveness.