IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 19 October 2023, accepted 30 October 2023, date of publication 1 November 2023, date of current version 8 November 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3329432

RESEARCH ARTICLE

A New Scheme to Solve the Compatibility Conundrum for CPU(TMSC320C32) Used as a Controller for Industrial Facilities

JUNYOUNG SON[1], (Member, IEEE), AND HEEMAN PARK[2], (Member, IEEE)
[1]Korea Atomic Energy Research Institute, Daejeon 34057, South Korea
[2]VARN Inc., Buk-gu, Gwangju 61008, South Korea

Corresponding author: Heeman Park (hareup@varn.tech)

This work was supported in part by the Ministry of Science and ICT in South Korea under Grant 2021M3C1C4039576.

ABSTRACT Texas Instruments (TI)'s SMQ320C32x is used in various fields such as military, nuclear facilities, and aviation. However, this CPU has difficulties in compatibility such as discontinued parallel port with Computer & Emulator for Joint Test Action Group (JTAG) Cable and security & availability problem such discontinued Windows OS. For development and maintenance of devices using this CPU, JTAG connection is essential, and parallel port (LPT) connection is essential now. However, PCs with built-in parallel port are not produced. And, for connecting Programmable Logic Controller (PLC) composed of this CPU in nuclear power plants or other industrial facilities to the computer, the XDS510PP-MPSD product in Spectrum Digital Inc must be used, and it is difficult to secure it. Also, you must use Windows XP or Windows 2000 with Code Composer program provided by TI, which has security problems and has been discontinued. According to the regulatory requirements in the nuclear field, these compatibility and security issues must be resolved before use. This paper presents the world's first solution to these difficulties.

INDEX TERMS PLC, XDS5100PP, TMS320C32SMQ, SMQ320C3x, control system, nuclear power plant, JTAG, parallel port, cyber security requirements, security, compatibility problem.

I. INTRODUCTION

In today's modern world, Information Technology (IT) has advanced dramatically and been applied to the Industrial Control Systems (ICSs) of critical national infrastructures, including power, energy, water, transportation, telecommunication and nuclear power. As the use of digital systems in infrastructure facilities increases and the possibility of intelligent cyber-attacks against infrastructures is emerging, the enhancement of cyber security is needed for the critical digital systems of various infrastructure facilities [1], [2], [3], [4], [5], [13], [14], [15], [16], [17], [18]. For example, the necessity of cybersecurity for nuclear power plants' systems was highlighted by the Stuxnet computer worm in 2010. Stuxnet caused substantial damage to the Iran's nuclear program. Since then, cyber threats and attacks have constantly threatened the systems of nuclear facilities, including the 2014 KHNP cybersecurity threat incident, the Monju malware attack in Japan, the Ukrainian power grid cyberattack in 2015, and the German NPP's computer virus infection [25]. However, when the control system in critical facilities was applied, it was no considered with cyber security function and requirements. Furthermore, control systems applied to critical facilities are used for a long time once developed and applied, and there are many difficulties in replacing them, thus, the existing systems are continuously utilized. In this industrial environment, there are various pending issues, such as being discontinued or having cyber security issues [22], [23].

Nuclear Regulatory Commission (NRC) Regulatory Guide (Reg) 5.71 [2] and Korea Institute of Nuclear Nonproliferation and Control (KINAC) 015 [3]., require to specify the cyber security policy for the vulnerability assessment and scan. The NRC Reg 5.71 describes specific cyber security requirements in the Appendix A "Generic Cyber Security PLAN TEMPLATE", Appendix B "Technical

The associate editor coordinating the review of this manuscript and approving it for publication was Junjian Qi.

Security Controls'', Appendix C ''Operation and Management Security Controls'' [2]. In Appendix A.3.1.3 ''security functional requirements or specifications that include the following: known vulnerabilities regarding configuration and use of administrative, A.3.1.6 '' Licensee/Applicant performed an effectiveness analysis, and vulnerability'', A.4.1.3 Vulnerabilities Assessments and Scans, A.4.2.2 ''Licensee/Applicant] manages critical digital assets (CDAs) for the cyber security of SSEP functions through on ongoing evaluation of threats and vulnerabilities and implementation of each the security controls provided. Dispositioning includes implementation of security controls to mitigate newly reported or discovered threats and vulnerabilities'', A.4.2.4 '' recent cyber security studies or audits (to gain insight into areas of potential vulnerabilities).'', B.1.2.1 ''alternative controls or countermeasures are implemented to mitigate vulnerabilities by the lack of security functions provided by third-party products'', B.5.1 ''Licensee/Applicant] documents the remediation period appropriate for software and service updates or workaround to mitigate all vulnerabilities associated with the products and to maintain the established level of security'', B.5.5 ''[Licensee/Applicant] established, implements, and documents the notification of vulnerabilities affecting CDAs to be conducted'', C.3.2 ''[Licensee/Applicant] established, implemented, and documented procedures for identifying the security alerts and vulnerability assessment process, communicating vulnerability information, performing vulnerability scans and assessment of the CDA''. As described in many cyber security requirements, discovery, defense, and prevention of vulnerabilities are one of the most important cyber security policies. In addition to known vulnerabilities, potential vulnerabilities should be discovered and countermeasures should be prepared in advance to ensure security safety against cyberattacks. Nuclear Instrumentation & Control (I&C) systems have been designed, developed and applied for decades. In addition, safety and physical security have been considered and developed, applied as important features for Nuclear Power Plant (NPP)'s system. On the other hand, nuclear I&C systems have not considered, prepared, developed, applied for cyber security. Recently, the importance of cyber security of industrial infrastructure including nuclear facilities has increased dramatically worldwide. Research on nuclear cyber security is actively being carried out [24]. Therefore, the worldwide nuclear and cyber security engineering will continue to find and supplement weaknesses in nuclear critical digital systems. NPP's systems are the most important system among infrastructures, so discovering and announcing vulnerabilities are sensitive. Even if vulnerabilities are found, a solution to the vulnerabilities must be presented. The components of NPP's control system are composed of various legacy systems and newer products. Thus, there are many difficulties to analyze and unknown important vulnerabilities which have not yet been founded. This section introduces the first analysis of potential vulnerabilities for JTAG communications and authentication used in one of NPP's control system. The PLC introduced in this paper uses TI CPU. To develop and debug the RTOS program on the TI CPU, the JTAG interface is used. Current using CPU model has been from the past, but is now discontinued. This section analyzes and find the vulnerabilities of JTAG interface used in connection with the control system and proposes the countermeasures. The PLC introduced in this paper is one of the latest control systems in the world. It is expected that more vulnerabilities will be found in other PLCs round the world. It is necessary to prepare a preliminary countermeasure by discovering important vulnerabilities. With proposed analyzing methodologies could be referenced to find vulnerabilities in many PLCs which have operated and developed in infrastructure facilities including NPPs around the world. And this paper proposes a method to solve these problems for the first time, and proves that the proposed method is applicable based on the developed results.

II. RELATED WORK

A. NUCLEAR DIGITAL CONTROL SYSTEM–PLC

In order to respond to a cyber security incident at a NPPs, it is necessary to fundamentally analyze the situation of infringement by obtaining operational information of the main system. This research targets POSAFE-Q PLC operating on APR1400 NPP [19], [20]. The CPU of the POSAFE-Q PLC is composed of SMQ320C32, which is the target system for discovering potential vulnerabilities in this chapter. It is an old product of TI and uses a parallel port (LPT) as an interface for information acquisition and development by JTAG interface. This study analyzes the communication protocol with computer connected to JTAG debugger based on the parallel port and the inter-working technology with code composer which is a development & debugging tool supported by TI as shown in Fig. 1. Development programs that are currently in used can be developed and acquired through this interface. Although the CPU used is a safe product, compatibility problems may occur in connection with the system used for development and data acquisition as an old product. If inter-working computer models are not manufactured and discontinued in the future, data acquisition and development will be difficult. Therefore, this research analyzes the communication technology of the parallel port interface used for the POSAFE-Q PLC and the JTAG connection and compatibility solution method. And this chapter describes the discovered floating points error in computing development using pSET-II program connected to PLC. In addition, the inspecting methodologies are proposed to detect the modified contents of the firmware of the PLC compared to the initially downloaded to the PLC. By analyzing the access interface and potential vulnerabilities in advance for developing, restoring, modifying, and acquiring the important information of the target PLC system, this paper describes the technology to find out the possible problems in the future and to prepare the solution.

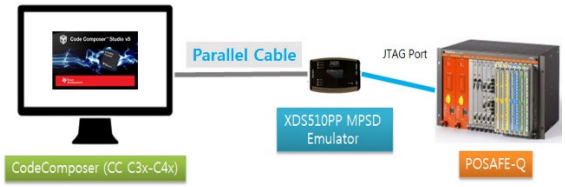
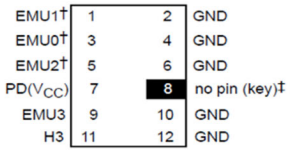


FIGURE 1. TMS320Cx core to code composer communication.



Header Dimensions:
Pin-to-pin spacing, 0.100 in. (X,Y)
Pin width, 0.025-in. square post
Pin length, 0.235-in. nominal

XDS510 Signal	Description	'C30 Pin Number	'C31 Pin Number
EMU0	Emulation Pin 0	F14	124
EMU1	Emulation Pin 1	F15	125
EMU2	Emulation Pin 2	F13	126
EMU3	Emulation Pin 3	F14	123
H3	'C3x H3	A1	82
PD(V_{CC})	PD(Presence Detect), Indicates that the emulation cable is connected and that the target is powered up. PD should be tied to Vcc in the target system		

FIGURE 2. 12 pins of MPSD.

B. TI CPU–SMQ320C32 AND TMS320C32 PROCESSOR

There have been a lot of products composed of TI CPU from the past. Among the many products of TI CPU, there are SMQ320C32 and TMS320C32 processors [9], [11], [12]. The TMS320C32 processor is widely used in general purpose, and the SMQ320C32 is a processor designed for environment which could be used for military product. The SMQ320C3 is part of Texas Instruments'320C3x digital signal processor generation. The SMQ320C32 is an enhanced 32-bit floating-point processor manufactured with 0.7-μm triple-level metal CMOS technology.

The SMQ320C32 optimizes speed by implementing the functions that other processors implement via software or microcode in hardware. This hardware-intensive approach provides performance previously unavailable on a single chip. The boot-loader functionality of the SMQ320C32 is equivalent to that of the '320C31. The 320Cx series CPU is developed and operated in the same environment as the TMS320C32. Therefore, the JTAG module and interface used for CPU development works in the same environment as TMS320C32.

III. DISCOVERED POTENTIAL VULNERABILITY ON JTAG INTERFACE COMPATIBILITY

A. C3X TO JTAG EMULATOR INTERFACE

The C3x, including SMQ320C32 and TMS320C32 processors, uses Modular Port Scan Device (MPSD) technology to allow full emulation through a serial scan path when communicating with JTAG interface.

There must be 12pins to communicate with MPSD. Number 8 Pin is removed to prevent improper connections as shown in Fig. 2 [11], [12]. Currently, the TMS320C32 DSP processor performs development and OS download, debugging through JTAG emulator. The JTAG emulator should use the XDS510PP-MPSD product to successfully connect to the JTAG [11], [12]. The XDS510PP-MPSD controller interface in Fig. 2 is a hardware tool used to develop hardware and applications for Texas Instruments embedded processors and to debug their behavior. The XDS510PP-MPSD and the processor are connected via JTAG communication, and the PC and XDS510PP-MPSD communicate by the parallel port interface. The PC with the Parallel Port is now discontinued to be produced as shown in Fig. 3. The debugger software used for the XDS510PP-MPSD controller interface is Code Composer. Code Composer is an integrated development environment (IDE) that supports the TMS320C30/C31/C32 DSP (Digital Signal Processor) development environment. It includes a debugger, C compiler, assembler, and link. Code Composer is a different development environment from Code Composer Studio and supports C2x, C24x, C3x, C4x, C5x, C54x, and C6x DSPs, which are not supported by Code Composer Studio [6], [7], [8], [9], [10], [12]. Code Composer is the latest version, released in 2001, version 4.10, and Code Composer for C3x and C4x DSP development is now available from Spectrum Digital, a partner in Texas Instruments. According to the Code Composer tool usage instructions, the following environment is recommended for Code Composer operation: 500MB RAM or more, SVGA (1024*768) color display, 2GHz or higher Pentium PC, Windows 2000 (Service Pack 4), Windows XP (Service Pack 1&2). In fact, after testing many things, I found that it worked more reliably on Windows XP Service Pack 3 than the recommended ones. It is assumed that the manual was written before Service Pack 3 was released. There are several options for operating the XDS510PP-MPSD, which are added to the xds510pp.ini file. The emulation driver references the xds510pp.ini file to set the driver's input parameters as followings: speed = <0-100>, mode = < SPP4, SPP8, EPP >, port = <278, 378, 3BC >, nopoll. Speed is the delay time between port accesses. The higher the value, the more delay. port is the parallel port of the computer. IBM computers usually have a parallel port starting with the address 0 × 278, 0 × 378, and 0 × 3BC. mode is the hardware type supported by the host computer. The available modes for the driver are SPP4, SPP8, and EPP (including ECP submode) types. The default setting is port = 378, mode = EPP, and speed = 0.

B. JTAG EMULATOR TO COMPUTER INTERFACE

PC for development and debugging to JTAG interface connections communicate with the parallel port. The computer's parallel port is typically used to configure the interface between the computer and external hardware. The parallel port on the back of the computer is a D-type 25-pin female connector. The parallel port can receive 9-bit data or transmit

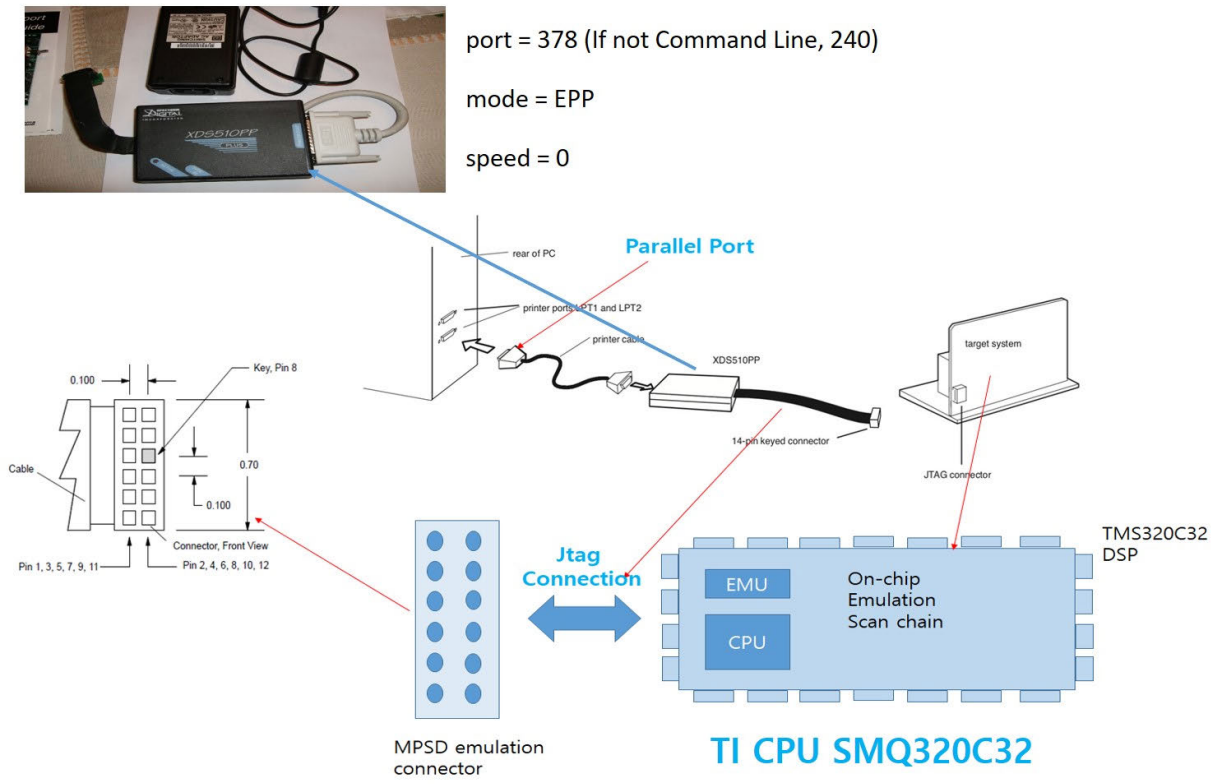


FIGURE 3. JTAG Emulator – PC communication.

TABLE 1. Description on parallel prot address.

Address	Description
0x3BC – 0x3BF	Efficient graphics port that integrates with normal cards
0x378 – 0x37F	LPT 1 address of normal PC
0x278 – 0x27F	Normal PC's LPT 2 address

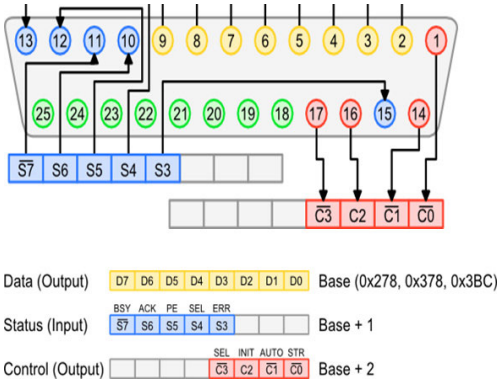


FIGURE 4. Parallel port pin connection.

12-bit data at a given time. To analyze the communication protocol between the JTAG interface and the PC, the communication drive and protocol for the modes of the parallel port should be analyzed in detail.

It is important to ensure that the correct address is used when reading from / writing to the parallel port. The parallel port is provided with one of the three base addresses (0×278, 0×378, $0 \times 3BC$) commonly used by computers. However, depending on which external device is active, it is easy to confuse the correct address and it is inconvenient to find. For the port address, $0 \times 3BC \sim 0 \times 3BF$: parallel port is integrated with the graphic card, $0 \times 378 \sim 0 \times 36F$: Normally LPT 1 address of the communication PC, $0 \times 278 \sim 0 \times 27F$: Normally describes the LPT 2 address of the PC as shown in Table 1.

1) STANDARD PARALLEL PORT (SPP)

The standard parallel port (SPP) is also known as the Centronics parallel port. The standard parallel port was developed by Centronics as an interface for unidirectional 8-bit unidirectional connection between host and printer. Standard parallel port interfaces have been widely used, but this interface has not been defined as an industry standard specification. Centronics' "standard" defines the 36-pin connector and interface signals on the printer side. Host-side implementations will vary until the IBM computer is released in 1981. The host parallel port implementation (also known as PC parallel interface) used on IBM computers is in fact the industry standard PC parallel port interface. The PC parallel interface defines a 25-pin DSub connector with eight unidirectional data lines, four control lines, and five status lines. Because there is no written standard, the timing relationship between the handshaking signals varies widely depending on the manufacturer's printer, even if compatibility with Centronics is

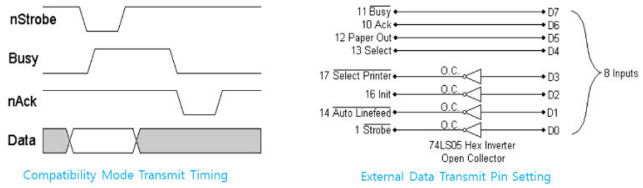


FIGURE 5. **Compatibility mode and data transmit.**

claimed. The parallel port has three pin groups: a data port, a status port, and a control port. The data port consists of 8 lines (pins 2 ∼ 9: I / O lines) and is used to send / receive data to / from an external device.

2) COMPATIBILITY MODE

Like most devices, the parallel port has several modes of operation. These operating modes range from standard modes that allow only one direction to extended function mode (ECP) which provides several additional functions using an extended function register (ECR). Generally, these operating modes can be set in the BIOS. Compatibility mode is a unidirectional mode used to transfer data from a computer to an external device at a rate of approximately 50 KB / s. There are four steps in the operation of transferring data from the compatible mode to the external device. 1) Write the data byte to the data port of the parallel port address to which the external device is connected. 2) A check is performed to check whether the connected external device is in use. 3) Set the STROBE line (pin 1) to LOW to transfer the data byte to the external device. 4) If the nAck line is set to LOW for 5 μs after receiving the data from the connected external device, the response is accepted. Generally, the compatibility mode is for unidirectional data transmission, but there are several ways to read data from an external device even in compatibility mode. The first one uses a bidirectional port, and the fifth bit of the control port is set to use this function. When this control port is set, the external device can access the connected parallel port address to transmit or receive data.

In the second method, the sum of the lines of the status port and the control port is 9, which can be used to transmit 9 bits. The external data lines are connected to each other using a digital device, Open Collector Inverters. The Open Collector Inverters allow the parallel port to continue to operate the state of each connected line.

3) BIDIRECTIONAL PORT

The IBM PS / 2 computer enhances the parallel port by adding a bi-directional driver to the data line. The I / O connector and signal assignment are the same. Parallel ports with bidirectional drivers are often referred to as extended mode parallel ports. IBM refers to a bidirectional port as a TYPE 1 parallel port, and defines a type 2 and a type 3 parallel port for reading or writing data blocks to or from a parallel port using a DMA channel. The register map for the IBM PS / 2 parallel port is shown below. TYPE 1 Parallel port has only the first three registers. This register has only the direction bit added to the parallel port control register, and the rest is the same as the SPP register set. TYPE 2 and 3 DMA transfers have the SPP timing described above. TYPE 2 and 3 During DMA write, the DMA controller writes data to the data port and transmits a STROBE pulse. When an ACK is received from an external device, a DMA request is transmitted and then byte data is transmitted. An external device can activate BUSY to hold the transmission. TYPE 2 and 3 During a DMA read, a pulse on the ACK line will generate a DMA request and initiate a transfer to system memory. The DMA controller reads the data port and generates a STROBE pulse.

4) ENHANDCED PARALLEL PORT (EPP)

EPP mode is much more effective than compatibility mode. Because it uses hardware rather than software to generate the timing, the transfer rate can be improved from 500KB/s to 2MB/s. This is the most used mode because the EPP port generates and controls all transfers to and from external devices. EPP mode activates a new register set in addition to the three registers used in compatibility mode. EPP mode adds a new address port and data port. SPP requires multiple software steps to transfer data, which EPP adds hardware and registers to automatically generate control STROBE and data transfer handshaking with a single I / O instruction. For ISA systems, the maximum transfer rate is 2MB/s. The EPP operation is a two-step bus cycle starting at the computer. The computer first selects the register of the external device and performs the address cycle. It then performs a series of reads / writes to the selected register. The EPP mode defines an INTR, which is a single interrupt request signal, so that an external device can send a signal to the computer. EPP mode consists of four operations: address read/write and data read/write.

5) ENHANDCED CAPABILITIES MODE (ECP)

The ECP mode was developed by Microsoft and Hewlett Packard as an extension of SPP. The ECP mode defines automatic hardware handshaking, command and data cycles, and FIFO DMA transfers. The handshaking signal for data transmission has the same timing relationship as defined for the SPP. When ECP mode uses DMA, the maximum transfer rate is 2.4MB/s. The ECP mode has a similar transmission speed to the EPP mode, but there are some additional features worth noting. The ECP mode uses a FIFO buffer to transmit or receive data. Compresses up to 64:1 using real-time data compression called RLE (Run Length Encoding), and enables other operations within the ECP mode using the Extended Controller Register (ECR).

IV. ANALYSIS OF POTENTIAL VULNERABILITY ON JTAG INTERFACE COMPATIBILITY

A. INTERFACE COMPATIBILITY

Communication between PC and JTAG interface uses parallel port. JTAG XDS 510PP-MPSD has its own address and

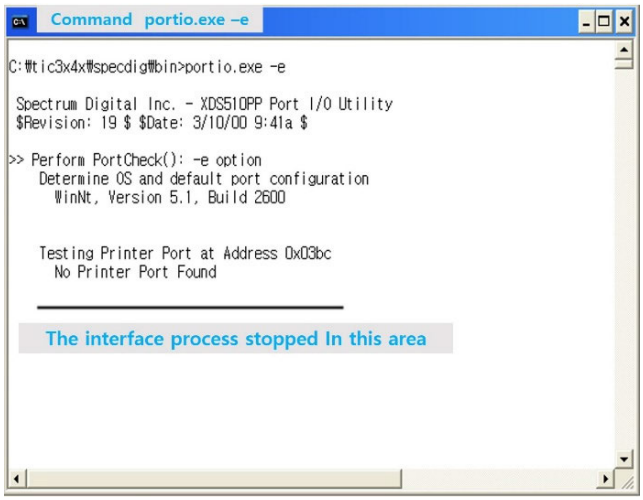


FIGURE 6. Stopping result with portio.exe -e.

mode. The XDS510PP-MPSD controller interface is a hardware tool used to develop hardware and application programs for TI's C3x and C4x DSPs and to debug their behavior. The XDS510PP-MPSD must be used for development, downloading and debugging of SMQ3210C32 and TMS320C32. However, there is a problem with availability. 1) PC with Parallel Port is discontinued. 2) Windows XP has also been discontinued and ninety seven Windows XP vulnerabilities were reported in year 2010 [26], [27]. 3) All of Parallel Port to USB convert products can't be connected to XDS 510PP-MPSD. Any product that uses the C3x processor can be a serious problem for availability. PLCs used in NPPs are also subject to problems such as product replacement, OS update, modification and development. In addition, since cyber security becomes important, when a cyber security incident occurs, it should be investigated through the JTAG interface. If the JTAG interface becomes unavailable after this, the cyber security incident investigation can't be done efficient.

B. CONNECTION WITH COMMERCIAL CONVERT CABLE

This research tried to connect to existing computer environment using most of commercially available USB to parallel port convert interface cable, but failed. The three factors: 1) PC OS to drive connection, 2) Drive to parallel port, 3) Parallel port to JTAG, are analyzed, but the most optimized best result is as shown in Fig. 6. The critical point to analyze this result and to research countermeasure is portio.exe program which is provided by Spectrum Digital. The company is only one providing the JTAG Emulator available to the PLC system

C. REVERSING THE FOUNDED PROBLEM

The IDA pro debugging tool [21] was used to analyze the configuration tool in real time, and it was confirmed that each mode is supported in the parallel port search process. The

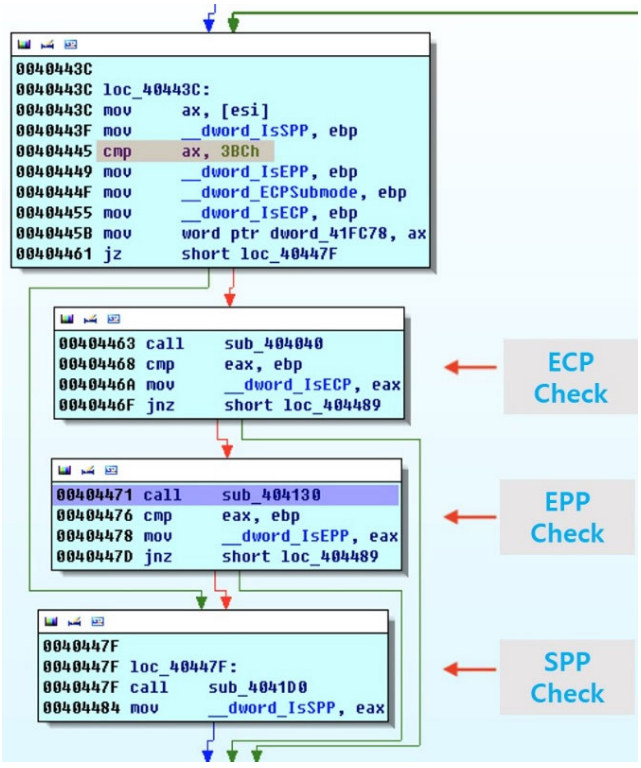


FIGURE 7. Process of checking each modes of the parallel port.

parallel port access communication is targeted to only three addresses: 0 × 3BC, 0 × 378, 0 × 278. Each parallel port should have a base address, and a physical address instead of a virtual address as shown in Fig 7. As a result of analysis of portio.exe, parallel mode is divided into three modes, and SPP is divided into SPP4 and SPP8. The ECP and EPP modes checking procedures are omitted for 0 × 3BC. Given the reason for this, it is assumed that the 0 × 3BC address is generally standardized for monochrome graphics adapters. All other addresses are test for ECP and EPP extension modes. As a result of the analysis, it was found out that an error occurred during the EPP mode test in the extended mode test process as shown in Fig. 8, Fig. 9.

The code reads the value of one byte by calling the inbyte() function on the [Base +3] address. which may cause a problem. If the parallel port is not in extended mode, there will be no more than [Base +3] address. Therefore, the process of checking whether the address exists is first required as exception processing. However, this configuration tool (portio.exe) omits exception processing and assumes that all 0 × 378 and 0 × 278 addresses are in extended mode.

As a result, the cause of the error is a critical problem with the setup tool itself provided by the JTAG manufacturer and is caused by the fact that all parallel ports except the 0 × 3BC address are recognized as an expansion mode by default.

V. COUNTERMEASURES OF DISCOVERED INTERFACE VULNERABILITY

As a result of the code analysis with reversing, the error problem is also one of the processes for testing the state of the

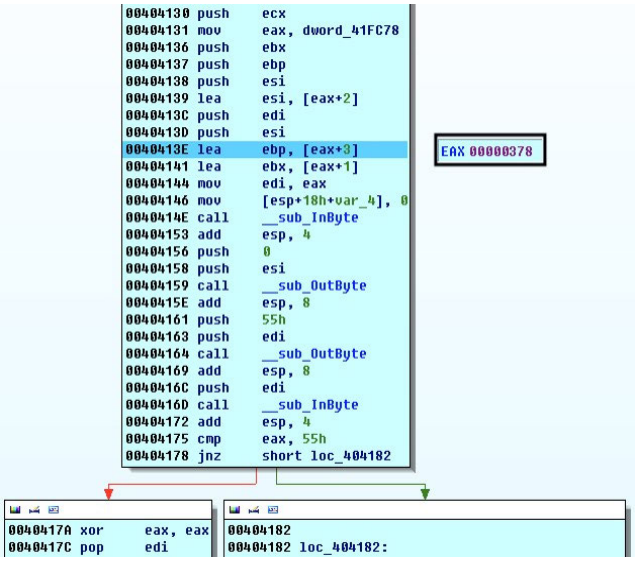


FIGURE 8. Checking EPP mode.

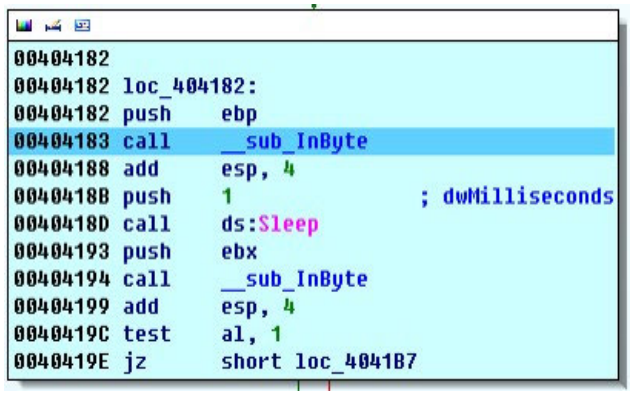


FIGURE 9. Founded error point for checking EPP mode.

EPP mode, and it could be described that the data is written to the address $0\times378 =$ [Base $(0\times378) + 3$]. This configuration tool provided the manufactures assumes that both the 0×278 and 0×378 addresses are in extended mode, except when the parallel port has a $0 \times 3BC$ address. In the standard SPP mode, the checking process is performed only when the address has a $0 \times 3BC$ address. Although code composer provides the best performance in ECP + CPP mode, unlike the official manual, SPP mode does not support it properly. This is because the SPP mode does not support addresses higher than [Base + 3], whether SPP4 or SPP8. Therefore, USB-to-Parallel converters are expected to be developed to support EPP extension mode normally.

VI. SUCCESS SIMULATION WITH PROPOSED CABLE

As a result, the cause of the error is a problem with the configuration tool itself provided by the manufacturer, and occurs because all parallel ports except for the $0 \times 3BC$ address are recognized as extended mode by default.

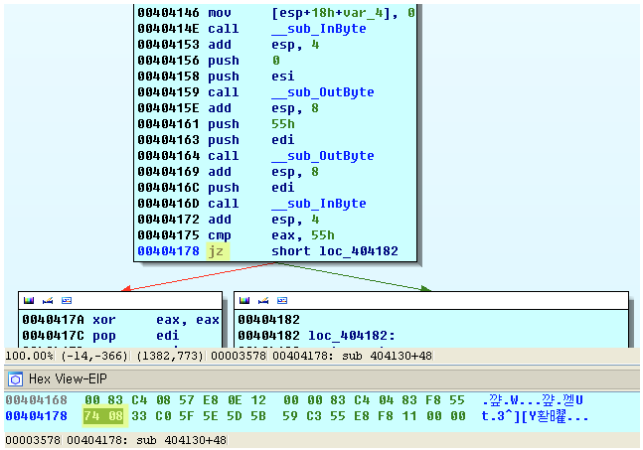


FIGURE 10. Bypassing errors in the EPP mode inspection process (jnz → jz).

In order to continue conducting these experiments, it is necessary to bypass parts where errors occur during the EPP mode inspection process. To this end, as shown in Fig.14, the jnz (Jump if accumulator Not Zero: 0×75) command code is replaced with jz (Jump if accumulator) in the branch statement in order to ensure that the check result of the [Base + 3] address returns False. Zero: 0×74). It is confirmed that the 0×378 address of the parallel port, which is the subject of experiment in this paper, does not support EPP mode, so even if patched like this, it does not affect the original operating flow of the program.

If you run the procedure again after the patch, you can confirm that it is being performed normally, and as a result of the inspection, the 0×378 address was searched in SPP4 mode.

Based on the search results, the address 0×378 can be designated as a parallel port for Code Composer (-p option). The address of the port to be used has been fixed. However, in the process of testing the status of the parallel port (-s option), a system error occurs again. The result of the recognized state should be saved in the configuration file and the Sdiont driver configuration should be completed based on this, but it stops again due to an error.

As a result of analyzing the code, it can be seen that this error occurs when data is written to the address $0 \times 37B$ = [Base$(0 \times 378) + 3$] during the process of testing the status of EPP mode. This configuration tool considers both 0×278 and 0×378 addresses to be in extended mode, except when the parallel port indicates the $0 \times 3BC$ address. SPP standard mode is performed only when it has an address of $0 \times 3BC$. Although Code Composer is said to provide the best performance in ECP+EPP mode, unlike the official manual, it does not properly support SPP mode. This is because SPP mode does not support addresses longer than [Base + 3], whether SPP4 or SPP8.

Therefore, the USB-to-Parallel converter must apply the above bypass method to properly support the EPP expansion mode. By applying the process in Fig. 19 newly proposed

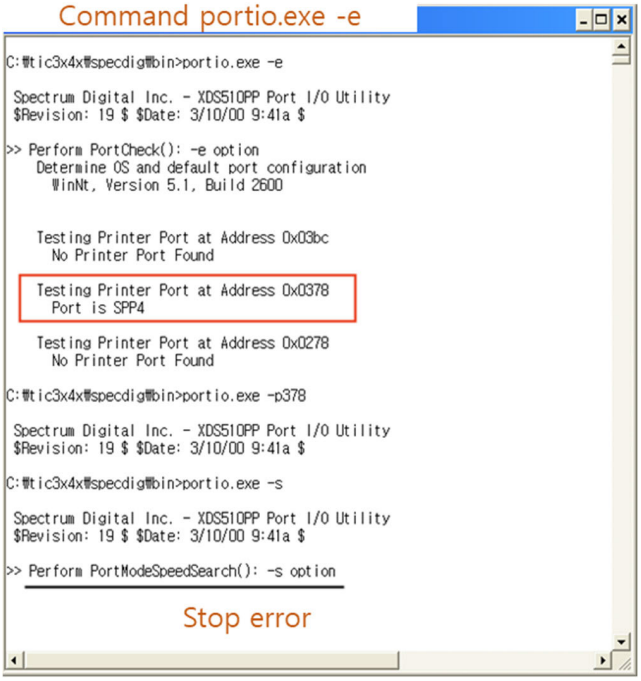


FIGURE 11. An error occurred while testing the status after successfully searching for the LPT's parallel port.

in this paper and applying the bypass technique described above, the final result is a successful connection.

As shown in Fig. 13 the statement that checks the $0 \times 3BC$ address in the code was modified to address 0×378, allowing the status test for SPP mode to be performed. In this way, the execution error was eliminated, but the mode test ultimately failed as shown in Fig. 14. Judging by the fact that the error code value of the SCIF Error item is not 0, it can be assumed that an input/output error has occurred.

SCIF (Sensor Controller InterFace) in Fig. 14, is a term that refers to the input/output driver for TI's Sensor Controller Studio. As the technology was transferred to SD, it is presumed that this configuration tool was redefined as sdiont, which indicates errors in the operation of the driver. It is expected to be a code.z

In the early stages of the test, you can see that the driver handle is obtained by calling the link of the sdiont device driver as shown in Fig.15. For analysis, the code was traced back from the point in Fig.16, where error code -145 (0xFFFFFF6F) was returned, and the code portion shown in Fig. 17, 19 was confirmed.

The important branching points in the above code are three code parts. Since 1 (True) cannot be returned, it can be seen that the following three conditions must be satisfied in order to avoid generating the error code.

1) The value of the first read [Base(0×378)+1] address is A.
2) Based on the Base(0×378) address, write 0×87 and read back the value of the address of [Base(0×378) + 1] as B,

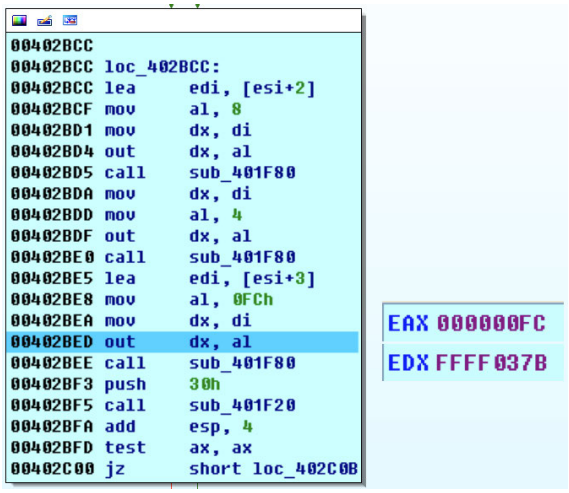


FIGURE 12. Error points in the process of testing the extended mode status of the parallel port.

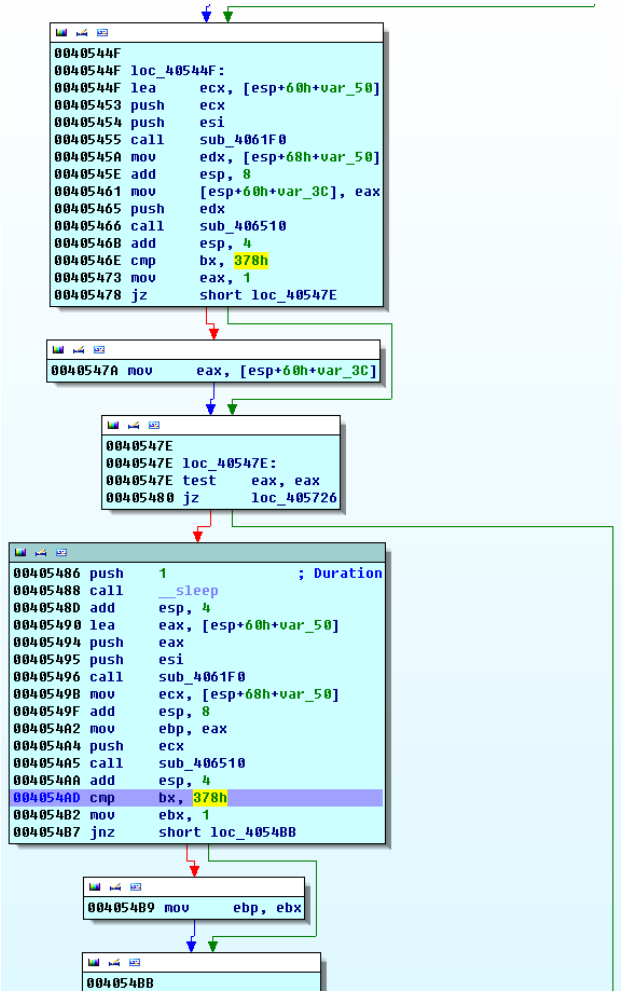


FIGURE 13. Bypassing errors during health testing ($0 \times 3BC \rightarrow 0 \times 378$).

3) When 0×78 is written in the Base(0×378) address and the value of the re-read [Base(0×378) + 1] address is C.

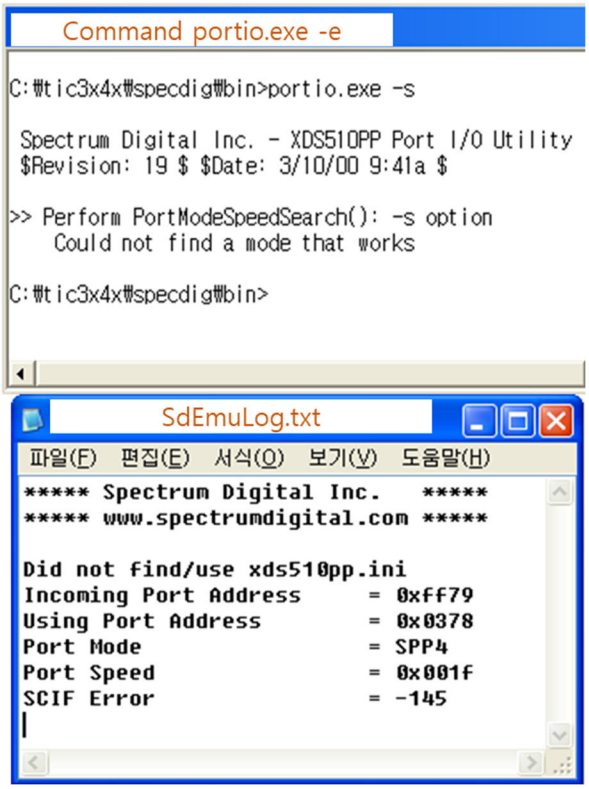


FIGURE 14. LPT parallel port status test error bypass results and status test log.

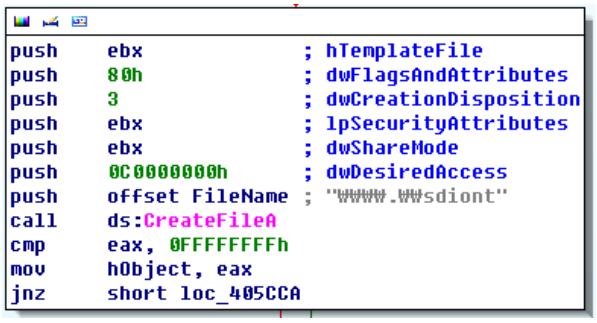


FIGURE 15. Sdiont device driver call.

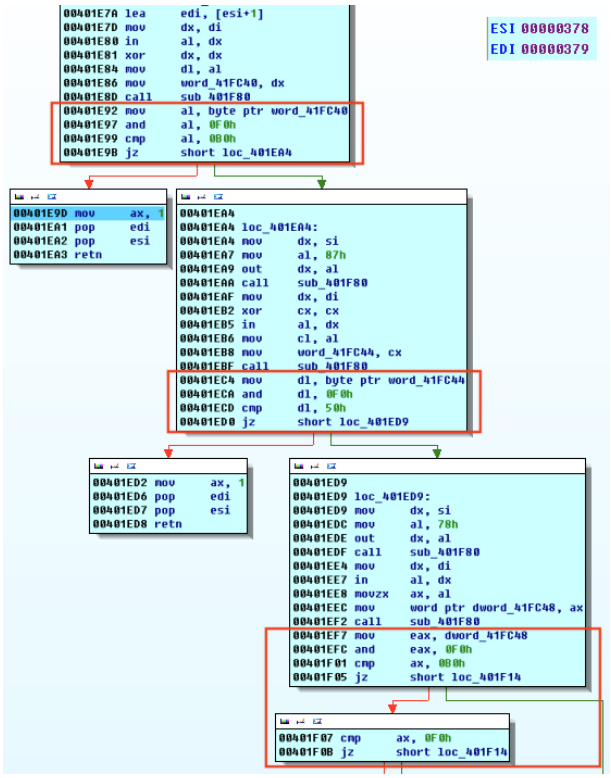


FIGURE 16. Root point that generates error code (−145).

4) Condition: A&0xF0 == 0xB0, B&0xF0 == 0 × 50, C& 0xF0 == 0xB0 || C&0xF0 == 0xF0.

Because replication is required for scientific progress, papers submitted for publication must provide sufficient information. A cable was developed to satisfy these proposed magnetic conditions. If all errors in the detailed processes above are satisfied and the portio.exe -e command is executed, it will ultimately succeed.

VII. POTENTIAL VULNERABILITY OF ACCESS CONTROL WITH AUTHENTICATION

With the XDS510PP-MPSD controller interface, you can read or write the program of the target device, compare it with the source program, debug it, monitor the register, the value of the specified memory area, and the variable value. As such, the XDS510PP-MPSD controller interface provides a robust feature for target devices, which should be more importantly managed from a security perspective. The XDS510PP-MPSD controller interface, which provides robust functionality to the target device, needs to be physically / logically accurately identified. Since the interface with a certain format called MPSD can access the target device all without special restrictions, these controller interfaces must be identified and managed by the operator. TI's C3x and C4x DSPs use the XDS510PP-MPSD controller interface to significantly increase the outflow of information in various I/O access processes. Therefore, it is necessary to establish reliability at the device level through authentication management of the XDS510PP-MPSD controller interface. In general, interface authentication will be one that accepts authentication requests and issues and tracks authentication tokens.

Whether or not authentication is actually granted will be determined by the interface acknowledgment service of the debugger system. In terms of security, the relationship between the XDS510PP-MPSD controller interface is shown as a target device that has information and is controlled by the target device, and an operator who requests access to the target device is an operator who operates the Code Composer or the CC. And that the access rights Code Composer requests

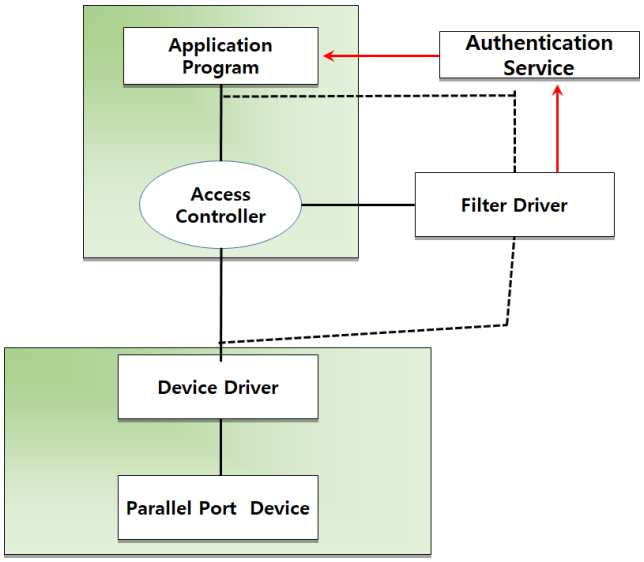


FIGURE 17. System device access control modeling.

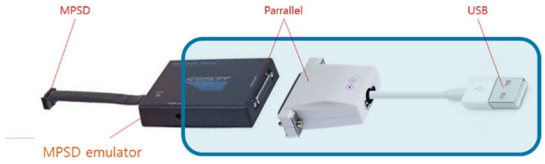


FIGURE 18. Developed cable.

to the target device is a function of the XDS510PP-MPSD controller interface. It is necessary to classify the XDS510PP-MPSD controller interface functions as access rights in order to maintain an appropriate level of control so that access control to target devices is not excessive or under-controlled. The problem can also be solved by applying the access control technology from the S/W point of view.

Access to device devices after the introduction of the Windows NT family is done through the device driver. Parallel port device access is handled by the parallel port driver, and effective access control techniques can be implemented by blocking access to the driver as shown in Fig 10. The access control module operates between the device driver and the application program and acts as an input / output manager. It is also called a filter driver, because it has the ability to monitor and modify I / O requests to existing drivers. In order to authenticate the user, a password input window is opened and the driver is allowed to be accessed when authentication is successful.

The filter driver can be roughly divided into Class Filter, Device Filter, and Bus Filter, and each of them can be divided into two categories according to the installed position. The Class Filter is loaded when all the drivers are loaded into a given class, allowing filtering on drivers of all classes. The filter drivers installed in this location are only affected by the Class and are loaded together when other drivers of the desired Class are loaded, regardless of the hardware ID, the manufacturer, and even the Bus Type. Since the Device Filter is a filter driver that is installed only in a specific device node, it can be filtered only for a desired device. Bus Filter is a filter that can be filtered for a specific bus driver. The Upper Filter is used to receive and filter I/O requests before the driver to be filtered. On the contrary, the Lower Filter is used to filter I/O requests that are processed by the driver to be filtered. Considering this functional requirement, it is considered that the production of the filter driver based on the device filter and the upper filter is most effective.

These methodologies are described in detail process in Fig. 10. The solution is the first research approach and result internationally., and the value of this proposed scheme is high and unique. If this proposed method is not applied, comparability and security issues would not be solved even if a commercially available parallel port to USB cable is purchased. Because this could not be connected to wanted systems. Fig.10 describes the proposed overall methodology, and the detailed technic procedure is shown in Fig. 12. In addition, by applying and implementing this scheme, a special purpose cable as shown in Fig. 11 has been developed. With this research result, the conundrum described in this paper could solved.

VIII. CONCLUDING REMARK

Operating control system in infrastructures including NPPs have mostly been composed of legacy systems. Thus, there could be many compatibility vulnerabilities with the recent system. The processor core of the control system used in APR 1400 is also an old component and has a problem in compatibility with the use of development and debugging interface. In this regard, this paper discovered vulnerabilities of compatibility and access control which have not been found yet, and analyzed the causes of the problems and presented the countermeasures.

XDS510PP-MPSD is an important product used in the development and maintenance, accident investigation of important controllers of nuclear power plants. Code Composer, as the debugger software used in the controller interface of this product, is operating with an integrated development environment (IDE) that supports the TMS320C30/C31/C32 DSP (Digital Signal Processor) development environment. After being released in 2001, there are no further version upgrades. It's not progressing. Therefore, the computing environment for interconnected use is still available only for low-end and older interfaces with old computer system. In particular, laptops and computers that support Parallel port, the communication interface used exclusively for Code Composer, have already been discontinued, and Windows XP, a compatible operating system, has also been discontinued, making installation difficult in recent computer environments. Critical systems operated in industrial facilities have a life cycle of decades and cannot be easily

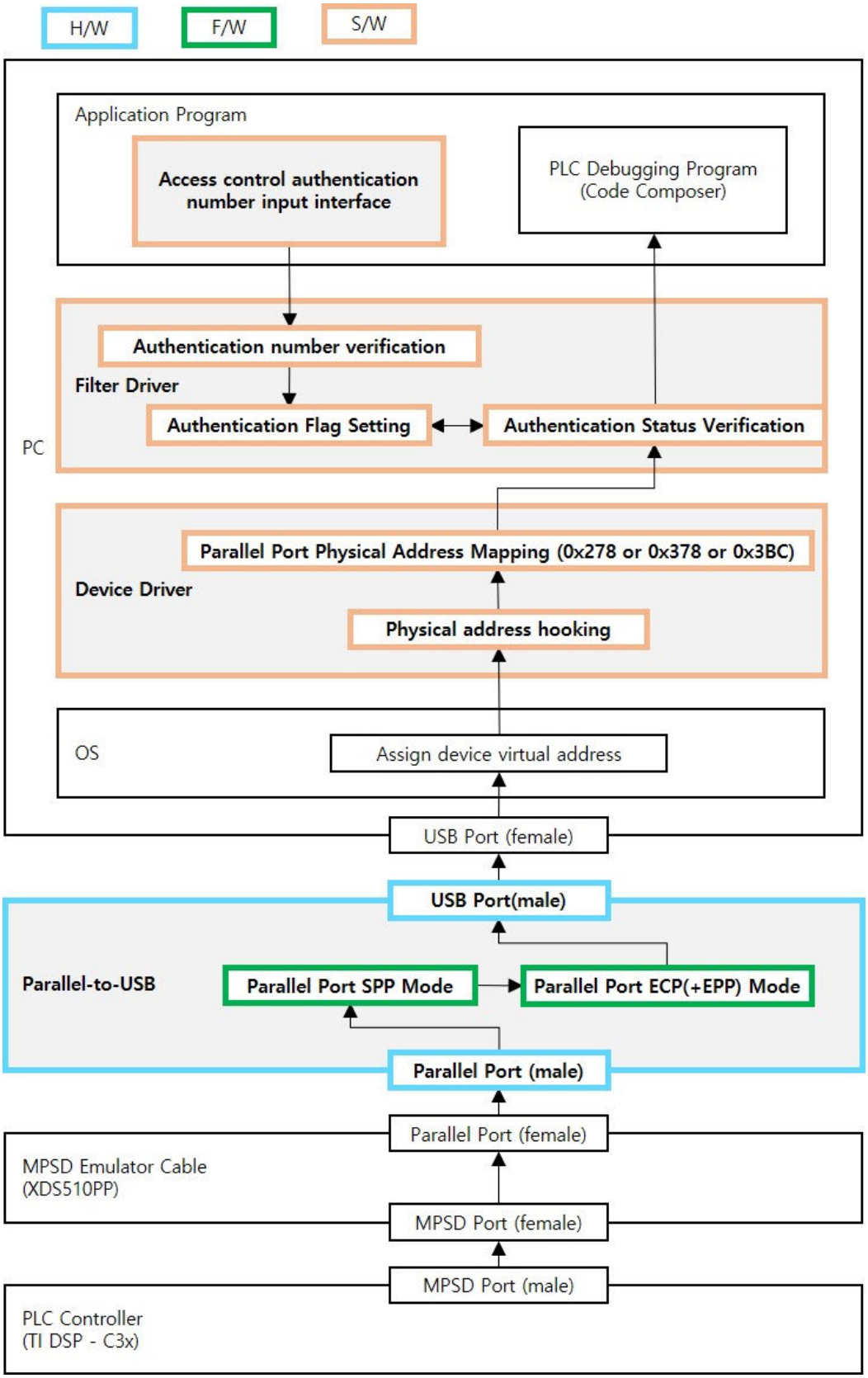


FIGURE 19. Proposed solution process description.

changed due to regulatory systems or various regulations. Because of this, industrial facility operators must continue to utilize the systems that are already installed and in operation. Therefore, the need to resolve the compatibility and security issues discovered in this paper is an important issue. This paper studied approaches to solve the problem from two perspectives. The first is a plan to convert the widely used USB interface into a parallel interface. The second is a plan that can be operated in an operating system environment of Windows NT 6.1 (Windows 7) or higher. As a result of analysis and experiment, simple interface conversion is possible when using a USB-to-Parallel converter, but it must be developed to support ECP+EPP mode rather than for simple printer parallel port use, and the network address must be developed to have an actual physical address. And the target converter must be able to respond to all test processes performed by the configuration tool. Since the Code Composer driver is a verification and setup process for safely connecting to a PLC, the development of a dedicated converter to support this is necessary. Therefore, in this paper, we developed a dedicated converter and succeeded in developing it as described in the main text. In addition, as a result of testing the product developed using the method proposed in this study by upgrading the operating system environment to Windows 7, it was eventually able to be successfully implemented after overcoming various limitations.

Through this study, problems with compatibility and security for existing systems using the TMS320C32 CPU Core were solved for the first time in this paper. The results of this study will be used not only in nuclear power plants, but also in various fields that utilize the TMS320C32 CPU Core, such as automobile noise control, aviation equipment, train control equipment, turbine systems, aerospace, UAV(Unmanned Aerial Vehicle) and other industrial facilities.

REFERENCES

[1] *U.S Nuclear Regulatory Commission, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, Regulatory Guide 1.152, Revision 3*, U.S. Dept. Energy, Washington, DC, USA, Jul. 2011.
[2] *U.S. Nuclear Regulatory Commission, Cyber Security Programs for Nuclear Facilities, Regulatory Guide 5.71*, U.S. Dept. Energy, Washington, DC, USA, Jan. 2010.
[3] *Kinac RS-015 Rev 01*, Kinac, South Korea.
[4] *Kinac RS-019 Rev 00*, Kinac, South Korea.
[5] *KINAC/RR-007/2015, Nuclear Security & Cyber Security Division 2014 Annual Report*, Kinac, Jan. 2015.
[6] *SM320C32-EP Digital Signal Processor, SGUS038*, Texas Instrum., Dallas, TX, USA, Aug. 2002.
[7] *TMS320C32-EP Digital Signal Processor, SPRS027C*, Texas Instrum., Dallas, TX, USA, Jan. 1995.
[8] *TMS320C32-EP Digital Signal Processor, SPRS027C*, Texas Instrum., Dallas, TX, USA, Jan. 1995.
[9] H. Cai and J. Qiao, "A sonar signal processing system based on TMS320 series," in *Proc. OCEANS*, 1994, pp. II/556–II/561.
[10] L. Khan and W. Scott, "320C3x, 320C4x, and 320MCM42x, power-up sensitivity at cold temperature," Texas Instrum., Dallas, TX, USA, SGUA001D, Appl. Rep., Aug. 2004.
[11] *Spectrum Digital, XDS510PP Plus Parallel Port JTAG Emulator Installation Guide, DSP Development System*, 2005.
[12] *JTAG/MPSD Emulation Technical Reference*, Texas Instrum., Dallas, TX, USA, 1994.
[13] *Security for Industrial Automation and Control System—Part 4-1: Secure Product Development Lifecycle Requirements*, Standard IEC 62443-4-1, IEC, Jan. 2018.
[14] "Security requirements for cryptographic modules, NIST, FIPS 140-2, category: Computer security," U.S., Tech. Rep., May 2001.
[15] *IEEE Standard for System and Software Verification and Validation*, IEEE Standard 1012-2012, IEEE Computer Society, May 2012.
[16] *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*, IEEE Standard 7-4.3.2-2003. 2003.
[17] "Computer security at nuclear facilities," Int. At. Energy Agency, Vienna, Austria, IAEA Nucl. Secur. Ser. no. 17, 2011.
[18] *Conducting Computer Security Assessments at Nuclear Facilities*, IAEA, Vienna, Austria, 2016.
[19] Y. C. Shin, H. Y. Chung, and T. Y. Song, "Advanced MMIS design characteristics of APR1400, GENES4/ANP2003," Paper 1066, Sep. 2003.
[20] M. K. Lee, S. W. Song, and D. W. Yun, "Development and application of POSAFE-Q PLC platform," IAEA, Vienna, Austria.
[21] *IDA Pro*. [Online]. Available: https://hex-rays.com/ida-pro/
[22] Z. Wang, Y. Zhang, Y. Chen, H. Liu, B. Wang, and C. Wang, "A survey on programmable logic controller vulnerabilities, attacks, detections, and forensics," *Processes*, vol. 11, no. 3, p. 918, Mar. 2023.
[23] A. Ayub, N. Zubair, H. Yoo, W. Jo, and I. Ahmed, "Gadgets of gadgets in industrial control systems: Return oriented programming attacks on PLCs," in *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST)*, May 2023, pp. 215–226.
[24] J. Son, J. Choi, and H. Yoon, "New complementary points of cyber security schemes for critical digital assets at nuclear power plants," *IEEE Access*, vol. 7, pp. 78379–78390, 2019.
[25] J. Son, T. Tak, and H. Inhye, "Modeling cryptographic algorithms validation and developing block ciphers with electronic code book for a control system at nuclear power plants," *Nucl. Eng. Technol.*, vol. 55, no. 1, pp. 25–36, Jan. 2023.
[26] S. Gaurav, A. Kumar, and V. Sharma, "Windows operating system vulnerabilities," *Int. J. Comput. Corporate Res.*, vol. 1., no. 3, p. 13, Nov. 2011.
[27] [Online]. Available: https://www.cvedetails.com/product/739/Microsoft-Windows-Xp.html?vendor_id=26

JUNYOUNG SON (Member, IEEE) received the Ph.D. degree from the Graduate School of Information Security in Computer Science, Korea Advanced Institute of Science and Technology (KAIST). He is currently a Senior Researcher with the Korea Atomic Energy Research Institute (KAERI), researching on nuclear cyber security. He was a Researcher with the National Security Research Institute (NSRI), from 2009 to 2012. He was a Senior Researcher and an Auditor with the Korea Institute Nuclear Safety (KINS), from 2013 to 2017. He has been a Senior Researcher of cyber security and system software, anti-drone, and cyber electronic warfare with KAERI, since 2017.

HEEMAN PARK (Member, IEEE) received the Ph.D. degree from the Graduate School of Information Security, Chonnam National University (CNU). He is currently a CEO with VARN Inc. He was an Associate Research Engineer with the System Security Laboratory, CNU, from 2004 to 2011; and the Information Industry Research Institute, Mokpo National University, from 2011 to 2013. He has been a CEO with VARN Inc., since 2012. He has been a member of the Evaluation Committee of the Institute for Information and Communications Technology Promotion (IITP), since 2017.