Secure Auto Programming System の概要

近年の ICT（情報通信技術）の飛躍的な進展、インフラの発達により引き起こされました
グローバル化の波により、生産のファブレス化が急速に進みました。
集中生産によるコストダウンの恩恵を受け、既に、求め易い価格で高機能な商品で満たされた
世の中が、訪れております。

今後更に、IoT、Smart Factory、AI の進化等により、多種多様でより斬新な製品が生み出され、
ファブレス化は、更なる進展を遂げると考えます。しかし一方で、
ファブレス化によって引き起こされてしまう、ファブレス化の脆弱性が問題視されております。
特に問題視されているものは、下記 2 点となります。

【問題点】
1．企業間でのデータ授受に伴う、Firmware 等の知的財産(IP)の盗難、流出
2．複製品の製造、流出、オリジナル製品の過剰生産等

★ファルコン電子ではこれらの脆弱性を、Secure Programming にて解決致します。

【Secure Programming による解決策】
1．Secure な Firmware の流通経路を担保
社内開発、OEM,ODM にかかわらず、開発段階から書込みまで、
Firmware の暗号化を徹底して行います。
これにより、Firmware 等の知的財産の盗難、流出を徹底的に防止致します。
2．IC 書込み数の管理
商品開発者により指定された IC 書込み数を絶対的な値として、
商品開発者が商品生産者での IC 書込み数を徹底的に管理致します。

Secure Programming とは、Secure Provisioning によって実現された、Secure な環境下にて、
IC の Programming を行うことを示します。
Secure Provisioning には、Secure な環境を担保する為に、HSM(Hardware Security Module)を
導入し活用しております。
故に、Secure な環境を実現する為に行われる、鍵生成、電子署名、証明書発行、認証、
暗号化、復号等の各処理は、より一層堅牢なものとなります。
また、Secure Programming により行われました、Provisioning、IC Programming 等の一連動作は、
ログに記録されます。従いまして、お客様は Secure Programming が行われた全ての IC の、
設計段階から書込みまでの Traceability を、一貫して管理することが可能となります。