d) an identification of the potentially affected asset(s).

Some examples of threat descriptions are:

- A non-malicious employee physically accesses the process control zone and plugs a USB memory stick into one of the computers;
- An authorized support person logically accesses the process control zone using an infected laptop; and
- A non-malicious employee opens a phishing email compromising their access credentials.

Given the potential for a large number of possible threats, it is acceptable to summarize by grouping sources, assets, entry points, etc. into classes.

4.6.3 ZCR 5.2: Identify vulnerabilities

4.6.3.1 Requirement

The zone or conduit shall be analysed in order to identify and document the known vulnerabilities associated with the assets contained within the zone or conduit including the access points.

4.6.3.2 Rationale and supplemental guidance

In order for a threat to be successful, it is necessary to exploit one or more vulnerabilities in an asset. Therefore, it is necessary to identify known vulnerabilities associated with the assets to better understand threat vectors.

A generally accepted approach to identifying vulnerabilities in an IACS is to perform a vulnerability assessment. Additional information on IACS cyber security vulnerability assessments is available in ISA-TR84.00.09 [15].

Additionally, there are numerous sources of information regarding known and common vulnerabilities in IACS, such as the industrial control system computer emergency response team (ICS-CERT), IACS product suppliers, etc.

4.6.4 ZCR 5.3: Determine consequence and impact

4.6.4.1 Requirement

Each threat scenario shall be evaluated to determine the consequence and the impact should the threat be realized. Consequences should be documented in terms of the worst-case impact on risk areas such as personnel safety, financial loss, business interruption and environment.

4.6.4.2 Rationale and supplemental guidance

Estimating the worst-case impact of a cyber threat is an important input in performing the cost/benefit analysis of security controls. If the worst-case impact is low, the risk assessment team may decide to proceed to the next threat.

Existing PHA and other related risk assessments (such as, information technology, functional safety, business and physical security) should be reviewed to assist in determining consequences and impact.

The measure of impact may be qualitative or quantitative. One method is to use a consequence scale that is defined by the organization as part of their risk management system (refer to Annex B for examples).