The industrial control systems (ICS) phase will consist of performing a black box testing of the infrastructure connected to the ICS.

Secarma Ltd recommends that a mature and industry respected methodology such as CRAMM is followed. However, should the customer prefer another industry standard risk assessment and management methodology, Secarma is happy to utilise the customer's preferred methodology.

The specific methodology used for the assessment will be bespoke and unique to the customer's specific network, systems and business. However, a general high-level overview of the methodology to provide insight into the types of steps that a determined attacker may carry out:

1. Information gathering

a) Identification of business assets.
   a. Cataloguing technical platforms.
   b. Data flow.
   c. Communication protocols used.
   d. Connectivity to other networks.
   e. Identify business processes supported.
   f. Identify data processed.

b) Identify the business impact should the data be exposed.

c) Identification of security goals.

2. Threat Analysis

a) Determine the threat:
   a. Malware.
   b. Malicious insiders.
   c. "Script Kiddie" outsiders.
   d. Hostile foreign states.
   e. Equipment or power failure.
   f. Theft.
   g. Human error.
   h. "Acts of god"

3. Risk Management and Elimination

a) Identify existing security controls.

b) Identify countermeasures.

4. Implementation of Assessment

a) Determine scope of testing.

5. Architecture Review

a) Identify types of ICS systems.

b) Review the network architecture.

c) Identify all network access points.

d) Review device "hardening".

e) Review state of security patching.

f) Review intrusion detection system.

g) Review firewall policies.

h) Review communication protocols.

i) Review physical security controls.

j) Review authentication and authorisation mechanisms.

k) Review security logging and auditing.

l) Review cryptographic controls.

6. Network Analysis

a) Identify services running on the systems.

b) Network and system mapping.

c) Host identification.

d) TCP and UDP service port scans.

e) Network resource enumeration.

f) Application enumeration.

g) User enumeration.