4.6.10.2 Rationale and supplemental guidance

The unmitigated likelihood determined in 4.6.5 does not account for existing countermeasures. In this step, countermeasures such as technical, administrative or procedural controls are considered and used to determine mitigated likelihood. Likewise, the consequences and impact determined in 4.6.4 should also be re-evaluated considering the identified countermeasures.

4.6.11 ZCR 5.10: Determine residual risk

4.6.11.1 Requirement

The residual risk for each threat identified in 4.6.2, shall be determined by combining the mitigated likelihood measure and mitigated impact values determined in 4.6.10.

4.6.11.2 Rationale and supplemental guidance

Determining residual risk provides a measure of the current level of risk as well as a measure of the effectiveness of existing countermeasures. It is an essential step in determining whether the current level of risk exceeds tolerable risk guidelines.

4.6.12 ZCR 5.11: Compare residual risk with tolerable risk

4.6.12.1 Requirement

The residual risk determined for each threat identified in 4.6.2, ZCR 5.1: Identify threats, shall be compared to the organization’s tolerable risk. If the residual risk exceeds the tolerable risk, the organization shall determine if the residual risk will be accepted, transferred or mitigated based upon the organization’s policy.

4.6.12.2 Rationale and supplemental guidance

The purpose of this step is to determine if the residual risk is tolerable or requires further mitigation. Many organizations define tolerable risk in their risk management policies.

4.6.13 ZCR 5.12: Identify additional cyber security countermeasures

4.6.13.1 Requirement

Additional cyber security countermeasures such as technical, administrative or procedural controls shall be identified to mitigate the risks where the residual risk exceeds the organization’s tolerable risk unless the organization has elected to tolerate or transfer the risk.

4.6.13.2 Rationale and supplemental guidance

When residual risk exceeds an organization's risk tolerance, steps need to be taken to reduce the risk to tolerable levels.

Countermeasures are applied to reduce risk. Cyber security countermeasures may be a combination of technical and non-technical (such as, policies and procedures). Another means of reducing risk is to reallocate an IACS asset from a lower security to a higher security zone or conduit in order to take advantage of the security countermeasures of the higher security zone or conduit.

IEC 62443-3-3 can be used as a guide to select appropriate technical countermeasures. The countermeasures identified in IEC 62443-3-3 have been assigned a SL-C rating which is beneficial in evaluating the effectiveness of the countermeasure.

Users may also want to evaluate the cost and complexity of countermeasures as part of the design process.