ASSESS℠

Every critical asset security (CAS) scenario presents a unique problem set to the defense design that must be overcome to be successful. The Assess process provides the guidelines and tools to the defense designer to overcome these challenges. The Assess process leverages years of real-world experience and state of the art hardware and software tools to provide better defense design outcomes for defense designers of all experience levels.

Site Survey

The Axient CAS team first conducts an on-site visit to conduct an initial assessment of the customer facilities:

- Infrastructure requirements (power availably and type, C2 location)
- Available support equipment
- Existing communications infrastructure (Ethernet, Fiber Optic, Wireless)
- Conduct spectrum analysis
- Sensor selection and coverage plan development
- Line of Site (LOS) analysis and initial sensor placement selection
- Determine possible threat avenues of approach
- Identify frequency use approval authorization process for Radar, wireless communications and possible electronic warfare (EW) effectors as applicable

Sensor Optimization Process

Threat assessment and system layout process with interactive planning tool used by Axient SMEs to survey and plan appropriate sensors and systems for protection of an asset, site, or facility. This planning tool is a COTS tool based on software developed to support the military in optimizing CUAS weapon systems and sensor placement that is tailored to the needs of commercial customers.

Buildings Tool:

The buildings tool imports building and elevation information using LIDAR data and has the ability to automatically detect buildings based on user settings. Buildings can also be manually selected or deselected by the user. The buildings are then used for line-of-sight (LOS) analysis and as well as sensor placement optimization.

Scenario Builder:

The Scenario Builder is where the user sets geofences for the "Defended Areas", sensor "Allowed Areas," sensor "Restricted Areas," and Named Areas of Interest (NAIs). The sensors and in some cases, effectors are placed on the areas initially identified during the site survey. NAIs are used to place threat systems points of origin to be used in the Defense Design Optimization process.

Defense Design Optimization:

The Defense Design Optimization takes the previously built scenario and runs user selected optimization algorithms. The primary reasons to use optimization include minimizing sensor coverage gaps, to better defend against a wide range of threat courses of action (COAs), and to provide the expert defense designer with a high-quality starting point.

Operational Analysis:

Operational Analysis (OA) provides decision-support for planners, facility and corporate leadership and staff by providing them expected performance against threat COAs. The types of OA available include:

- Line-of-Sight (LOS) – Visualizes LOS obstructions which impact the ability to detect, acquire, and track objects of interest.
- Defended Area (DA) – A measure of how well a given area is defended against threat COAs.
- Raid Metrics (RAID) – Measures how well the system of systems defends against multiple, simultaneous threats.

Using Monte Carlo simulations and other analysis algorithms, OA points out potential weaknesses and strengths in the defense design which may indicate the need for additional sensors or mix of sensors.

System Deployment

After the site survey and analysis are completed, the customer-selected sensors are emplaced on site in accordance with the selected defense design sensor locations. The sensors are then connected to the command and control (C2) software, AWARE™, and undergo an onsite quality assurance test (QAT) to ensure the system operates as designed.

Defense Design System Testing:

The system is tested with Red Team assets similar to projected threats to test the defense design. If any deficiencies are found during the testing, appropriate adjustments will be made to correct the issues and the system will be tested again.