TruLink Control Logic Module CL6882-M1
Non-Proprietary Security Policy

Document No.: 93858
Revision: 3.3
Date: March 16, 2022

Prepared By:
TELEPHONICS CORPORATION
815 Broad Hollow Road
Farmingdale, New York 11735

REVISION HISTORY

Rev	Description	Date
Internal Release, Version 2.5	TruLink Control Logic Module CL68820M1 Security Policy Telephonics Sweden Document Version 2.5 – Internal Release	July 1, 2013
3.0	Updated for format and clarity	July 01 2021
3.1	Added hardware configuration to Section 1. Module Overview Updated algorithm certificate numbers in Section 2.1 Added additional information to Table 5.2	August 03 2021
3.2	Corrected proprietary notice on title page	September 8, 2021
3.3	Updated Section 1 to include processor information	March 16, 2022

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

SECTION 1

1. MODULE OVERVIEW

The TruLink Control Logic Module CL6882-M1 (P/N 010.6882-01 Rev. B2 FW Versions Boot: SW7158 v2.5 and Application: SW7151 v2.13) (CL6882) is a hardware multi-chip embedded module as defined by Federal Information Processing Standard (FIPS) 140-2.

The CL6882's cryptographic boundary is defined as the entire CL6882 module (see red outline in Figure 1-1). It is comprised entirely of production grade components. It is the central component supporting TruLink's secure versatile wireless communication system. The TruLink Control Logic Module is designed to be embedded in the Enhanced Mobile Equipment and Integrated Aircraft Interface Unit transceivers and to operate in a variety of critical situations and extreme environments.

The TruLink Control Logic Module contains two processors, one a general-purpose processor (ATMEL AT91R40008-66AU) and the other, a digital signal processor (Analog Devices ADSP2187) used for more intensive numeric computation. The TruLink system requires timing constraints to allow for uninterrupted audio transmissions. It also requires power constraints to allow for a long run time from the internal battery packs. Sharing the processing load between the two low power processors, with each specializing in their own processing capabilities, allows for speed in execution and power efficiency.

The general-purpose processor is the system scheduler and runs the main program loop to address all of the functions of the TruLink system, including firmware load. When required, it fires off requests to the DSP to provide high speed, numeric intensive functions such as AES, or audio processing algorithms such as adaptive noise reduction (amongst others).

The TruLink system is a full-duplex system that provides conversational speech capability, which enables multiple users to speak simultaneously. Unlike conventional "walkie-talkies", TruLink users can converse among themselves via a voice activation (VOX) function without the need to press a Push-to-Talk (PTT) button or waiting for another user to finish their transmission. A PTT function is provided however, to complement the VOX feature for desired or operational requirements.

Depending on the system configuration:

1. The system supports 50 (0-49) or 100 (0-99) channels.

2. Up to 31 users can be logged onto a channel which functions as an independent network.

A TruLink network is composed of one TruLink unit designated as the “master” and all other TruLink units operating as “slaves”. The master in the system acts as the central controller which handles network separation and routing of all user traffic.

Although the system’s central purpose is voice transmission, it also supports the wireless transmission of bulk user data over the same system. This enables the TruLink system to address a wide range of user needs.

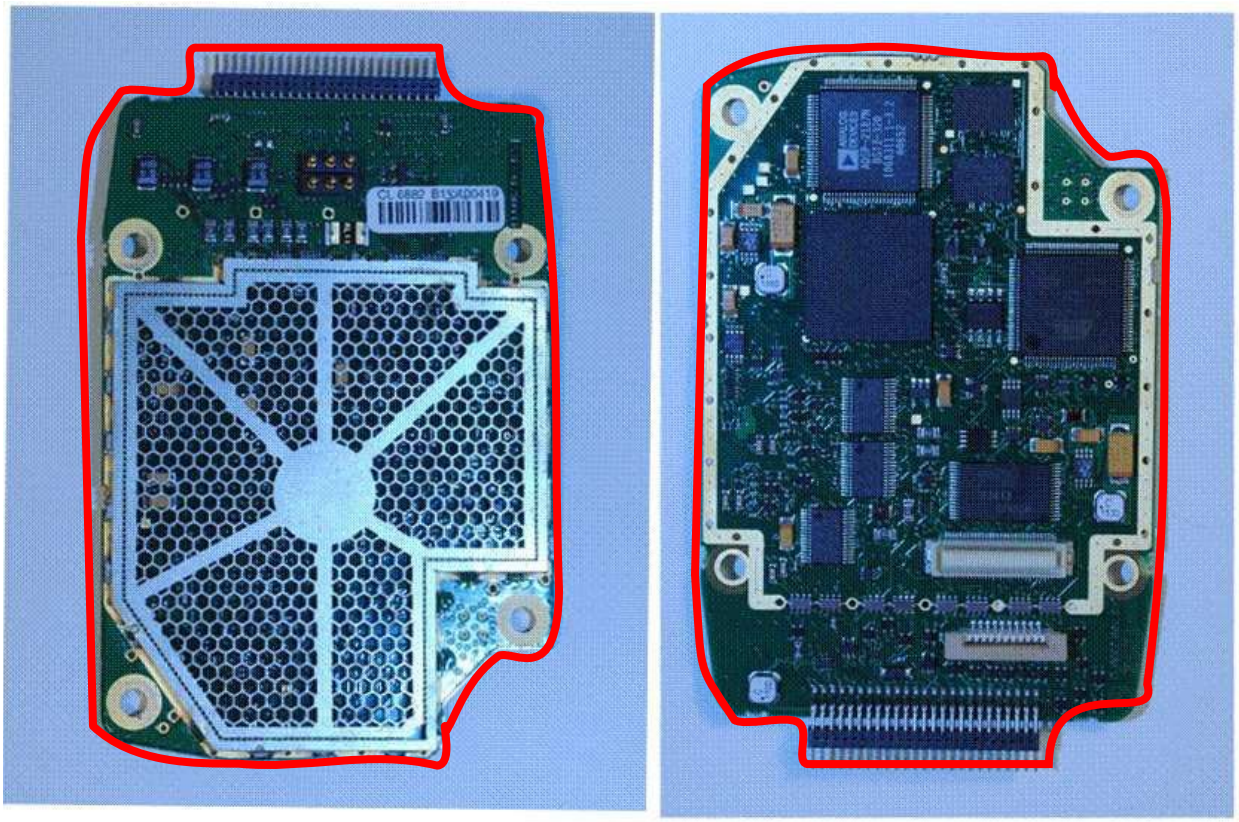

Figure 1-1. TruLink Control Logic Module CL6882-M1 (Image of Control Logic (CL) Board)

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Table 1-1. Module Security Level Specification

FIPS Security Requirements Section	Level
Cryptographic Module Specification	1
Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A

FIPS Security Requirements Section	Level
Cryptographic Key Management	1
EMI/EMC	1
Self-Test	1
Design Assurance	1
Mitigation of Other Attacks	N/A

SECTION 2

2. MODES OF OPERATION

2.1 FIPS APPROVED MODE OF OPERATION

In FIPS mode, the cryptographic module only supports the following FIPS Approved algorithms:

- AES 128, 256 ECB (Cert. #C1794)
- HMAC-SHA-1 (Cert. #C1793)
- SHA-1 (Cert. #C1793)

The module can only enter FIPS mode after authenticated (signed) firmware has been successfully loaded via the HMAC-SHA-1 firmware load operation.

SECTION 3

3. PORTS AND INTERFACES

The CL6882 module provides the following physical ports and logical interfaces:

Table 3-1. Ports and Interfaces

Physical Port	Qty	Logical interface definition	Description
50 PIN Port	1	• Power input • Status Output • Control Input • Data Input • Data Output	The main physical port provided by the module. It provides access to the majority of the supported interfaces.
Key Flex Port	1	• Control Input • Status Output	This interface provides the input and output to a key pad and LED. The LED and Key Pad are not included within the crypto boundary.
TR Port	1	• Data Input • Data Output	This is the transceiver port which provides the input and output accessed by an attached radio interface. The radio interface is not included within the crypto boundary.
Battery (Power) Port	1	• Power Input • Status Input • Control Input	Provides power and status from an external battery. It also provides control Input while the module is in a battery charging state.

SECTION 4

4. IDENTIFICATION AND AUTHENTICATION POLICY

4.1 ASSUMPTION OF ROLES

The module supports the FIPS required roles of Crypto-Officer and User as well as an Application User. The Operators of the module are not required to authenticate as this is a Level 1 module.

Table 4.1-1. Roles and Required Identification and Authentication

Role	Type of Authentication	Description
Crypto-Officer	No Authentication is provided and/or required at Level 1.	Administrator of the module, with full access to configurations. This role is assumed when an operator accesses the module using a GPC.
User	No Authentication is provided and/or required at Level 1.	The “day-to-day” user of the module, with limited access to services provided by the module. This role is assumed when an operator uses the physical radio in which this module is installed.
Application User	No Authentication is provided and/or required at Level 1.	A full access user, allowing access via the application programming interface (API). This role is assumed when an operator accesses the module using a GPC, over the RS-232 interface and in data mode. This gives the user of the external application access to a part of the system configuration and also to the functions granted to the Crypto-Officer.

SECTION 5

5. ACCESS CONTROL POLICY

5.1 ROLES AND SERVICES

Table 5.1-1 defines the supported roles and supported services.

Table 5.1-1. FIPS Approved Mode Services Authorized for Roles

Crypto-Officer	User	Application User	Authorized Services	Description
x	x	x	Unit Configuration	Module functional configuration service. Provides a very limited part of configurable parameters for the module.
x	x	x	Data Transmit and Receive	Transmit or Receive data either encrypted or in plaintext.
x	x	x	Bypass	Enable or Disable encryption
x	x	x	Status Output	Receive Status Output
x	x	x	Clear AES KEY	To erase the stored AES Key
x		x	Zeroize	Actively write over all plaintext CSPs.
x		x	Key Entry and Output	Manually Enter or Output the Traffic Encryption Key(TEK)
x		x	Load Firmware	Load external firmware
		x	Application Services	Application specific configuration service (via an API). Provides access to part of the configurable parameters and the behavior for the module. This can't affect the crypto functionality except for key handling. Full access is limited to Telephonics Corporation.

5.2 DEFINITION OF CRITICAL SECURITY PARAMETERS (CSPs)

The following Critical Security Parameters (CSP) are contained within the module:

Table 5.2-1. Critical Security Parameters

Key	Description/Usage	Generation	Storage	Entry	Output	Zeroization
Traffic Encryption Key (TEK)	This is an AES 128 bit key or AES 256 bit key used to encrypt and decrypt user data within the system.	N/A (Externally)	Plaintext	Manual distribution (establishment) with electronic entry (input) in plaintext, as allowed by FIPS 140-2 IG 7.7	Manual distribution (establishment) with electronic entry (input) in plaintext, as allowed by FIPS 140-2 IG 7.7	Zeroize Service
Soft/Firmware Authentication Key	A 64-bit HMAC SHA-1 key which is used to authenticate externally loaded software/firmware.	N/A (Externally)	Plaintext	During Manufacturing	N/A	Zeroize Service

5.3 PUBLIC KEYS

The module does not employ the use of public keys.

5.4 DEFINITION OF CRITICAL SECURITY PARAMETERS MODES OF ACCESS

The implemented key establishment method is manual. Keys are entered in plaintext via a direct connection with a key loading device or via the RS232 interface with a GPC and a terminal application.

Table 5.4-1 defines the relationship between access to CSPs and the different module services.

Table 5.4-1. Critical Security Parameters Access Rights within Roles and Services

CSP	Unit/System Configuration	Data Transmit and Receive	Status Output	Key Entry and Output	Clear AES Key	Application Services	Zeroize	Load Firmware
TEK	--	E	--	WZ	E	RWEZ	Z	--
Soft/Firmware Authentication Key	--	E	--	--	--	--	Z	E

The modes of access shown in the table are defined as follows:

- (R) Read: The data item is read from memory
- (E) Execute: Utilize the key within an approved security function
- (W) Write: The data item is written into memory
- (Z) Zeroize: The data item is actively overwritten

SECTION 6

6. OPERATIONAL ENVIRONMENT

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the device does not contain a modifiable operational environment.

SECTION 7

7. SECURITY RULES

The cryptographic module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

1. The cryptographic module shall provide three (3) distinct operator roles. These are the User role, Crypto-Officer role, and Application User role.
2. When the cryptographic module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
3. The cryptographic module shall encrypt message traffic using the AES-128 or 256 ECB algorithm.
4. The cryptographic module shall perform the following tests:

   A. Power up Self-Tests:

      1. Cryptographic algorithm tests:

         a. AES ECB Known Answer Test (AES KAT Encrypt/Decrypt)

         b. HMAC-SHA-1 Known Answer Test. (SHA-1 KAT)

      2. Firmware Integrity Test (16 bit Checksum)

   B. Conditional Self-Tests:

      1. Bypass test: Ensures proper application of encryption to data after a switch has been made from clear text transmit and receive to encrypted transmit and receive.

      2. Manual key entry test: Duplicate entry

      3. Firmware Load Test: (Boot FW and Application FW): HMAC-SHA-1

5. At any time an operator can power cycle the module to initiate self-tests.
6. Data output shall be inhibited during self-tests, zeroization, and error states.
7. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

8. The operator is made aware of self-test errors via the Key Flex Port status output interface.

9. The operator is made aware of the bypass state via the 50 Pin Port status output interface.

10. The module supports exclusive bypass as defined by FIPS 140-2.

11. The module does not support concurrent operators.

12. Procedural controls shall be in place to ensure initial control and access of the module.

    1. The Crypto-Officer and Application User shall use the Key Entry and Output service using manual distribution/electronic entry per FIPS 140-2 IG7.7 (i.e., the Crypto-Officer or Application User must be directly connected to the module when entering/outputting keys).

    2. The Crypto-Officer and Application User shall use a Telephonics Corporation provided RNG or another Approved RNG when using the Key Entry service.

SECTION 8

8. PHYSICAL SECURITY POLICY

8.1 PHYSICAL SECURITY MECHANISMS

The module employs production grade components which meet FIPS 140-2 Level 1 requirements.

SECTION 9

9. MITIGATION OF OTHER ATTACKS POLICY

The module has not been designed to mitigate against other attacks, outside of the scope of FIPS 140-2 Level 1 requirements.

SECTION 10

10. DEFINITIONS AND ACRONYMS

AES – Advanced Encryption Standard

CSP – Critical Security Parameters

ECB – Electronic Code Book

GPC – General Purpose Computer

FIPS – Federal Information Processing Standard

HMAC – Hash Message Authentication Code

KAT – Known Answer Test

PTT – Push To Talk

SHA – Secure Hash Algorithm

TEK – Traffic Encryption Key

VOX – Voice Activation Transmission