USER REPROGRAMMABILITY IN EW TRAINERS

Rollin L. Olson
Senior Engineering Analyst
AAI Corporation
Baltimore, Maryland

ABSTRACT

There is a general trend toward user reprogrammability in EW equipment, as exemplified by the ARL-74 Radar Warning Receive and ALQ-165 ASPJ jammer. EW trainers are likewise moving toward greater reprogrammability by the user. EW trainers have large data bases for simulated threats and ownship equipment. Reprogramming enables the user to keep the trainer current with updated threat data and with modified versions of EW equipment employed in the trainer. EW trainers are reprogrammed by changing input data. Data can be performance parameters or control data that trigger various functions in the trainer software. Off-line data editors ease the task of changing data. A number of problems remain in the generation and use of reprogramming facilities. The first is the definition of user requirements. Second, the user must collect and digest data to make updates. Finally, the user must contend with configuration control problems if each user site can reprogram the trainers separately.

INTRODUCTION

In recent years, Electronic Warfare equipment has been moving toward greater user reprogrammability. With the advent of digital electronics and software control of intelligent devices it has become feasible for the user of EW equipment to modify control parameters in EW receivers and transmitters to provide great flexibility in responding to electronic threats. Typical of the new reprogrammable devices are the AN/ALR-74 Radar Warning System and the AN/ALQ-165 Airborne Self-Protection Jammer. Both devices contain large data files that control the processing of threat signal data. These data files are reprogrammable on the flight line by means of a truck-mounted loader-verifier.

EW trainers mirror this trend toward reprogrammability. Trainers of a generation ago consisted of hard-wired electronic components and, if computer-controlled, a single inflexible and inaccessible computer program. Recent trainers, however, rely heavily on sophisticated computer software and large data bases for simulated threats and EW equipment. Reprogrammable features included with modern trainers enable the user to keep the trainer current with updated threat data and with modified versions of EW equipment employed in the trainer. Such features greatly increase the flexibility of the trainer and grant the user a large measure of control in making modifications to the functional operation of the trainer. This paper describes some of the reprogrammable features employed in EW trainers and discusses the responsibilities placed on the user by these increased capabilities.

WHAT IS REPROGRAMMABILITY?

The term "reprogrammability" is a rather broad umbrella that covers several distinct aspects of an electronic device. There are several levels at which the operation of a device can be reprogrammed. At the highest or most superficial level, the user may change input data such as RF frequency. This type of data is separate from the functioning of the device and may be altered without knowledge of the operational details of the device. In resetting these data values, the reprogrammer may alter operating ranges, etc., but has little or no control over the functions performed by the device. On the other end of the scale are changes to the operational software, altering the algorithms employed in the device. Altering the software permits the user to make any number of changes to the device, of any magnitude. This type of change requires training in software programming as well as an understanding of the software being modified. Software modifications by the user can lead to a host of difficulties involving incompatibility with the original software.

Between these two extremes lies the realm of data-driven software. Many EW devices employ software that depends heavily on the data to tell it what to do. For example, a radar signal processor may contain a number of standard software routines to perform various signal processing functions. These functions are activated by a data table that lists the functions to be performed and the conditions under which they are to be performed. This arrangement affords the user great flexibility in controlling the functions of the device without the necessity of altering the program software in the device. Figure 1 illustrates some possible control data for a hypothetical signal analyzer. Each line of the data instructs the device to examine a particular signal characteristic within a given range. If the signal passes all the tests, then it is identified as the emitter listed at the end of the table. Any number of different data tables may be written for different emitters. In each case the user "programmer" is instructing the device as to what functions to perform without concerning himself with the actual software that performs the functions.

Step Number	Type of Analysis to be Performed	Tolerance
1	Frequency	4000 to 4200 MHZ
2	Pulse Width	2.0 to 2.2 msec
3	Scan Rate	2.0 to 3.0 Hz
4	Received Power	-30 to -20 db

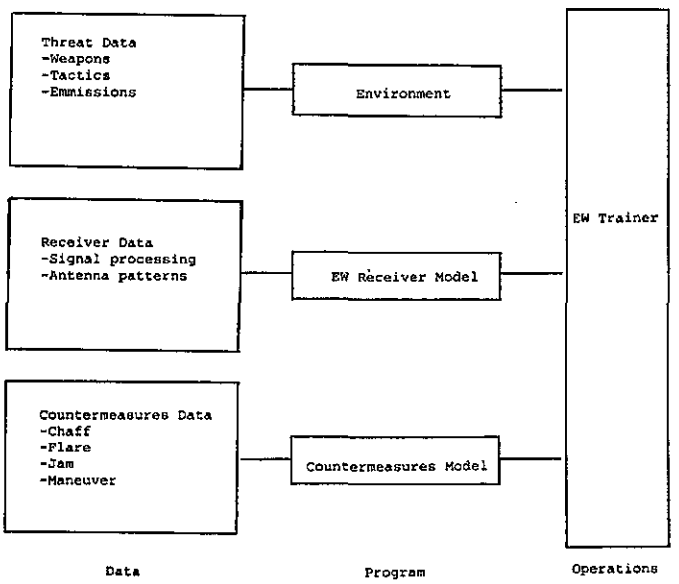
Identified Signal: Hard Ware - IIIA

Figure 1. Hypothetical Signal Analysis Software Control Table

A software-driven device may also use "flags" or bits of data to act as on-off switches. If a particular data word is set to "on", then the function it controls is turned on; if the data indicates "off", then the function is turned off. This type of control is particularly powerful if a series of flags can be used to enable and disable a sequence of functions.

REPROGRAMMABLE FUNCTIONS IN EW TRAINERS

Modern EW trainers employ many of the reprogramming features employed in field EW equipment. Figure 2 describes an EW trainer in terms of data and programming requirements. This trainer includes software models for the threat environment, EW receiver equipment and electronic countermeasures. The details of this structure may vary considerably among trainers, but most trainers include these basic components. The modelling consists of two levels - the software model and the supporting data.



SOFTWARE STRUCTURE FOR EW TRAINER
Figure 2

The software model is the actual software program, written in FORTRAN or some other computer language. The software model in Figure 2 has three major sections. The threat environment model selects and updates a simulated threat environment continuously during the trainer mission. The EW receiver model simulates the response of the ownship EW signal detection equipment. The countermeasures model detects the countermeasures performed by the student and simulates their effect on the threat.

Each of these three software units depends heavily on the supporting data supplied to it. The threat model employs data supplied in a threat data library containing data on signal characteristics, weapons and offensive and defensive tactics. The EW receiver model depends on data supplied for the EW equipment. This data may take the form of control parameters or emitter identification data for signal processing in the receiver. The countermeasures model employs data on the effectiveness of various countermeasures against each threat. In each of the three modules, the operation of the software is largely controlled by the data that is fed into the program. In this way the software modules can be changed or "reprogrammed" by altering the input data.

AAI Corporation has developed a series of off-line data entry facilities for entering and modifying the supporting data. Each major area of data is handled by an interactive data editor designed specifically for the data to be entered. The user enters data via the terminal by making choices in a menu or filling in a data form on the computer terminal screen. The user may enter all new data or examine and update old data. A typical editor program will store the user's inputs, then process the data into a format that is usable by the real-time simulation program. The input data is retained so that it may be called up again, examined and modified to produce new output. The structure and functions of a typical data editor are illustrated in Figure 3.

These editors allow the user to significantly alter or "reprogram" the simulator. The operation of threat signals and weapons, EW receivers

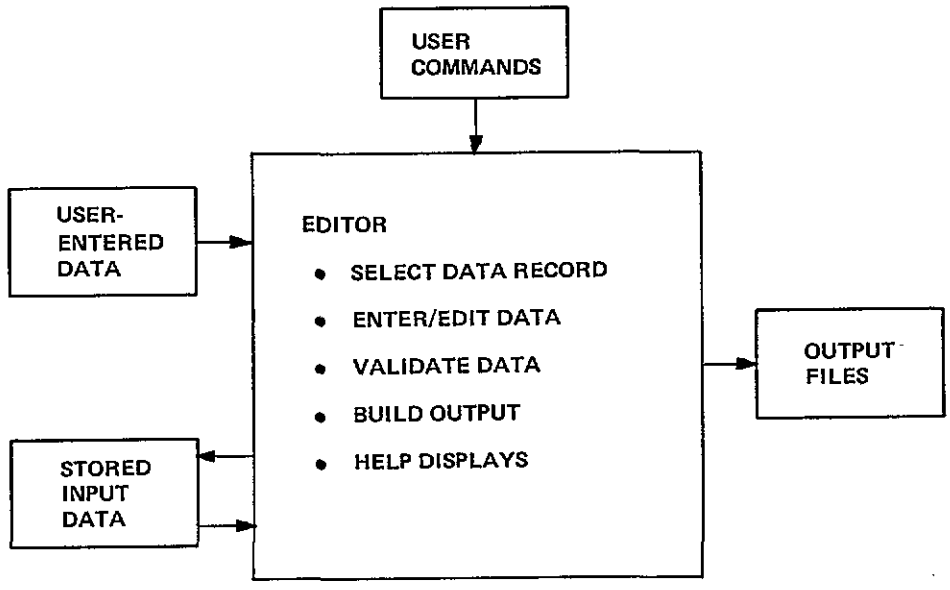


Figure 3

and countermeasures may all be greatly modified by altering their input data. This is particularly true in the software that is data-driven, as described above, such as the threat tactics algorithms which are triggered by control data in the data library. For example, by altering the data in the tactics editor, the user can change the tactics performed by one or more threats.

The editors are used as part of the data preparation process illustrated in Figure 4. The data is gathered from information sources and reviewed for completeness and validity. It is usually necessary to check the data, fill in data gaps and reconcile any inconsistencies in the data. Once the data is in good form it is entered into the data editors, which produce output files for use in the simulation.

The data editors for any particular trainer are developed in conjunction with the real-time simulation software. The data requirements of each real-time software module are reflected in its supporting data editor. Thus, if a module requires a significant amount of control data, the supporting data editor will be oriented largely toward specifying and entering this control data.

It may be noted that this system of off-line data editors does not permit the user to alter the software modules themselves. Any change in software operation that falls outside the control of the supporting data must be made by skilled programmers who understand the software. Such a change of course requires more expertise than a simple change in the data.

DESIGN OF A REPROGRAMMABLE TRAINER

The design and use of a reprogrammable trainer poses a number of challenges to the system designer as well as to the user. The design of the trainer poses the fundamental question as to what functions should be reprogrammable and to what extent. The user may prefer to have everything reprogrammable by data, but in some areas such a housekeeping tasks this would be difficult or irrelevant. The degree of reprogrammability more commonly comes into question. The user may specify more reprogrammable features than he is likely to use. On the other hand, over-eager software designers may well build in a number of reprogramming features that will never be used after the trainer has been delivered.

It is important when defining the reprogrammable features of an EW trainer to determine the current and future needs for flexiblity in the trainer. For example, the data-entry facilities should certainly allow for changes in threat emitter characterics, but will the trainer require the inclusion of entirely new characteristics in the future? Will the EW Receiver and Countermeasure modules require frequent revision as the equipment in actual aircraft undergo a series of modifications? How serious will the changes be? Can the updates be handled by changes in data or will they require software modifications? The areas requiring the greatest flexibility should have the greatest degree and ease of reprogramming. Control-data tables such as the one illustratd in Figure 1 are especially desirable when great flexibility is required. If

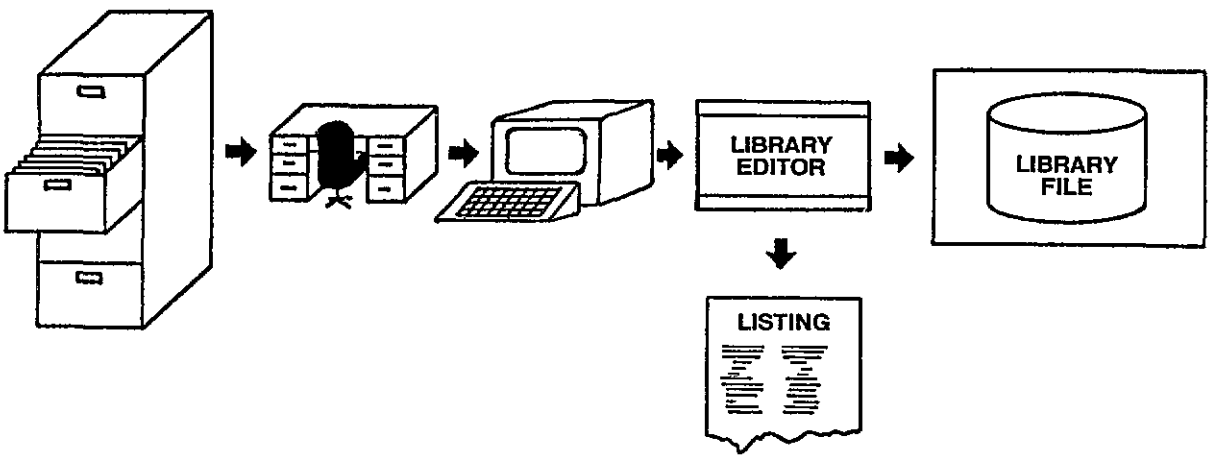


Figure 4

changes are going to be made frequently, the reprogramming facilities should be designed to maximize ease of data collection and entry.

USER RESPONSIBILITY FOR DATA

After the trainer is built and delivered to the user, the wealth of data stored in the trainer and the facilities for updating this data give the user powerful capabilities in modifying the trainer, yet exercising this capability requires considerable care on the part of the user. Changes to the trainer data require that the change be identified precisely and data requirements for this change to be specified. Then the data must be researched. A search of available data sources usually yields incomplete or contradictory information. The user must search further for the data or extrapolate from known values. The data required by a simulation nearly always represents a particular model or view of the real world. The person who develops the data must conform to or keep in mind the simulation model in extracting data from the real world. This is particularly true of threat modelling, where a potentially vast number of facts concerning a weapon system must be reduced to the relatively small set of data required by the trainer. Even when data values are collected automatically from computerized data files, it is still necessary to examine the extracted data for reasonableness. Altering the data to conform to software model will require some familiary with the software algorithms and data specifications.

It is apparent, then, that user reprogrammability requires some familiarity with the data and with the trainer software model. The original system designers can design the trainer in such a way as to minimize the knowledge required by a reprogrammer, but it is impossible to make the process of reprogramming entirely mechanical. It is very desirable for the user and the system designers to come to an agreement on the level of sophistication that will be required during reprogramming, since the limitations on reprogramming effort may well be a deciding factor in choosing one type of system design over another. Elaborate and complex software may prove to be less usable in long run than a simple model, if the complex model is too difficult to reprogram.

Configuration control also presents a problem for the user with reprogramming capabilities. End-users often want the flexibility to reprogram each individual trainer to conform to the requirements of the field units to which they are assigned. This is particularly true where the trainer simulates flight-line-reprogrammable equipment such as the ALR-74 RWS, which may be programmed individually at the wing level. Minor differences among trainers will not ordinarily cause serious problems. However, if major modifications are to be made to the trainer, the accumulation of changes to the original trainer may be incompatible with the new design. Problems also arise when changes are made to an individual trainer and not documented. Such changes may introduce quirks into the trainer that are extremely difficult to trace.

One method of configuration control is to provide a single depot site with reprogramming facilities that perform reprogramming tasks for all trainer sites. The depot site can maintain data libraries and reprogramming expertise that need not be duplicated at each trainer site, as well as configuration and changes records for each trainer. Each trainer site can request a

change in its trainer, which will be performed and recorded at the depot site and delivered to the trainer on disk or tape. Major changes affecting all trainer units can originate at the depot and be transferred to all trainers. This central depot system is currently in general use, and despite some advantages of on-site reprogrammability, will continue to provide the best balance between flexibility and control.

CONCLUSIONS

The growth of the use of computer software and large data bases in EW trainers has made it possible to modify and update the trainers by changing data alone. Data-driven software models and off-line data entry facilities give the user a large degree of control over the functional operation of the trainer. The increasing use of reprogrammable avionics equipment and continuing updates to this equipment make it all the more necessary that EW trainers be easily reprogrammable.

However, this reprogramming capability imposes increased responsibilities on the user. The user must participate in designing the reprogrammable features, specifying current and future requirements for flexibility in the trainer. When the times comes to reprogram the trainer, the trainer, the user must concern himself with EW data, models used in the trainer software, and configuration control. In these areas the end user must develop some of the expertise required for the original system designs.

ABOUT THE AUTHOR

MR. ROLLIN L. OLSON is a Senior Engineering Analyst in Electronic Warfare Operations, Electronics Division of AAI Corporation. He is currently involved in design and development of Electronic Warfare trainers. He has developed software simulations for radar emitters and receivers as well as data entry editors for EW trainers. His educational background includes graduate studies in computer science at Loyola college and in urban planning and history of technology at Johns Hopkins University.