Tait P25 products

Encryption Key Loading Guide

MTA-00004-02
Issue 2
September 2006

Tait Contact Information

Tait Radio Communications
Corporate Head Office

Tait Electronics Limited
P.O. Box 1645
Christchurch
New Zealand

For the address and telephone number of regional offices, refer to the TaitWorld website:

Website: http://www.taitworld.com

Technical Support

For assistance with specific technical issues, contact Technical Support:

E-mail: support@taitworld.com
Website: http://support.taitworld.com

Tait Electronics Limited is an environmentally responsible company which supports waste minimization and material recovery. The European Union's Waste Electrical and Electronic Equipment Directive requires that this product be disposed of separately from the general waste stream when its service life is over. Please be environmentally responsible and dispose through the original supplier, your local municipal waste "separate collection" service, or contact Tait Electronics Limited.

Contents

Introduction

The encryption and decryption of radio voice communications requires the use of encryption keys. Tait mobiles and portables provide a standard P25 key-fill interface for the loading of encryption keys. Currently, Tait recommends using the Motorola KVL3000+ key fill device for this task. First you enter into the KVL3000+ the encryption keys required, and then you connect the KVL3000+ to each radio in turn, loading one or more keys into it. If your system has P25 Console Gateways, they must also be supplied with encryption keys, as they are an encryption and decryption point.

This guide gives an overview of encryption and supplements the KVL3000+ documentation with information on how to use the KVL3000+ with Tait equipment.

For instructions on how to use the KVL3000+, see the KVL3000+ User's Guide.

Equipment Required

- Motorola KVL3000+ key fill device with the following:
    - battery
    - charger
    - user's guide
    - option for ASTRO P25 mode
    - option for ASN mode (required for operation in ASTRO P25 mode)
    - option for DES/DES-XL/DES-OFB encryption.
    - option for AES encryption (if you plan to use AES encryption)
- Tait 9000 series to KVL3000+ adapter (TPA-SV-020). This includes a cable for connecting to the KVL3000+.
- Cabling for connecting the adapter to the radio.

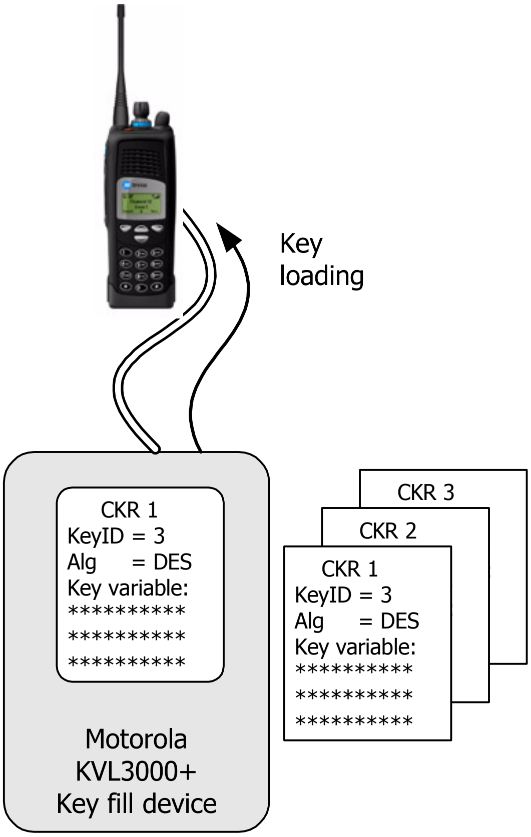
Note Tait TM9100/TP9100 radios and P25 Console Gateways require the Base encryption feature license. This license enables P25-compliant DES encryption. With mobiles and portables you must obtain the license before loading encryption keys. An additional license is required to enable AES encryption.

Encryption Overview

When you enter a key into the KVL3000+, you need to specify a Common Key Reference (CKR). This is the reference number for a set of secure key data.

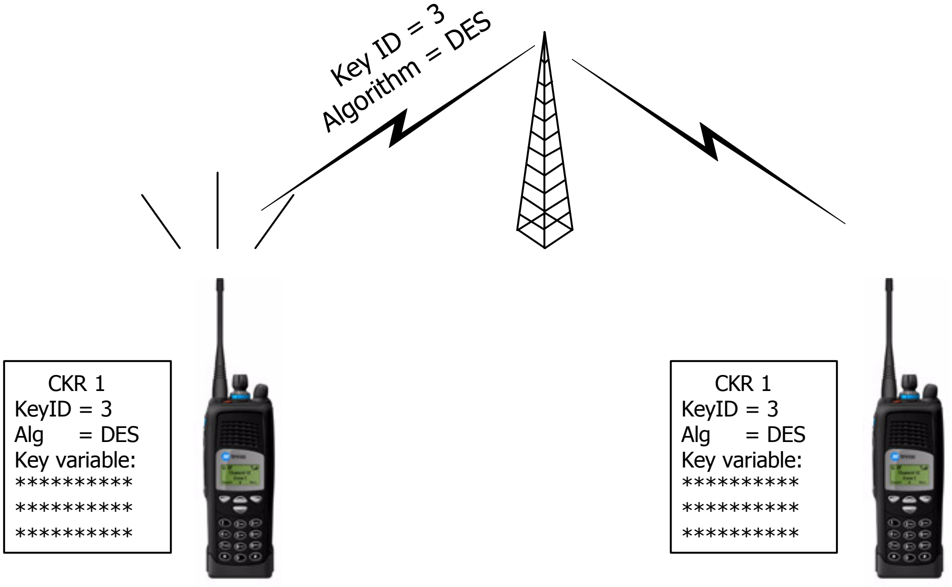
This key data consists of the following information:

- Key ID, used to identify the key over the air to the device decrypting the call.
- Algorithm ID, which specifies which encryption algorithm is to be used (DES-OFB or AES).
- Key variable, a multi-digit number that the crypto-module uses when encrypting and decrypting.



In addition, the Tait TM9000/TP9000 programming software (for mobiles and portables) or Customer Service Software (for the P25 Console Gateway) gives each CKR a name. Only the CKR is visible to the software.

When a radio makes an encrypted call, it includes in the call the Key ID and the Algorithm ID that it used. If the receiving radio has the same key, it can decrypt the call. The Key ID that it received tells it what key to use and the Algorithm ID tells it the encryption algorithm to use.



Entering Encryption Keys

Note Before encryption keys are entered, your organization should have developed a policy and procedures for encryption key management. This will answer questions such as "How many keys will be needed?" "How will re-keying occur?" and "How and when will users change from one key to another?"

Enter into the KVL3000+ all the keys that your system will need, following the instructions for ASTRO 25 operation in the KVL3000+ User's Guide.

Important Make sure that you follow your organization's security policy when handling keys. If encryption information falls into unauthorized hands, the security of voice communications could be compromised.

- The CKR can be any number from 1 to 4095. For example, if all radios will use the same keys, you can use 1–16 as the CKR numbers. If you need two groups of keys, use 1–16 for the first group and 17-32 for the second group.
- The Key ID can be any hexadecimal number 0–FFFF.
- For DES encryption, you must select DES-OFB. OFB (Output Feedback mode) is the only DES mode specified by the P25 common air interface.
- For DES encryption, the key variable is an 8-octet number, for example 01 23 45 67 89 AB CD EF. An octet is two hexadecimal

numbers. Each octet must have odd parity (an odd number of 1s in the binary number).

- For AES encryption, enter a key variable of the required length. There are no parity restrictions. For example, enter 32 octets for AES 256.

Important Once you have entered a key variable into the KVL3000+, you can no longer view it.

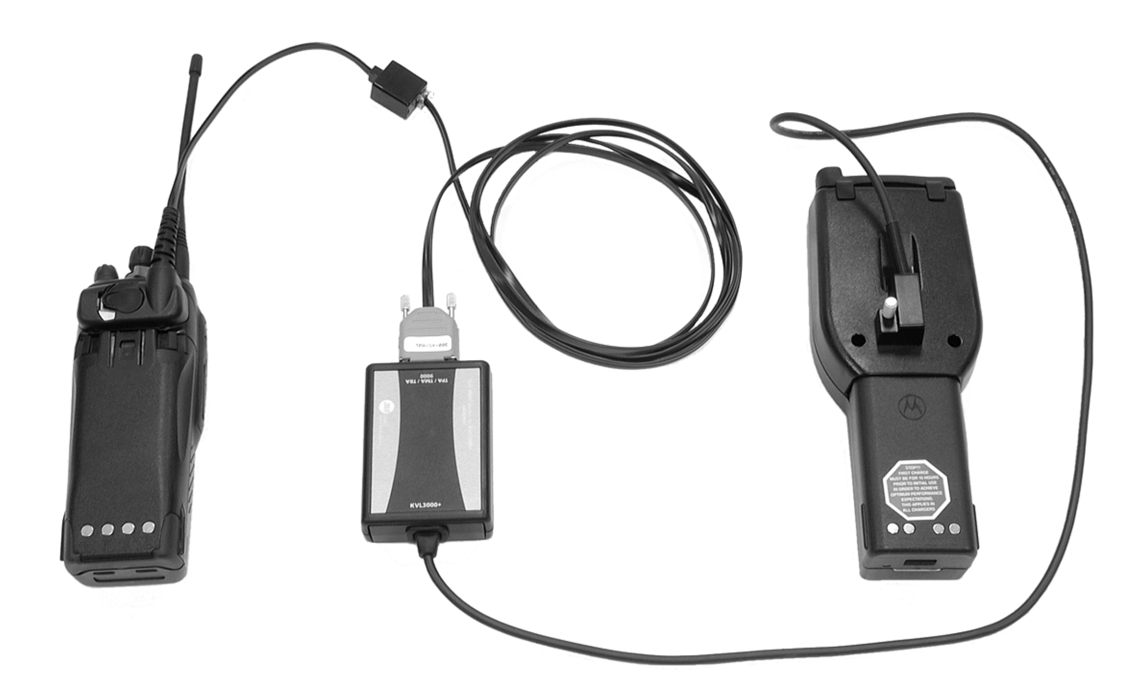
The KVL3000+ also lets you group keys into key groups for easier loading or zeroize keys you no longer want to use.

Connecting the KVL3000+ to the Target Device

1. Connect the cable attached to the Tait adapter to the keyload port on the back of the KVL3000+. (This cable provides power from the KVL3000+ to the adapter.)

2. Connect the other end of the adapter to the target device using the appropriate cabling.
   - For a TM9100 mobile, connect a TPA-SV-006 programming lead (9-pin to RJ12) to the programming (microphone) port.
   - For a TP9100 portable, you need the above programming lead and a TPA-SV-007 cable (RJ12 to TPA) as well.
   - For a P25 Console Gateway, connect an ordinary DB9 to DB9 extension cable to the connector marked DIG at the rear of the gateway module.

Figure 1 Connecting the KVL3000+ to a TP9100 Portable



Loading Keys

1. With Tait mobiles and portables, wait for the display ‘Keyloading mode.’ With P25 Console Gateways, wait for the control panel LEDs to all go on.

2. Following the instructions in the KVL3000+ user’s guide, load the desired keys into the target device. Tait P25 equipment can store up to 16 keys. You can use the KVL3000+ to load a single key, a key group, or all the keys it has.

3. When you are finished, disconnect the adapter. This takes mobiles and portables out of Keyloading mode. If the target device is a P25 Console Gateway, it automatically resets.

Supported KVL3000+ Tasks

The following table indicates which KVL3000+ tasks can be carried out on Tait target devices. These tasks must be carried out in ASTRO P25 mode. (The KVL3000+ has two operational modes, ASTRO P25 and ASN. Only ASTRO P25 mode applies to Tait equipment.)

KVL3000+ Task	Supported by Tait Equipment?
Load a key	Yes
Load a group of keys	Yes
Load all keys	Yes
Zeroize a keys	Yes
Zeroize a group of keys	Yes
Zeroize all keys	Yes
View keys[a]	Yes
View/Load OTAR parameters	No
Change Keyset[b]	No
Store and forward keys that have been downloaded from a Key Management Facility	No

[a] This task can only display information about loaded keys, not the key variables themselves.

[b] Tait equipment operates with a single keyset

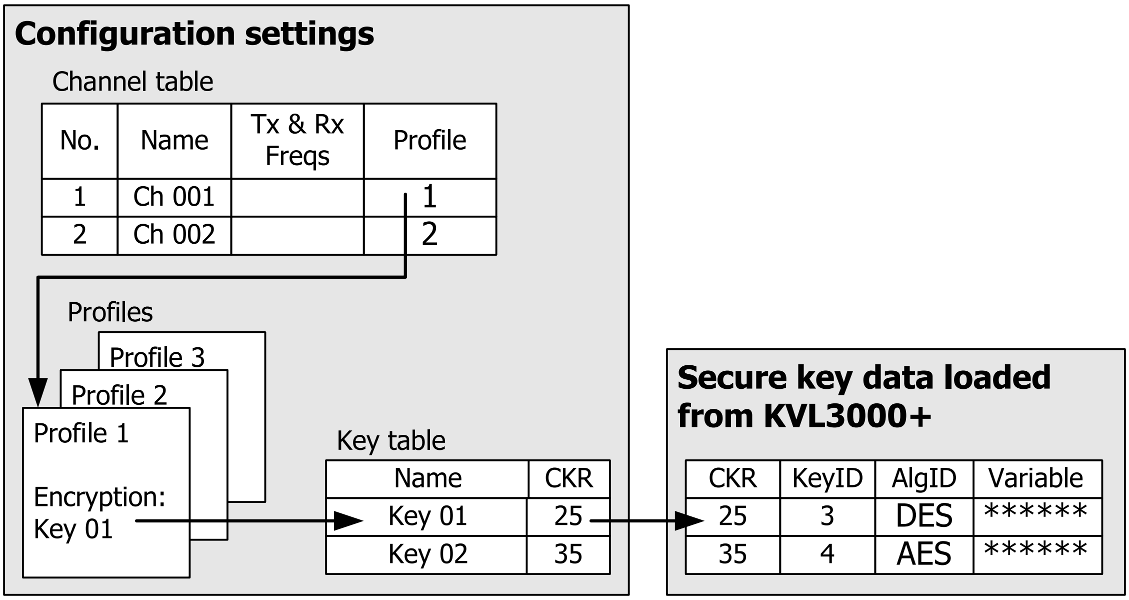
Configuring Encryption Operation

In addition to loading secure key data into the Tait P25 equipment, you need to configure the way the equipment uses these keys. Configuration settings refer to keys by name, so before you can select a key, you must give it a name.

Because the secure key data is invisible, you have to name keys by mapping a name to a CKR number. This is done in a Keys table. You add a row for each key and ensure that each row contains a suitable name and CKR.

Once you have a set of named keys, you can choose which one to assign to each channel profile (mobiles and portables) or calling profile (P25 Console Gateway) that supports encryption.

When the equipment encrypts a call, its default operation is to look in the current profile for the key name, and then to read the CKR number corresponding to that name. The CKR number tells it where to go in the secure key data storage area to obtain the encryption key data it needs.



Configuration settings

Channel table

No.	Name	Tx & Rx Freqs	Profile
1	Ch 001		1
2	Ch 002		2

Profiles

Profile 3

Profile 2

Profile 1

Encryption:
Key 01

Key table

Name	CKR
Key 01	25
Key 02	35

Secure key data loaded from KVL3000+

CKR	KeyID	AlgID	Variable
25	3	DES	******
35	4	AES	******

This indirect way of referring to keys by name makes it possible to update keys without changing the configuration. You simply use the key fill device to load different secure key data using the same CKR numbers.

Tait General Software Licence Agreement

This legal document is an Agreement between you (the "Licensee") and Tait Electronics Limited ("Tait"). By using any of the Software or Firmware items prior-installed in the related Tait product, included on CD or downloaded from the Tait website, (hereinafter referred to as "the Software or Firmware") you agree to be bound by the terms of this Agreement. If you do not agree to the terms of this Agreement, do not install and use any of the Software or Firmware. If you install and use any of the Software or Firmware that will be deemed to be acceptance of the terms of this licence agreement.

The terms of this Agreement shall apply subject only to any express written terms of agreement to the contrary between Tait and the Licensee.

Licence

TAIT GRANTS TO YOU AS LICENSEE THE NON-EXCLUSIVE RIGHT TO USE THE SOFTWARE OR FIRMWARE ON A SINGLE MACHINE PROVIDED YOU MAY ONLY:

1. COPY THE SOFTWARE OR FIRMWARE INTO ANY MACHINE READABLE OR PRINTED FORM FOR BACKUP PURPOSES IN SUPPORT OF YOUR USE OF THE PROGRAM ON THE SINGLE MACHINE (CERTAIN PROGRAMS, HOWEVER, MAY INCLUDE MECHANISMS TO LIMIT OR INHIBIT COPYING, THEY ARE MARKED "COPY PROTECTED"), PROVIDED THE COPYRIGHT NOTICE MUST BE REPRODUCED AND INCLUDED ON ANY SUCH COPY OF THE SOFTWARE OR FIRMWARE; AND / OR

2. MERGE IT INTO ANOTHER PROGRAM FOR YOUR USE ON THE SINGLE MACHINE (ANY PORTION OF ANY SOFTWARE OR FIRMWARE MERGED INTO ANOTHER PROGRAM WILL CONTINUE TO BE SUBJECT TO THE TERMS AND CONDITIONS OF THIS AGREEMENT).

THE LICENSEE MAY NOT DUPLICATE, MODIFY, REVERSE COMPILE OR REVERSE ASSEMBLE ANY SOFTWARE OR FIRMWARE IN WHOLE OR PART.

Important Notice

THE SOFTWARE OR FIRMWARE MAY CONTAIN OPEN SOURCE SOFTWARE COMPONENTS ("OPEN SOURCE COMPONENTS"). OPEN SOURCE COMPONENTS ARE EXCLUDED FROM THE TERMS OF THIS AGREEMENT EXCEPT AS EXPRESSLY STATED IN THIS AGREEMENT AND ARE COVERED BY THE TERMS OF THEIR RESPECTIVE LICENCES WHICH MAY EXCLUDE OR LIMIT ANY WARRANTY FROM OR LIABILITY OF THE DEVELOPERS AND/OR COPYRIGHT HOLDERS OF THE OPEN SOURCE COMPONENT FOR THE PERFORMANCE OF THOSE OPEN SOURCE COMPONENTS. YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF EACH SUCH LICENCE. FOR MORE INFORMATION SEE: http://support.taitworld.com/go/opensource

Title to Software

THIS AGREEMENT DOES NOT CONSTITUTE A CONTRACT OF SALE IN RELATION TO THE SOFTWARE OR FIRMWARE SUPPLIED TO THE LICENSEE. NOT WITHSTANDING THE LICENSEE MAY OWN THE MAGNETIC OR OTHER PHYSICAL MEDIA ON WHICH THE SOFTWARE OR FIRMWARE WAS ORIGINALLY SUPPLIED, OR HAS SUBSEQUENTLY BEEN RECORDED OR FIXED, IT IS A FUNDAMENTAL TERM OF THIS AGREEMENT THAT AT ALL TIMES TITLE AND OWNERSHIP OF THE SOFTWARE OR FIRMWARE, WHETHER ON THE ORIGINAL MEDIA OR OTHERWISE, SHALL REMAIN VESTED IN TAIT OR THIRD PARTIES WHO HAVE GRANTED LICENCES TO TAIT.

Term and Termination

THIS LICENCE SHALL BE EFFECTIVE UNTIL TERMINATED IN ACCORDANCE WITH THE PROVISIONS OF THIS AGREEMENT. THE LICENSEE MAY TERMINATE THIS LICENCE AT ANY TIME BY DESTROYING ALL COPIES OF THE SOFTWARE OR FIRMWARE AND ASSOCIATED WRITTEN MATERIALS. THIS LICENCE WILL BE TERMINATED AUTOMATICALLY AND WITHOUT NOTICE FROM TAIT IN THE EVENT THAT THE LICENSEE FAILS TO COMPLY WITH ANY TERM OR CONDITION OF THIS AGREEMENT. THE LICENSEE AGREES TO DESTROY ALL COPIES OF THE SOFTWARE OR FIRMWARE AND ASSOCIATED WRITTEN MATERIALS IN THE EVENT OF SUCH TERMINATION.

Limited Warranty

THE SOFTWARE OR FIRMWARE (INCLUDING OPEN SOURCE COMPONENTS) IS SUPPLIED BY TAIT AND ACCEPTED BY THE LICENSEE "AS IS" WITHOUT WARRANTY OF ANY KIND EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT BEING LIMITED TO ANY IMPLIED WARRANTIES AS TO MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE. THE LICENSEE ACKNOWLEDGES THAT THE SOFTWARE OR FIRMWARE (INCLUDING OPEN SOURCE COMPONENTS) IS USED BY IT IN BUSINESS AND ACCORDINGLY TO THE MAXIMUM EXTENT PERMITTED BY LAW NO TERMS OR WARRANTIES WHICH ARE IMPLIED BY LEGISLATION SHALL APPLY TO THIS AGREEMENT. TAIT DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE OR FIRMWARE (INCLUDING OPEN SOURCE COMPONENTS) WILL MEET THE LICENSEE'S REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE OR FIRMWARE (INCLUDING OPEN SOURCE COMPONENTS) WILL BE UNINTERRUPTED OR ERROR FREE.

Exclusion of Liability

IN NO CIRCUMSTANCES SHALL TAIT BE UNDER ANY LIABILITY TO THE LICENSEE, OR ANY OTHER PERSON WHATSOEVER, WHETHER IN TORT (INCLUDING NEGLIGENCE), CONTRACT (EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT), EQUITY, UNDER ANY STATUTE, OR OTHERWISE AT LAW FOR ANY LOSSES OR DAMAGES WHETHER GENERAL, SPECIAL, EXEMPLARY, PUNITIVE, DIRECT, INDIRECT OR CONSEQUENTIAL ARISING OUT OF OR IN CONNECTION WITH ANY USE OR INABILITY OF USING THE SOFTWARE OR FIRMWARE (INCLUDING OPEN SOURCE COMPONENTS).

THE LICENSEE'S SOLE REMEDY AGAINST TAIT WILL BE LIMITED TO BREACH OF CONTRACT AND TAIT'S SOLE AND TOTAL LIABILITY FOR ANY SUCH CLAIM SHALL BE LIMITED AT THE OPTION OF TAIT TO THE REPAIR OR REPLACEMENT OF THE SOFTWARE OR FIRMWARE OR THE REFUND OF THE PURCHASE PRICE OF THE SOFTWARE OR FIRMWARE.

General

THE LICENSEE CONFIRMS THAT IT SHALL COMPLY WITH THE PROVISIONS OF LAW IN RELATION TO THE SOFTWARE OR FIRMWARE.

Law and Jurisdiction

THIS AGREEMENT SHALL BE SUBJECT TO AND CONSTRUED IN ACCORDANCE WITH NEW ZEALAND LAW AND DISPUTES BETWEEN THE PARTIES CONCERNING THE PROVISIONS HEREOF SHALL BE DETERMINED BY THE NEW ZEALAND COURTS OF LAW. PROVIDED HOWEVER TAIT MAY AT ITS ELECTION BRING PROCEEDINGS FOR BREACH OF THE TERMS HEREOF OR FOR THE ENFORCEMENT OF ANY JUDGEMENT IN RELATION TO A BREACH OF THE TERMS HEREOF IN ANY JURISDICTION TAIT CONSIDERS FIT FOR THE PURPOSE OF ENSURING COMPLIANCE WITH THE TERMS HEREOF OR OBTAINING RELIEF FOR BREACH OF THE TERMS HEREOF.

No Dealings

THE LICENSEE MAY NOT SUBLICENSE, ASSIGN OR TRANSFER THE LICENCE OR THE PROGRAM EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT. ANY ATTEMPT OTHERWISE TO SUBLICENSE, ASSIGN OR TRANSFER ANY OF THE RIGHTS, DUTIES OR OBLIGATIONS HEREUNDER IS VOID.

No Other Terms

THE LICENSEE ACKNOWLEDGES THAT IT HAS READ THIS AGREEMENT, UNDERSTANDS IT AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. THE LICENSEE FURTHER AGREES THAT SUBJECT ONLY TO ANY EXPRESS WRITTEN TERMS OF AGREEMENT TO THE CONTRARY BETWEEN TAIT AND THE LICENSEE THIS IS THE COMPLETE AND EXCLUSIVE STATEMENT OF THE AGREEMENT BETWEEN IT AND TAIT IN RELATION TO THE SOFTWARE OR FIRMWARE WHICH SUPERSEDES ANY PROPOSAL OR PRIOR AGREEMENT, ORAL OR WRITTEN AND ANY OTHER COMMUNICATIONS BETWEEN THE LICENSEE AND TAIT RELATING TO THE SOFTWARE OR FIRMWARE.