

# PROGRAMMIERTOOL FÜR DEN MISSIM SIMULATOR DER RUAG AEROSPACE



ENTWICKLUNG EINER PC-APPLIKATION ZUR ERSTELLUNG UND VERWALTUNG VON EMITTERN INKL. ÜBERPRÜFUNG UND DOWNLOAD

TECHNOLOGIE:

- C#.NET
- EMBEDDED LINUX
- Z-MODEM

KUNDENBEDÜRFNIS

Zur Überprüfung elektronischer Selbstschutzsysteme auf Flugzeugen und Helikoptern entwickelte die RUAG Aerospace den „missim“ Simulator. Dieser simuliert spezifische Bedrohungen (Laser, Missiles und Radar). Für die Programmierung des Simulators benötigte die RUAG eine Software mit einer benutzerfreundlichen und übersichtlichen Bedienoberfläche.

LÖSUNG

ibw ag entwickelte für die Programmierung des „missim“ Simulators eine PC Applikation auf .NET Basis. Die diversen Bedrohungsarten werden in Explorerform verwaltet. Zusätzlich überprüft die Software alle Eingaben und unterstützt mehrere verschiedene „missim“ Modelle. Die Software erlaubt zudem, über RS-232 und USB, die kundenspezifisch erstellten Programmierungen zum Simulator zu transferieren. Für Unterhaltszwecke kann über eine Konsole direkt mit dem Simulator kommuniziert werden.

## FUNKTIONALITÄT

### Programmierung

Der Simulator kann (momentan) mit 3 verschiedenen Modulen bestückt werden (Laser, Missile und Radar). Das Programmiertool erlaubt auf einfache Art und Weise das Aufsetzen fast beliebiger kundenspezifischer „Emitter“. Diese werden anschliessend auf den verschiedenen Modulen abgespielt.



### Erstellen von Sequenzen

Das Kernstück der Programmierung ist der Sequenzdialog, in welchem die Emitter einem Drehbuch ähnlich angeordnet werden. Die verfügbaren kundenspezifischen Emitter (Laser, Missile und Radar) werden in Listen eingebunden und mit zusätzlichen Parametern ergänzt, die später auf dem „missim“ Simulator verarbeitet werden.

### Validieren der Daten

Die programmierten Emitter und erstellten Sequenzen werden laufend auf die technische Simulationsfähigkeit überprüft. Als Grundlage dient ein hardware-spezifisches Konfigurationsfile, welches vom „missim“ Simulator ausgelesen wird. Das Programmiertool markiert allfällige Über- oder Unterschreitungen der vom Anwender programmierten Werte. Wenn die Validierung erfolgreich war, kann ein Threat Library Set (TLS) erstellt und auf den „missim“ Simulator übertragen werden.

## KOMMUNIKATION

Gültige Threat Library Sets (TLS) können über RS-232 oder USB zum Simulator gesendet werden. Bevor dies geschieht, wird ein TLS sicherheitshalber vorgängig mit dem hardware-spezifischen Konfigurationsfile verglichen.

## UNTERHALT

Der „missim“ Simulator basiert auf einem Linux Betriebssystem. Damit die Wartung des Gerätes ebenfalls über das Programmiertool geschehen kann, wurde ein zusätzlicher Betriebsmode eingebaut, in welchem über eine Konsole direkt mit der Hardware kommuniziert werden kann.

