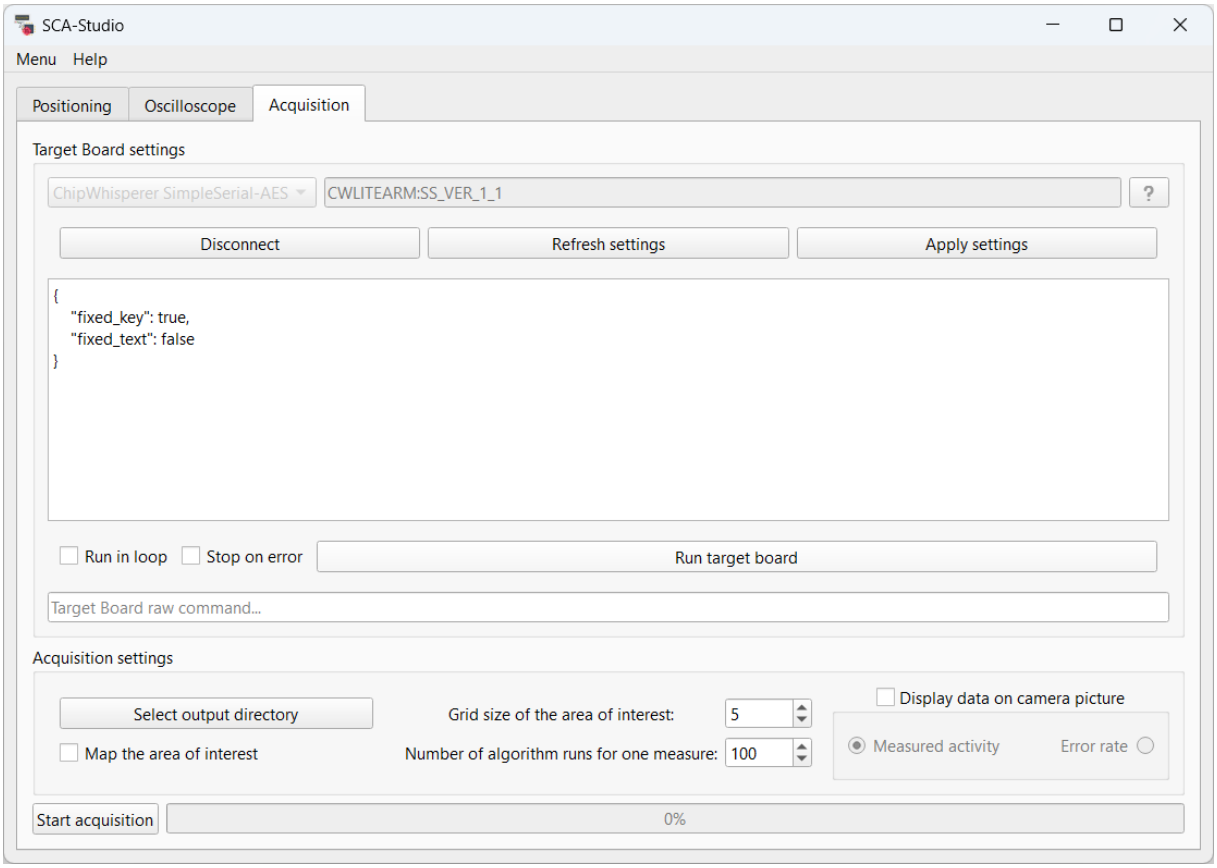
SCA-STUDIO : Acquisition



L'onglet « Acquisition » permet de se connecter et de configurer une carte cible, et d'effectuer des mesures automatiques avec l'ensemble des autres appareils.

Target Board settings

Device : sélection du type de carte cible utilisée

Address : champ de texte permettant d'indiquer l'adresse de la carte cible utilisée et d'autres éventuels paramètres de connexion

❓ : bouton d'aide fournissant des informations complémentaires sur la carte cible sélectionnée, dont le format d'adresse attendu

Connect / Disconnect : bouton de connexion et de déconnexion d'une carte cible

Refresh settings : actualise la configuration de la carte cible

Apply settings : applique la configuration à la carte cible

Zone de texte : configuration de la carte cible, qui peut être modifiée directement dans ce champ

Run in loop : lors du lancement, si cette case est cochée, l'algorithme sera lancé en boucle

Stop on error : lors du lancement, si cette case est cochée, l'algorithme s'arrêtera si une injection de faute est détectée

Run target board / stop target board : lance ou stoppe l'algorithme de la carte cible.

« *Oscilloscope raw command…* » : envoie des commandes textuelles choisies par l'utilisateur à l'oscilloscope. Une commande se valide par la touche « entrée ». Un message s'affiche pour indiquer la réponse de l'oscilloscope.

Acquisition settings

Select output directory : sélectionne le dossier dans lequel enregistrer les mesures

Map the area of interest : si coché, l'acquisition se déplacera sur le quadrillage défini dans l'onglet « Positioning ». Sinon, l'acquisition portera sur le point actuel.

Grid size of the area of interest : nombre de cases dans la grille de la zone d'intérêt

Number of algorithm runs for one measure : nombre de mesures effectuées pour chaque point lors de l'acquisition automatique

Display data on camera picture : si coché, traite les données enregistrées dans le dossier sélectionné, pour afficher l'intensité moyenne (centrée et en valeur absolue), ou le taux de fautes détectées, en chaque point sur la vue de la caméra de l'onglet « Positioning »

Start acquisition

Démarre l'acquisition en fonction des paramètres définis. Il est nécessaire que tous les appareils soient connectés et que l'algorithme de la carte cible ne soit pas déjà lancé. Il n'est plus possible d'interagir avec les appareils.

La barre de progression augmente avec l'avancement de l'acquisition. La position du système de positionnement est mise à jour sur la vue de la caméra de l'onglet « Positioning ».

Le bouton « *Stop acquisition* » permet de stopper l'acquisition.

Les données d'une acquisition sont enregistrées selon les coordonnées du système de positionnement à chaque point, avec une mesure par ligne, dans les fichiers suivants du dossier sélectionné :

- « x_y.measures.txt » : données retournées par l'oscilloscope
- « x_y.errors.txt » : nombre de fautes détectées
- « x_y.info.txt » : informations supplémentaires sur chaque mesure

Cartes cibles supportées

Nucleo

Permet d'interagir avec une carte de test. Cette carte communique en serial, reçoit en entrée un entier N codé sur 2 octets, et retourne le nombre de fautes détectées sur 2 octets. L'algorithme effectue N opérations de chiffrement avec une clé et un message fixes, et compare le résultat obtenu avec le résultat attendu.

- L'adresse doit spécifier le *port* et le *baudrate*. Le *port* peut se trouver dans le gestionnaire de périphériques de l'ordinateur.
  Par exemple : « *COM*3:9600 »
- Les paramètres de cette carte permettent d'ajuster l'entier N, indiquant à la carte le nombre d'opérations de chiffrement qu'elle doit effectuer à la suite
- Cette carte peut détecter l'injection de fautes, mais ne donne aucune autre information particulière sur les opérations de chiffrement
- Il est possible d'envoyer directement des commandes personnalisées à ce type de carte, bien que cela ne permette pas d'avoir accès à d'autres fonctionnalités avec le firmware de test tel quel

ChipWhisperer SimpleSerial-AES

Permet d'interagir avec une carte ChipWhisperer et le firmware de démonstration *simpleserial-aes*. Cet appareil a été testé avec un ChipWhisperer Lite STM32.

- L'adresse doit spécifier la plateforme et la version de *SimpleSerial*. Par exemple : « CWLITEARM:SS_VER_1_1 »
- Les paramètres permettent de régler le comportement de la génération de clés et de messages : ceux-ci peuvent être fixés ou variables. La génération suit la fonctionnalité « Basic Key Text Pattern » inclue avec les outils de ChipWhisperer.
- Cette carte ne détecte pas les potentielles fautes injectées. Les fichiers « .errors.txt » contiendront toujours « 0 ». Les fichiers « .info.txt » sont au format « {clé} {message en clair} {message chiffré} », où chaque information est encodée en hexadécimal.
- Il n'est pas possible d'envoyer directement des commandes personnalisées à ce type de carte