Research and Development of High Reliability Calibration Software

Jian Xiong [a], Hong Gu [b]

School of Control Science and Engineering, Dalian University of Technology, Dalian, China

[a]cd_xj@163.com, [b]guhong@dlut.edu.cn

Abstract

More and more electronic control functions have been added to vehicles. The number of electronic control unit (ECU) has also been gradually increased. Calibration work is an important part of ECU development. At present, the calibration software on the market follows the ASAP protocol standard. It reads and extracts the text-based A2L file. This A2L file is plaintext, which probably has a serious data security risk in the process of multi-user calibration. This paper presents and designs a calibration system with A2L files encryption and decryption based on 3DES algorithm. ECU calibration experiment results showed that based on the encryption and decryption method effectively ensures the A2L file reliability and security.

Keywords

Calibration; 3DES Encryption Algorithm; Calibration Software; ECU; XCP Protocols; Measurement DAQ.

1. Introduction

With the widespread applications of Electronic Control Unit (ECU) in automobile industry, the degree of automotive electronics is getting higher and higher. Unified calibration system features include calibration and measurement data functions. In order to meet the engineering goal, the electronically controlled diesel engine obtains the competitive fuel economy index and the high reliability requirement under the premise of meeting the strict emission. All the variables in the electronic control software are adjustable. The process of assigning all the variables to the optimized value is called calibration. It can be calibrated to maximize the potential of diesel engines, to achieve the goal of the pursuit. Given the greater flexibility and adjustability, poorly calibrated engine performance is even worse than mechanical pump engines. Relative to the calibration of the gasoline engine, the calibration of the diesel engine is more difficult and more challenging. Diesel compression-ignition combustion parameter is closely related to the injector, turbocharger, and the airway valve mechanism or the like, and the fuel injection only calibration, the calibration work is focused on engine performance and emissions work content development. The calibration of the diesel engine must be synchronized with the development of the combustion system.

Due to the complexity of the electronic control unit, especially the automotive electronic control unit, the complexity of the operating system of the controlled system, such as stability, emissions performance, fuel economy, etc., is required in the measurement system On a variety of interactive performance indicators on the line measurement; Second, many parameters interact with each other. The development of an electronic control system in designing an ECU measurement system is crucial. The relative protocols and is relationship as shown in Figure 1:

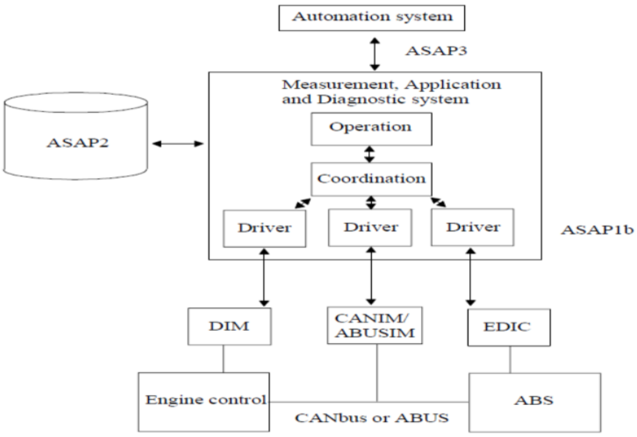


Figure1. Calibration diagram

The calibration of engine electronic control system is an important stage in the application of electronically controlled engine. R & D personnel to calibrate the electronic control system, because of the complexity of the engine control process, and this complexity is embodied in the following aspects: (1) The engine electronic control system needs to achieve a large number of control projects, such as Control start-up, idle speed, speed control and other operating conditions; (2) control of the engine electronic control system so that the full potential of the engine to make power, fuel consumption, emissions and automotive control and other aspects of performance to achieve the best combination of the state ; (3) many factors affect the performance of the engine, a wide range of changes, such as engine load and speed, coolant temperature, intake temperature, fuel temperature, oil temperature, boost pressure, electronic control system for all these factors Changes must make the appropriate adjustments; (4) engine electronic control system must adapt to complex changes in the external environment, such as seasonal changes and changes in altitude and so on.

Paper [1-2] descript the XCP protocol of the calibration software. Paper [3-5] describes the ASAM MCD-2 formats build the data basis of an MCD system. Paper[6] introduces the seed key -algorithm of calibration. Paper[7-10] introduces the development of calibration software.

2. Design overview

From the perspective of control technology, the engine is a dynamic, multivariable and highly nonlinear time-varying system with response lag. Its working process includes very complicated processes of dynamics, thermodynamics, fluid mechanics and chemical reaction kinetics. It is precisely because of the serious non-linear engine system and other reasons; on the one hand, the use of classical linear control theory to control the parameter optimization method has been impossible. On the other hand, the method of calculating the control parameter values obtained by real-time calculation is impossible to meet in the current hardware technology. Therefore, when developing the electronically controlled engine, only a large number of tests can be conducted first, According to certain optimization criteria and relevant laws and regulations, the appropriate optimization methods are adopted for the test data such as power, fuel economy and emission performance under various working conditions. The final control parameters and various correction parameters are calculated according to the engine speed and Load and other factors change the law, and the use of three-dimensional map, two-dimensional curve, etc., according to this law changes in the control parameter values stored in the electronic control unit, the so-called MAP map. In the actual operation of the electronically controlled engine, the electronic control unit performs logic analysis and judgment according to the collected control parameter of the engine operating condition and the stored data, and according to the preset control algorithm, the control to the actuator can be obtained after a simple calculation (Such as fuel injection, injection timing, rail pressure, etc.), so as to achieve the purpose of real-time control of the engine, the so-called look-up table or check the map method.

ECU calibration is a complex system of work, and system development strategy is closely related. In the meantime, different teams are required to be responsible for the calibration of different modules respectively. Different calibration personnel have different authority. However, current standards do not support different teams can modify the calibration of the value of other modules, the reliability of the system calibration data less than adequate assurance.

2.1 Principles of calibration software encryption and decryption

The definition of the ASAM MCD-2MC interface and hence the specification of the ASAM MCD-2MC data base is aimed at defining a database independently of a computer or an operating system in such a way that a transparent and manufacturer-independent standard is established. As exchange format for such ECU descriptions *.a2l files are used.

From the calibration point of view the database in accordance with the ASAM MCD-2MC interface contains the complete description of all control unit relevant data in a project. A project consists of project specific header, which is typically created by the project manager, data and one or more control unit specific descriptions. These control unit descriptions (description of an ECU) include all conversion formulas and explanations about the applicable (adjustable) and measurable (non-adjustable) quantities and present a format description of the interface specific parameters. The measurement and calibration system needs only to evaluate the quantities (and their conversion etc.), but not the interface specific parameters. The latter are only passed on to the structures of the driver.

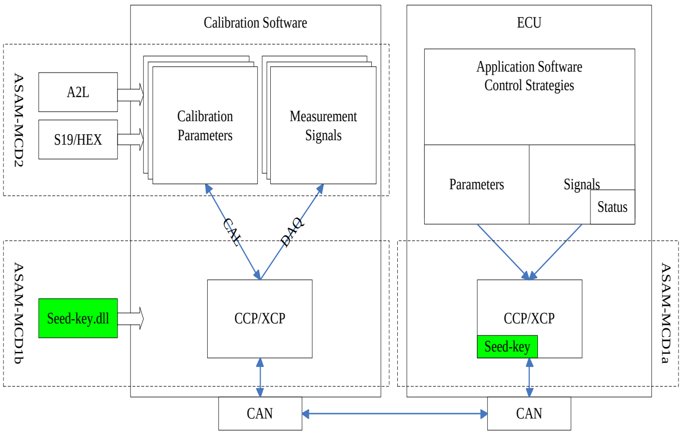


Figure2 Traditional calibration and its security

The ASAM MCD-2MC database thus consists of a number of different subcomponents structured in accordance with the following diagram. The MODULE keyword denotes an independent ECU or device. ASAM MCD-2D ODX in its versions since 2.0 is a unique, open XML exchange format for diagnostics data. The seamless data exchange between different partners along the process chain (suppliers, OEMs or service partners) is a very important process improvement. Diagnostic tools like service testers or more development oriented tools can be parameterized via this format. The ODX standard defines an object-oriented data model, which is described in UML (Unified Modeling language). Inheritance and associations help to avoid data redundancies. In contrast to the ASAM MCD-2MC standard, ODX data describe the parameters and access information for a diagnostic service oriented ECU access.

2.2 SEED-&- KEY

With serial application at the beginning the access to the ECU might be locked. Then, after initialization, the ECU should be unlocked to make further communication possible. For this purpose a Seed-&Key procedure is used. To make it possible to unlock the ECU, the ECU first transfers a random number (the SEED) to the application system. The application system uses the SEED in an algorithm and sends the result (the KEY) back to the ECU. The ECU also uses the SEED in the same algorithm and calculates an ECU-internal result. The results calculated by INCA and by the ECU are compared. If both match, the ECU is unlocked and access is granted. The explanation below is limited to the use of the calibration software that we development in this paper.

1).Procedure to unlock the ECU

The application system requests the SEED. An Access Mode is transferred. The ECU generates the SEED (random number) and sends it to the application system. The application system calculates a KEY and sends it to the ECU. This action is the request to unlock the ECU.- The ECU also calculates a KEY and compares it with the KEY received from the application system. If both match, the ECU sends a positive response to the application system. Otherwise it sends a negative response with a reason for the refusal.

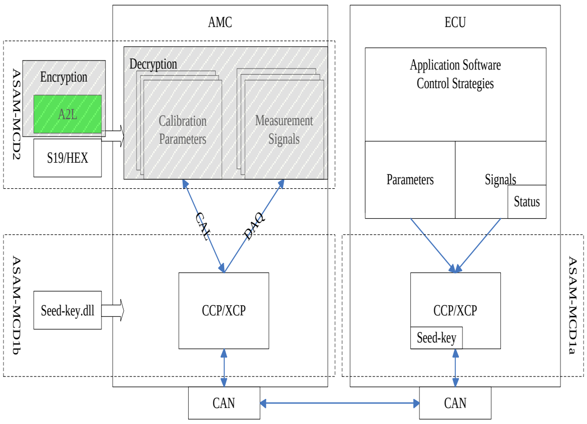
2).SEED-&-KEY with the calibration software

The algorithm that is necessary for calculating the KEY based on a SEED, is not part of INCA. It is made available for INCA by means of a Seed-&-Key-DLL. At the moment that a KEY is needed, INCA calls the algorithm encapsulated in the DLL with the SEED as an input parameter. The ECU-SW supplier can freely program the algorithm inside the DLL. Of course it should be the same algorithm as it is used inside the ECU software.The return value of the DLL is sent from the application system to the ECU.

2.3 Software architecture of enhance information security calibration

In different calibration tests or for different OEM customers, the required calibration variables and their data should be released in a controlled and differentiated manner. ECU calibration data encryption is to protect the calibration data security, optimization of calibration tasks, and maintenance of calibration test results necessary measures. This design scheme aims at the ECU data safety during the calibration test, analyzes the application requirements and proposes solutions.

The calibration staff uses the calibration software to calibrate the ECU. The ECU's database description file (A2L file) and calibration data file (S19, HEX file) are required to create the calibration project. The database description file (A2L file) defines the attributes and rules of the ECU internal calibration parameters and measurement signals from which the calibration software converts the ECU data to a calibrated view. After the calibration software establishes the communication connection with the ECU through the calibration protocol (CCP / XCP, etc.), it also needs to obtain the corresponding authority to calibrate, measure and program the ECU. Encrypting A2L files and using the seed-key mechanism to obtain calibration privileges protects the calibration data from both ASAM-MCD2 and ASAM-MCD1 levels. As shown in Figure 3:



Figur3. ECU data encryption framework

The calibration protocol itself also provides a security mechanism for protecting ECU's internal resources. It can set permissions on resources, establish an unlock procedure that requests the seed and then sends the key, and each resource can use an independent unlocking algorithm. The calibration software needs to obtain Seed-key.dll, which is consistent with various resource unlocking algorithms inside the ECU, to perform operations such as calibration, measurement, excitation or program brushing. The calibration software uses both A2L file encryption and the seed-key authority mechanism to encrypt ECU data.

3. Development of encryption algorithm

3.1 Process of A2L files encryption

Encrypt A2L files, convert database description information to binary files, and avoid known-plaintext attacks. Instead of passing the original A2L file during a calibration test or project implementation, issuing a modular or privileged encrypted database file can facilitate calibration task demarcation and calibration authority grading.

Encryption A2L file can use 3DES (Triple Data Encryption Standard) algorithm. DES is a packet encryption algorithm that outputs a 64-bit cipher text based on a 64-bit key (56-bit valid), plaintext input in 64-bit groups, chaos and spread (that is, substitutions first) and multiple combinations. DES algorithm shown in Figure 4. It is a symmetric algorithm (the same algorithm used for encryption and decryption) and belongs to private key encryption。

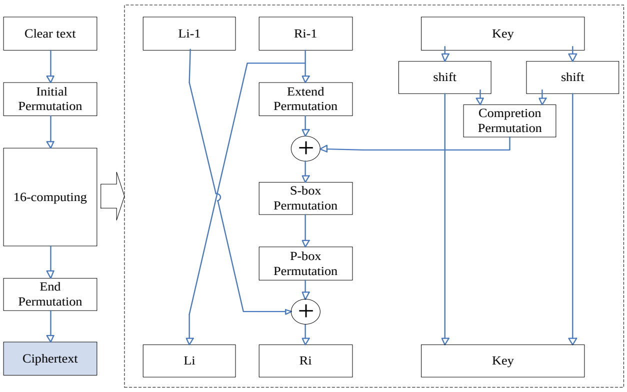


Figure 4. DES algorithm structure flow chart

3DES extends the DES key length to 128 bits (or 192 bits), encrypts plaintexts three times with two (or three) keys, and concatenates them with block ciphers to increase the encryption strength, as shown in Figure 5.

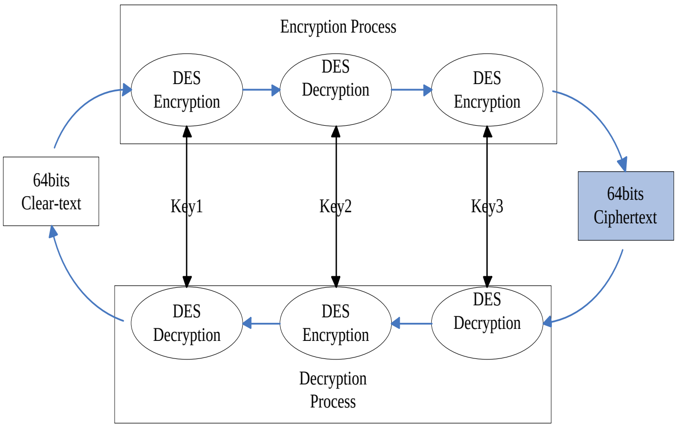


Figure5. 3DES encryption and decryption diagram

Use the encryption algorithm in the 3DES tool to convert the A2L file to an encrypted database file; use the decryption algorithm in the AMC calibration software to restore the encrypted database file to A2L before resolving the variable information. ECU Data Encryption Manager manages 3DES tools, releases variables in A2L files based on tasks and permissions, and issues encrypted database files.

3.2 A2L file decryption

As described in the previous section, we know that A2L files will be encrypted and the database description will be converted to binary files to avoid known plaintext attacks. Therefore, during the calibration test or project implementation, instead of transmitting the original A2L file, a distributed or authorized encrypted database file is issued and the decryption work is performed by the calibration system, so as to facilitate task demarcation and calibration permission grading.

4. Application

4.1 Encryption A2L file

Using the ideas and methods presented earlier in this article, we developed an A2L file encryption tool, the main interface of the tool is as Figure 6：

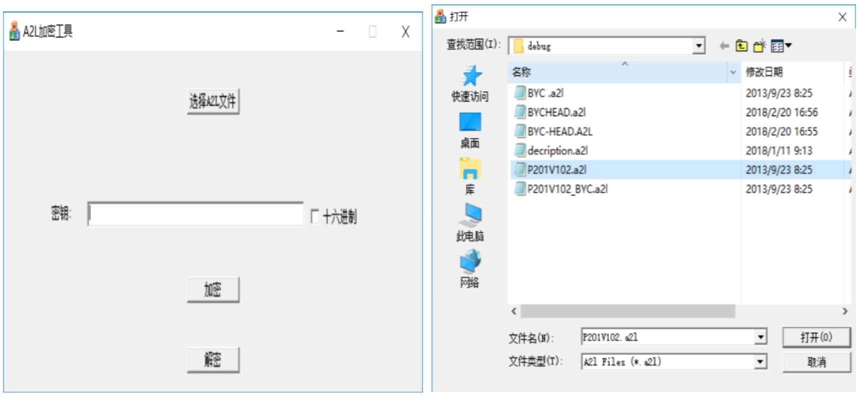
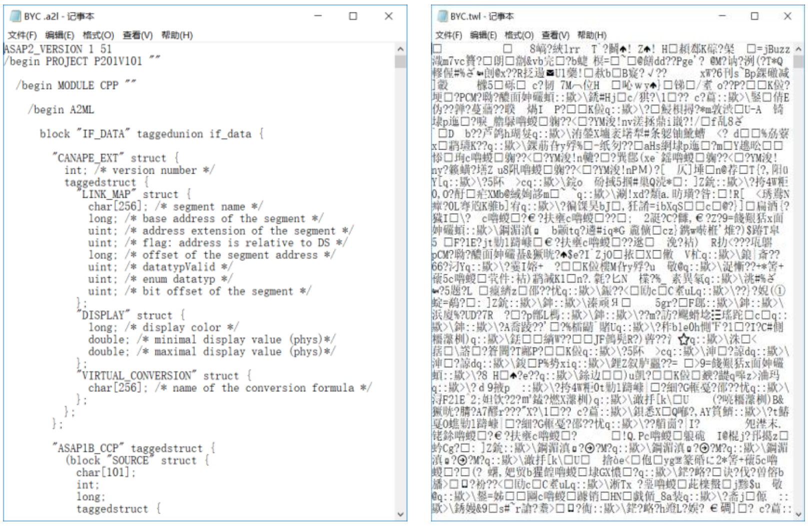

A2L加密工具
选择A2L文件
密钥:
十六进制
加密
解密
打开
查找范围(I): debug
快速访问
桌面
库
此电脑
网络
名称
修改日期
BYC .a2l 2013/9/23 8:25
BYCHEAD.a2l 2018/2/20 16:56
BYC-HEAD.A2L 2018/2/20 16:55
decription.a2l 2018/1/11 9:13
P201V102.a2l 2013/9/23 8:25
P201V102_BYC.a2l 2013/9/23 8:25
文件名(N): P201V102.a2l
文件类型(T): A2l Files (*.a2l)
打开(O)
取消

Figure 6. Interface of Encryption Application Software

Select the file you want to encrypt, and then enter the appropriate password, click the Encryption button, the system will automatically generate a file with the same name as the original A2L file extension TWL file, the file that we have encrypted data file.

Following is the contents of the A2L file.


BYC .a2l - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
BYC.twl - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
ASAP2_VERSION 1 51
/begin PROJECT P201V101 ""

  /begin MODULE CPP ""

    /begin A2ML

      block "IF_DATA" taggedunion if_data {

        "CANAPE_EXT" struct {
          int; /* version number */
          taggedstruct {
            "LINK_MAP" struct {
              char[256]; /* segment name */
              long; /* base address of the segment */
              uint; /* address extension of the segment */
              uint; /* flag: address is relative to DS */
              long; /* offset of the segment address */
              uint; /* datatypValid */
              uint; /* enum datatyp */
              uint; /* bit offset of the segment */
            };
            "DISPLAY" struct {
              long; /* display color */
              double; /* minimal display value (phys)*/
              double; /* maximal display value (phys)*/
            };
            "VIRTUAL_CONVERSION" struct {
              char[256]; /* name of the conversion formula */
            };
          };
        };

        "ASAP1B_CCP" taggedstruct {
          (block "SOURCE" struct {
            char[101];
            int;
            long;
            taggedstruct {
```

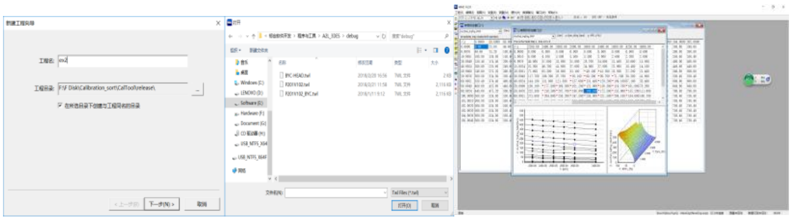
a).Plaintext of A2L b).Encryption file

Figure 7. Contents of plaintext and the Encryption of a same A2L file

Figure 7a is the plaintexts of the original A2L (file name is BYC.A2L) abide by the international ASAM standard. The Figure 7b is the encrypted file（We define the default encrypted extended file name is *.twl, so the file name is BYC.twl）which encrypted from the same file BYC.A2L.

4.2 Import the encrypted A2L file

Generally, A calibration have a wizard to help user create a project, and the guider will open a *.a2l file and a *.hex file. In this calibration software which have decryption function, it must open a *.twl (which has been Encrypted by the encryption software descripted in IV A.) and a .hex file. The interface showed in Figure 6.



工程名: ex2

工程目录: F:\F Disk\Calibration_sort\CalTool\release\

☑ 在所选目录下创建与工程同名的目录

BYC-HEAD.twl
R201V102.twl
R201V102_BYC.twl

Figure8. Interface of Encryption Application Software

5. Conclusion

In this paper, we firstly proposed a method for the protection of calibration variables and the a2l file integral. And then we further implement the symmetric encryption algorithm based on 3DES algorithm in to the calibration software. Meanwhile, according to this method and algorithm principle, we have developed a calibration data description data encryption software independly, as well as built-in decryption function calibration software. The actual engine ECU calibration experiments show that the encryption and decryption methods effectively ensure the reliability and safety of A2L files.

References

[1]. Schuermans R, Zaiser R, Hepperle F, et al. XCP-Part 1-Overview-1.0.Association for Standardization of Automation and Measuring System, 2003.

[2]. Schuermans R, Zaiser R, Hepperle F, et al. XCP -Part 2-Protocol Layer Specification-1.0. Association for Standardization of Automation and Measuring System, 2003

[3].[ASAM AE CDF] ASAM: Calibration Data Format V2.0.0, 2006

[4].[ASAM MCD-2FIBEX] ASAM: FIBEX - Field Bus Exchange Format V3.0, 2008

[5]. [ASAM MCD-2D ODX] ASAM: Diagnostic Data Model Specification V2.2, 2008

[6].[ASAM AE COMMON SEED&KEY] ASAM: Seed&Key and Checksum Calculation API V1.0

[7]. Yuejiao DING,Junchao ZOU,Jian TANG, Design of New Energy Vehicle Air Conditioning Calibration Software Based on CAN Bus, Automotive Engineering [J],2007 (Vol. 29)No. 7

[8]. AB Dariane,MM Javadianzadeh,LD James, Developing an Efficient Auto-Calibration Algorithm for HEC-HMS Program, Water Resources Management , 2016 , 30 (6) :1923-1937

[9]. Chunyang MU etal., Development and Implementation of Calibration System for ECU in Electronically Controlled Diesel Engine, Automotive Engineering 2007 (Vol. 29)No. 7

[10] JiaQi CHEN, Xuan LIU, Li-Quan DUAN, Electronic Control Engine ECU Calibration System,Computer system application[J],2012,Vol 21,No1.