# Trusted Processor: A Result of the Evolution of Information Barrier Technologies

Vyacheslav Kryukov, Pavel Talantov, Vladimir Sotnick, Ilya Yurovskikh
All-Russian Research Institute of Theoretical Physics (RFNC-VNIITF) named after
Academician E.I. Zababakhin, Snezhinsk, Russia

Keith Tolk
Sandia National Laboratories, Albuquerque, New Mexico, USA

## Abstract

Sandia National Laboratories (SNL) has previously developed a trusted processor (TP) for use with radiation identification technologies utilizing information barrier applications. Based on prior experience, including that gained via the evaluation of the SNL TP, VNIITF has been developing its own TP. The design of the VNIITF TP is associated with strict limitations being imposed by the sensitivity of the measurements being made.

A TP design that recognizes the principles of security of sensitive data should also provide evidence for the presence of these functions. At the same time, the TP design should provide for simplicity and technological efficiency of any control operations. This paper will describe the following major technical principles, laid down into the Russian version of a TP during its design:

- non-intrusiveness of TP
- assurance of the reliability and authenticity of data in TP
- transparency of TP
- assurance of the authentication of TP

## Background

One of the problems slowing the development of technologies for verification of fissile material (FM) is the intrusiveness of the potential methods. *Intrusiveness* is taken to mean the ability of methods to obtain sensitive information that, from the standpoint of the objectives of the inspection, is not needed. Various methods and technologies have been proposed to preclude such intrusiveness. Initially, those technologies were envisioned as some device that separates the system for acquiring information from the system for analysis and decision-making. The device was to prevent protected information from getting to the analyzer, since it was located between the measuring instrument and the analyzer. The basic flaw of such an approach involves the need to provide a careful balance in terms of the information being kept and the information being filtered out — the more information that remains in the stream, the more potentially intrusive the system becomes. At the same time, excessive filtration results in a sharp drop in the reliability of the results of the inspection, which is also unacceptable.

An alternative approach relies on the fact that the final result of the processing of the measurements, expressed in the form of one bit of information, yes/no, in the sense of being an answer to the basic question of the inspection, is not intrusive. For that reason, if the

Sandia National Laboratories is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy’s National Nuclear Security Administration under contract DE-AC04-94AL8500.

procedure for processing and analyzing the measured data is completely automated and only the final result is given, then the fundamental dilemma associated with the technologies for verification of FM is resolved — all the data are subjected to analysis, which guarantees that the result of the verification will have a high level of reliability, and the information given out is kept to a minimum, which guarantees the non-intrusiveness of the technique. Thus, the measuring system now has a device that must process the measured data and generate an output in the form of one bit of information. The personnel who take part in the procedure for FM verification must trust both the device and the results obtained with it. For that reason, such a device is called a "trusted processor," or TP.

Further development of the concept of the TP has made it possible to formulate a number of basic requirements for it. Those requirements consist of the principles of non-intrusiveness, validity, transparency, and authenticity.

***Non-intrusiveness*** consists in the impossibility of the unauthorized disclosure of sensitive information from the system during the performance of the measurements.

***Validity*** consists in the impossibility of sensitive information being distorted in the TP either as a result of the TP being purposely compromised via spurious channels to falsify measurement results or as a result of random interference.

The TP's design, which implements the principles of the safekeeping and integrity of sensitive information, must ensure the obvious presence of those qualities via the simplicity and efficiency of all the inspection operations. Those properties of the processor are manifest in the principles of transparency and authenticity.

***Transparency*** consists in the possibility of a full and sufficient understanding of the structural design and the algorithms of operation of any device, as well as its functional characteristics, so as to increase the trust in that device to the level at which it is acceptable for use.

***Authenticity*** consists in the conformance of a given device to an agreed-upon reference standard, and to it only.

## Ensuring the Non-intrusiveness of the Trusted Processor

The emissions of electronic and computer devices are modulated by the legitimate signal and are propagated both conductively and in the form of emitted electromagnetic interference (EMI). Spurious emissions and conducted interference create information leakage channels, against which both active and passive methods are used. Active methods for protecting information are geared to creating masking EMI. In terms of the procedures for the use of the TP, the presence of any extraneous emitting device clearly lowers the degree of trust in the design of the processor, and for that reason, active methods cannot be used. Passive methods for protecting information include measures to suppress parasitic oscillations (sources of spurious emissions), the shielding of equipment, and the filtration of conducted signals.

***Suppression of sources of spurious emissions*** is accomplished with an optimal design of electrical circuits and layout of printed circuit interconnections.

***Shielding*** is a structural means for attenuating any emissions and, in practical terms, confines electromagnetic energy created by a field source.

***Filtration*** is the principal means for attenuating conducted interference in power-supply and grounding circuits and in interface lines.

Implementing the principle of the TP transparency requires providing easy access to the electronic modules of the processor, which means the processor housing must be sectional. The housing itself, in addition to providing reliable shielding, must accommodate the cooling of the electronics and the input of signal and supply cables and must protect against dust, moisture, mechanical damage, and corrosion. Compliance with most of those requirements makes providing effective shielding difficult. The following is necessary to improve the shielding properties:

- reliable electrical contact between the housing parts (spring-loaded lugs along the perimeter of the cover; elastic, electrically conducting gaskets)
- electromagnetic protection of cable inputs and ventilation openings (connectors with metal sheath, metallized fabric sleeve)

Opening the housing of the TP not only disrupts its shielding function, but, while collecting sensitive information, it should also cause the termination of processor operations and the destruction of all information in the system. Tamper-indicating devices — unauthorized access detectors — are installed at the separation points of the housing. The triggering of an unauthorized access detector during processor operations should reset the hardware, clear the processor memory, and disconnect the measurement unit power. The duration of the processing of the measurement results can serve as an indirect indicator of the isotopic composition of the FM sample being measured. To eliminate that factor, the result is displayed after a fixed time interval, regardless of the real time of data processing.

## Ensuring the Validity of the Information in the TP

The personnel who take part in the verification of FM must be confident that the results of the sensitive information processing in the TP cannot be falsified. The probability of falsification is linked to the possibility of the existence of so-called hidden switches in the processor. The term *hidden switch* is taken to mean anything that could selectively affect the results of the measurement of the FM characteristics. A system with a hidden switch could provide accurate results during calibration and testing with known samples, yet give false results while in actual use. The hidden-switch problem is divided into two components:

1. the presence in the TP of hardware or software for altering a result of the processing of the sensitive information
2. the existence of a hidden control channel for initializing such hardware or software

In analyzing the hardware and software of the processor for the absence of hidden switches, one must inspect the structure of the hardware and the software to a smallest indivisible component. For the software, this is the processor command to which the assembly language instruction clearly corresponds. If there is comprehensive documentation on the software being used, the software switches are unavoidably detected. The presence of comprehensive documentation for the hardware of the processor does not guarantee the absence of hardware-based hidden switches, since the actual combination of the silicon structures of the electronic components is not reflected in accessible documentation; also, even if there were such documentation, it could not be quickly authenticated. In the extreme case, the problem of hardware-based hidden switches can be formulated as follows: ***all electronic components potentially have undocumented properties that make it possible to affect, in the modules of a legal TP, a "shadow processor." The shadow processor is initialized via a hidden control channel, and is capable of monitoring and adjusting the result of program execution in the processor. Exchange of information between the processor units can be done both via the processor's internal buses and via a wireless link.***

The following are examples of measures that can be taken to ensure trust in the hardware part of the processor:

- Use publicly accessible electronic items acquired on the free market from different makers.
- Use microelectronic components that are identifiable when they are part of the system and that support the IEEE 1149.1 boundary-scan standard (JTAG), to enable non-destructive testing of the processor.

Those measures still cannot fully guarantee the absence of hardware-based hidden switches. For that reason, under the assumption that the electronic components of the processor could potentially contain them, it is necessary to use design to ensure the impossibility of the initialization of hidden switches.

Protecting the processor against hidden control channels can be passive or active. Active methods create noise masking in the ranges of the physical fields where the hidden control channel is presumed to be. As with active methods for protecting information, these methods clearly evoke a lack of trust among the personnel who are conducting the verification of FM, which is why they cannot be used. Passive methods of protection include placing the processor in housing that shields it from any physical field that is a transmitting medium for a hidden control channel.

The TP may include different types of detectors that control the volumetric space inside the processor housing. A detector event indicates the possible initialization of a hidden control channel and must automatically cause a hardware reset of the processor, along with the destruction of all sensitive information, as with the tamper-indicating device for the processor housing. Such detectors can be regarded as tamper-indicating devices with expanded functions.

## Ensuring the Transparency of the TP

An analysis of the transparency should consider the following:

- the principle of operation of the system as a whole and of the interrelationship among the components
- the structural design of the system as a whole and of its components, to the level of the smallest indivisible component

- the smallest indivisible component
- the software

The transparency of the TP’s structural design is facilitated by the following conditions:

- the presence of comprehensive design documentation that is supported by the in-house development of the TP modules
- the use of a sectional housing that enables one to see the location of the electronic modules of the TP and the links between them, and ease of installation/removal of the modules
- provision of access with test equipment to the electronic modules without having to place them on an extension or removing adjacent modules; authentication of the operation of the TP modules can be done without altering the status of the system
- the use in the modules of only two-layer printed circuit boards that ensure the transparency of the conductor paths without the use of additional measures (x-ray analysis of the inside layers of multilayered printed circuit boards)

To ensure the transparency of the structural design of the TP, there should be a correspondence between the structural element with a minimum set of functions and a separate electronic module. Figure 1 shows the block diagram of the TP, and Table 1 presents the correspondence between the processor function and the module that performs that function.

The transparency of the TP’s software is facilitated by adherence to the following conditions:

- the presence of full documentation for the software; this condition is ensured by abandoning the use of operating systems and orienting oneself on the in-house development of software
- minimal size of software; to manage the resources of the TP and the connected measurement equipment, a monitor/program is developed that performs necessary functions only
- uniqueness of compilation of the software source terms; this condition is ensured by the use of an assembler as the programming language

**Table 1**

| | Processor function | Module |
|---|---|---|
| 1 | Control of the TP/display of result | Control panel/display |
| 2 | Control of the measurement devices and processing of the measurement results | Computational module |
| 3 | Monitoring of access to the inside of the TP's housing (unauthorized access detectors), tracking of potential hidden control channels (signal detectors) | State-of-health monitoring module of processor |
| 4 | Link with measurement equipment | Input/Output module |

## Ensuring the Authenticity of the Trusted Processor

Authentication is a check to determine that a system conforms to some reference standard. The ability to authenticate a system involves the ability to perform such a check before, during, or after the measurement of the FM characteristics. The duration of the authentication procedure and the cost to perform it must be minimal.

During system authentication, the validity of the following assertions needs to be determined:

1. The system has been designed for proper operation.

2. The system conforms to the design.

3. System functioning conforms to the design.

The check of assertions 1 and 2 is facilitated by implementing the principle of the transparency of the TP's hardware and software.

Validating the system functioning of the TP is to be done in two modes: in the established terminology, that would be "open" and "closed" mode. In open mode, radiation measurements are tested both from a panel and a connected personal computer on reference sources that have known characteristics. On the control computer, it is possible to obtain detailed intermediate results of the measurements. Also, the open mode accommodates testing of the electronic components of the processor modules by means of a JTAG boundary scan. In open mode, tamper-indicating devices function to ensure their inspection, but the reset function of the processor's computational module is blocked.

The closed mode corresponds to measurements of the FM sample being tested. The link to the personal computer is blocked, and the triggering of any tamper-indicating device results in the reset of the computational module of the TP, along with the destruction of sensitive information in the module memory and the disconnection of the power to the measurement equipment. The impossibility of a hidden changeover of the TP from closed mode to open mode is ensured by implementing the hardware reset of the processor when the mode changes.

After the authentication of the system is completed, seals or other tamper-indicating devices must be applied to the TP's housing.

## Requirements for the Computer Resources of the TP

In terms of functions performed, the TP's software can be divided into two fundamental sections: the controlling program (monitor) and programs for processing measurement results.

The monitor is a complex of subprograms that perform the functions of controlling the measurement equipment, executing the commands of the control panel and/or controlling computer, and displaying the results. Those functions do not require appreciable computational costs. The main contribution to the resource intensity of the processor tasks is made by the programs for processing the results of the spectrometric measurements, in which the presence and quality of the FM in the sample under study are determined from the location of the characteristic peaks of the gamma spectrum of the FM.

The stage for processing the measurement results has the following requirements:

- Issuing the final non-intrusive result must have a fixed time, including the real time for processing and the delay in display.
- The sensitive information in the measurement equipment and TP must be destroyed after the final non-intrusive results are prepared.

From an analysis of the TP functions, it follows that the computational module's processor must have the following characteristics:

**1. For interaction with external equipment and the control panel:**

- a timer for controlling the stages for the performance of measurement procedures
- a serial port for linking to the panel and/or the controlling computer
- a parallel port for linking to the input/output module

**2. For implementation of the computational resources requirements:**

- support of operations involving 32- and 64-bit data in floating-point format
- speed of at least 100 MFLOPS

**3. For ensuring specific properties of the TP:**

- support of the IEEE 1149.1 boundary-scan interface (JTAG)
- location in a flat pack (PQFP, TQFP) for installation on a two-layer printed board of the computational module
- use of a low-frequency oscillator to reduce the leakage on the board (the internal multiplication of the frequency is performed in the processor synchronization unit)
- the processor's supply voltage must not exceed 3.3 V in order to ensure reduced energy consumption and heat generation

Based on the above requirements for the computational module's processor, ways of implementing the TP with the mode widely used and accessible types of electronic devices were examined: digital signal processors (DSP), general-purpose microprocessors, and programmable logic integrated circuits (PLIC).

A **system designed with a general-purpose microprocessor** requires, in addition to the microprocessor itself, the proper chipset to execute the functions of memory management, interrupts, and input/output. The result is a configuration that is largely redundant and less transparent.

**Implementation of the TP on commercial PC-104-type computational modules** involves the use of operating systems. The printed circuit boards of the PC-104 modules are multilayered, and the microprocessor and chipset are in BGA housings, which degrades the transparency of the modules. For that reason, such modules cannot be used in the TP.

The option that best meets the requirements is the **implementation of the TP with PLIC**. A TP based on PLIC makes it possible to ensure to a greater extent the transparency and authenticity of both the software and the hardware. The methods for implementing those requirements are identical — for the software and the hardware, open source terms are in the appropriate programming languages, and the configuration of the hardware and the loading of the software are done with the same media, which simplifies operations for verifying the information contained in them. A shortcoming of the PLIC option is the lengthy period for the in-house development of the TP's nucleus.

Implementing the TP on the basis of DSP, in comparison to the general-purpose microprocessors, is preferable, due to the following DSP properties:

- The size of the internal memory of the DSP enables it to house storage areas that contain the sensitive results of the computations. A feature of the circuits of some DSPs enables them to immediately destroy information in internal memory upon the activation of a certain external signal (without the programmed initialization of memory).
- Phase-locked loop frequency control (PLL) makes it possible to employ low-frequency clock signal generators to reduce EMI without appreciable degradation of the processor's performance.
- A DSP has a minimal set of built-in peripheral functions sufficient to control the TP (such as a serial port for linking to the control panel and external computer, or hardware timers for assigning time intervals for the operation of outside equipment).
- The programming of the duration of the exchange cycle on the external bus of the DSP makes it possible to manage external devices in keeping with their speed.
- The expanded accuracy in the performance of operations with a floating point (40 bits) with the proper organization of computations (storage of intermediate results in the register storage) is sufficient for processing the measurement results.
- Two- and three-operand instructions, parallel performance of operations, hardware repetition of a block of instructions, and the mechanism for performing programmed cycles without overhead ensures a high level of performance for the DSP in the implementation of programs for processing measurement results.

## Conclusion

The development of a TP involves rigid constraints imposed by the specific nature of the task being addressed. The structural design of the TP must not only guarantee the safekeeping and integrity of sensitive information, but must also ensure the simplicity and efficiency of operations involving verification and validation of the information protection function.

The specific requirements for the TP, in comparison with the task of computational processing of information, acquire the status of system requirements. The use of off-the-shelf hardware, such as single board computers, does not satisfy the high-priority principle of system requirements. Implementing a TP requires specialized development.

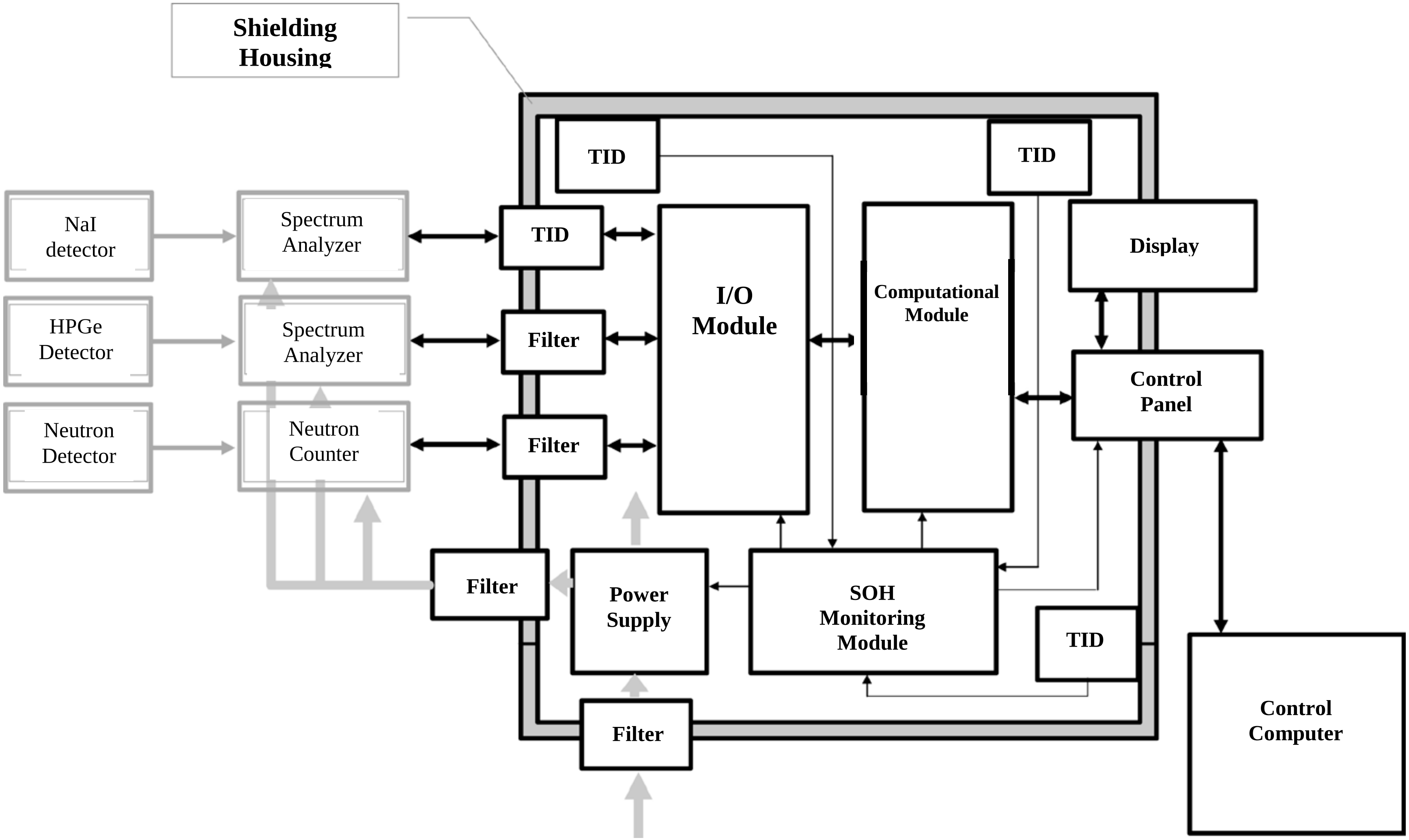

**Figure 1.  TP Structural Diagram**