48th Annual INMM Conference
Tucson, Arizona July 8-12, 2007

SAND2007-3943C

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

Vyacheslav Kryukov, Pavel Talantov, Vladimir Sotnick, Ilya Yurovskikh

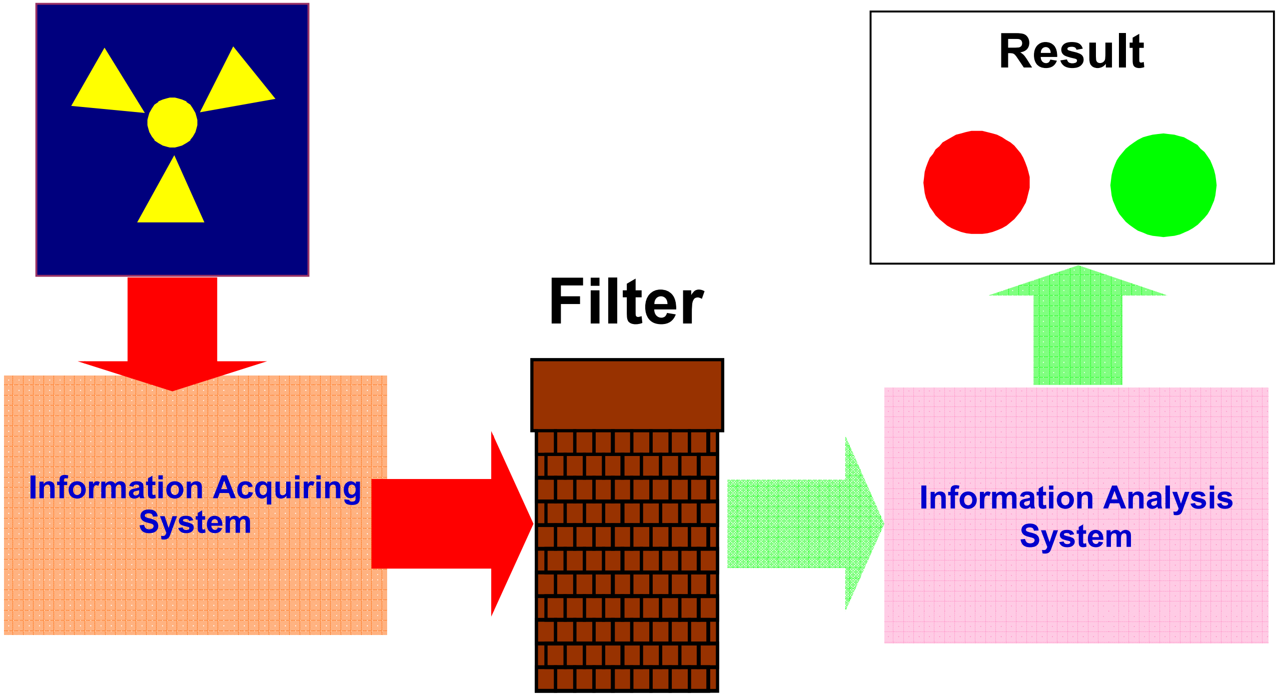
Russian Federal Nuclear Center - All-Russian Research Institute of Theoretical Physics (RFNC-VNIITF) named after Academician E.I. Zababakhin, Russia

Keith Tolk

Sandia National Laboratories, USA

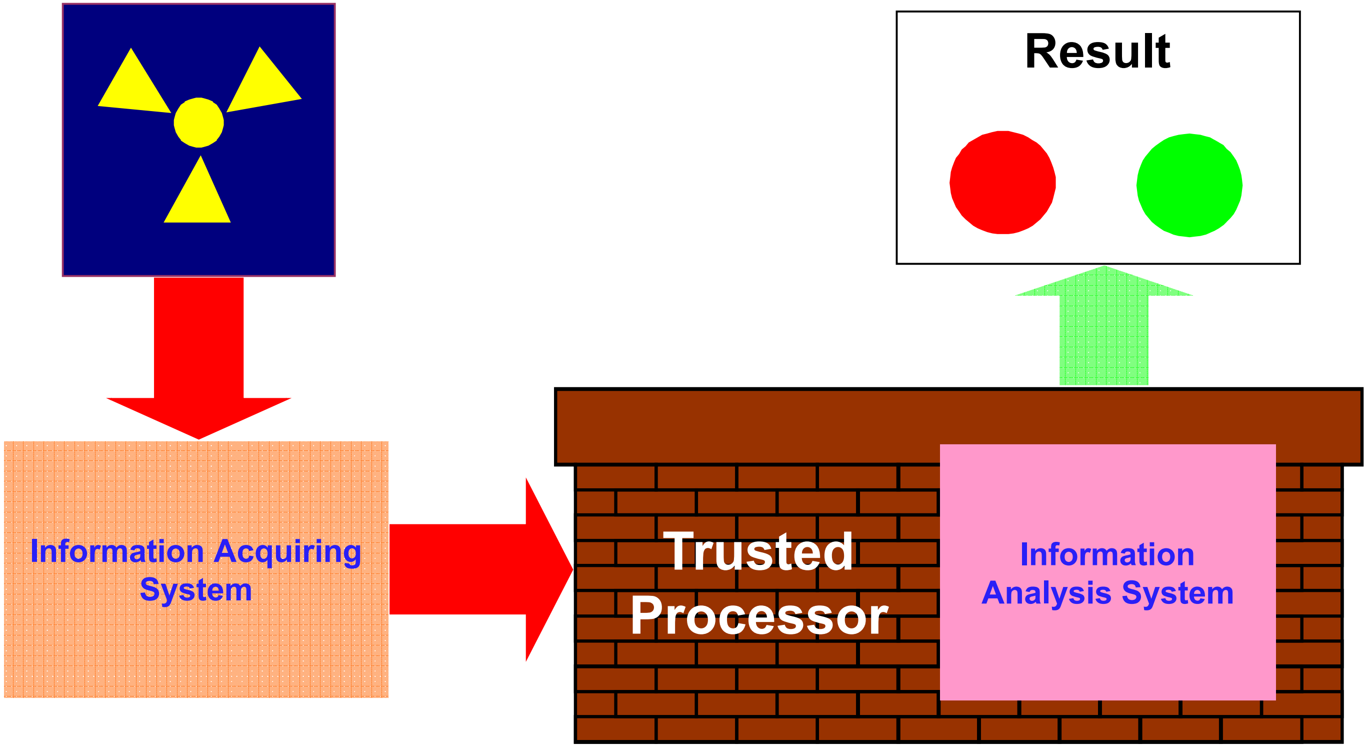
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.

Development of Fissile Material Verification Technologies



The flaw: the need to provide a careful balance in terms of the information being kept and the information being filtered out.

Development of Fissile Material Verification Technologies (cont.)



All the data are subjected to analysis, which guarantees that the ***result*** of the verification will have ***a high level of reliability.***

Trusted Processor Concept

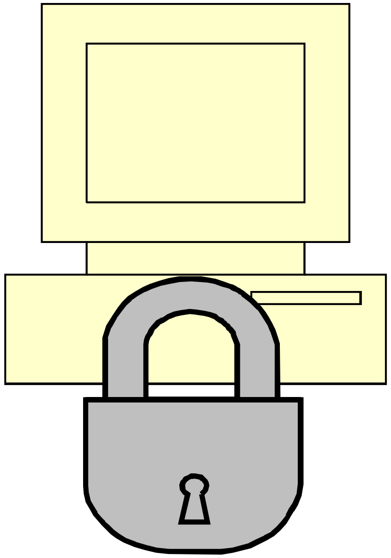
System Requirements for Trusted Processor (TP):

- Non-intrusiveness
- Validity
- Transparency
- Authenticity
- Computer Resources (processor speed, memory size)

Ensuring TP Non-intrusiveness

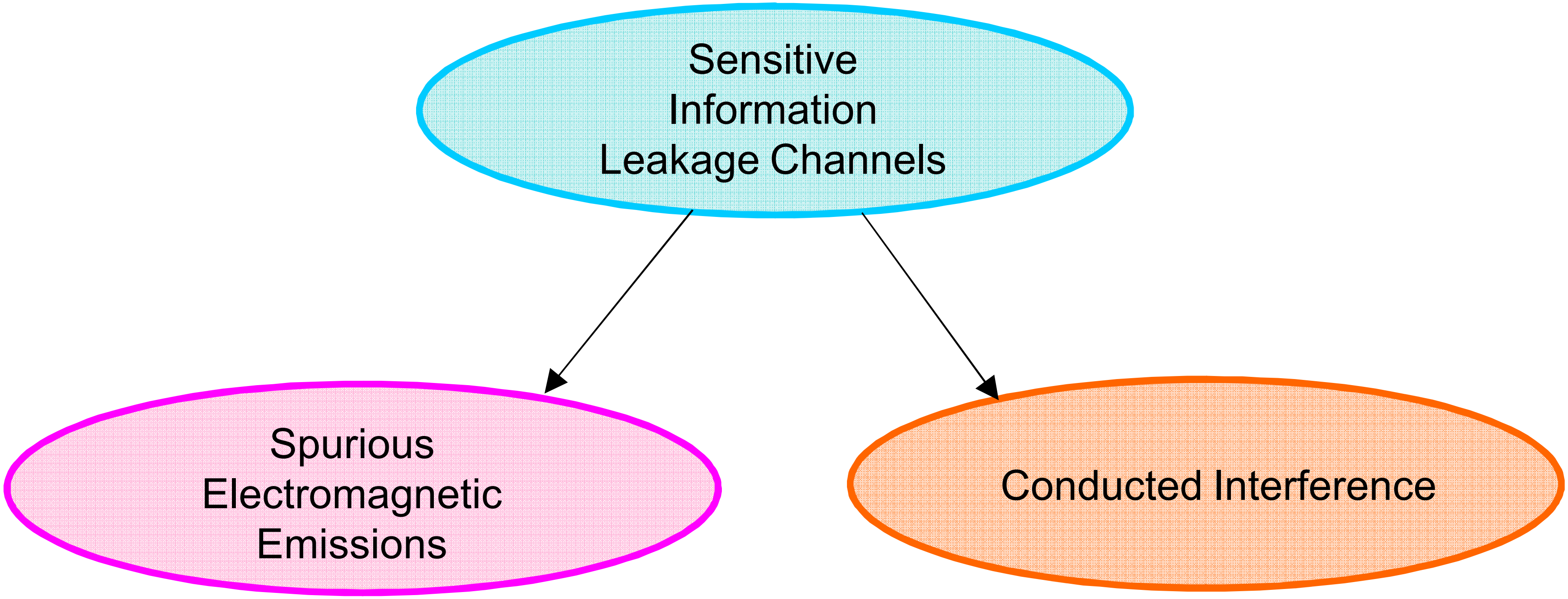
- Non-intrusiveness

  is the impossibility of unauthorized disclosure of sensitive information from the system during the performance of the measurements.



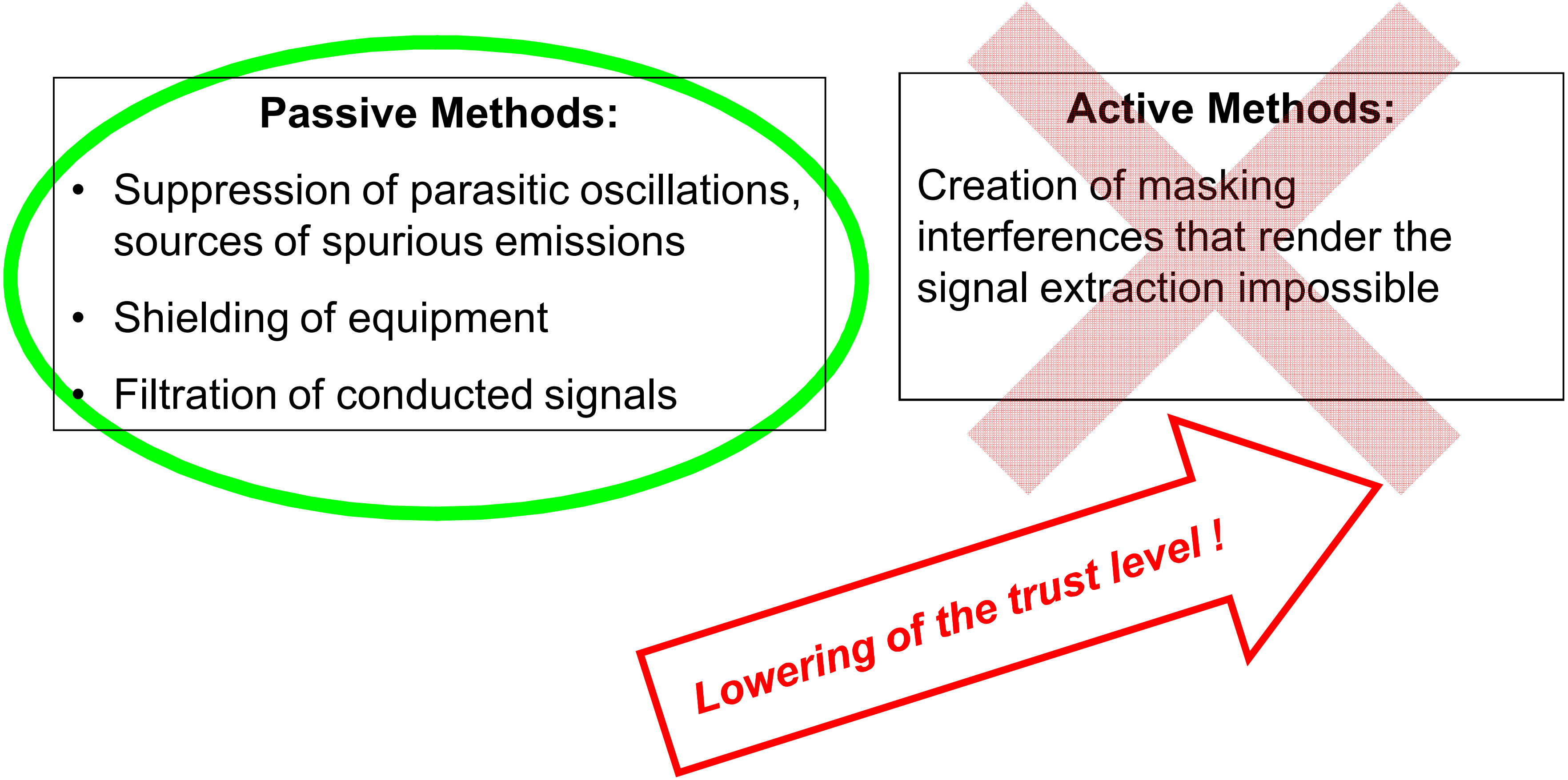
Ensuring TP Non-intrusiveness

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***.


Sensitive Information Leakage Channels
Spurious Electromagnetic Emissions
Conducted Interference

Ensuring TP Non-intrusiveness

Methods of controlling information leakage channels



Passive Methods:

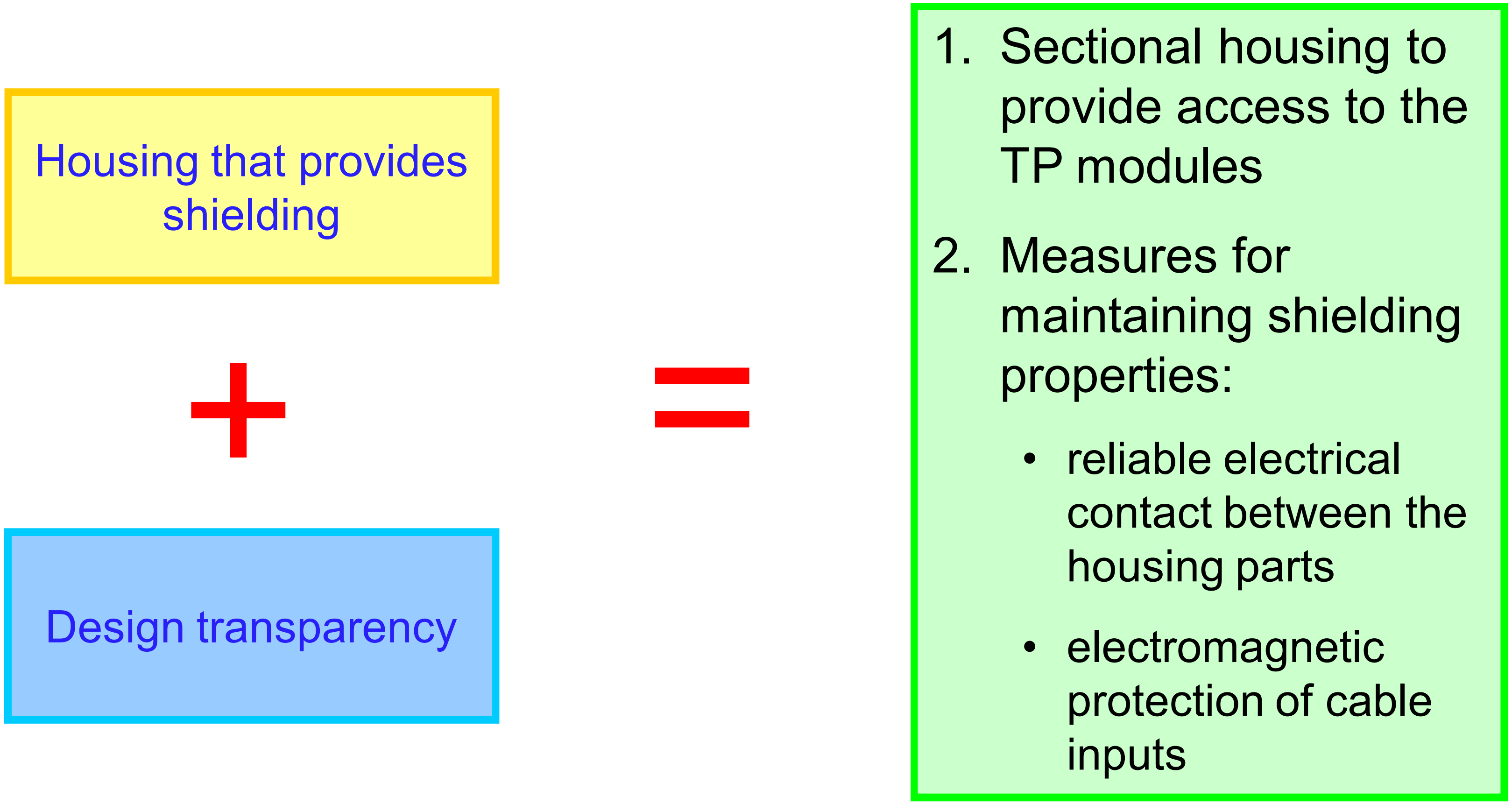
- Suppression of parasitic oscillations, sources of spurious emissions
- Shielding of equipment
- Filtration of conducted signals

Active Methods:

Creation of masking interferences that render the signal extraction impossible

Lowering of the trust level !

Ensuring TP Non-intrusiveness



Housing that provides shielding

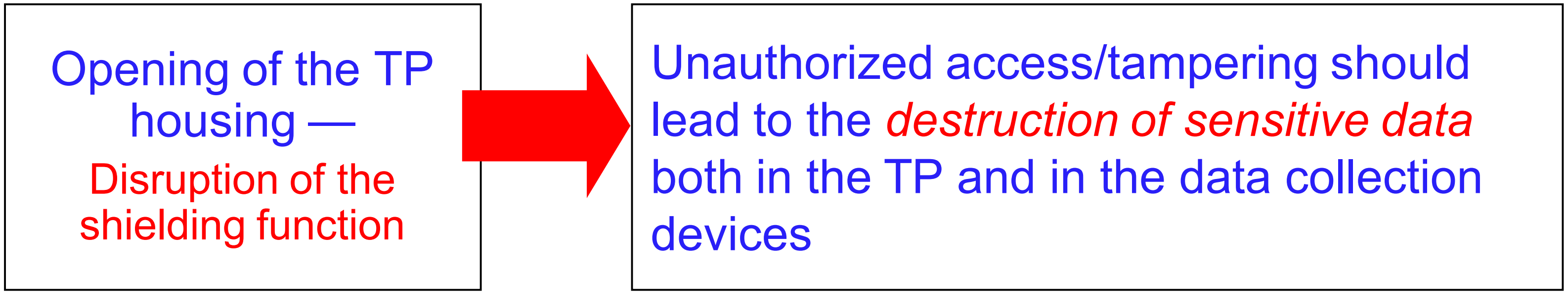
+

Design transparency

=

1. Sectional housing to provide access to the TP modules
2. Measures for maintaining shielding properties:
   - reliable electrical contact between the housing parts
   - electromagnetic protection of cable inputs

Ensuring TP Non-intrusiveness



Opening of the TP housing — Disruption of the shielding function

Unauthorized access/tampering should lead to the *destruction of sensitive data* both in the TP and in the data collection devices

Use of ***tamper-indicating devices — unauthorized access detectors***. The triggering of such a detector during TP operations should ***reset the hardware.***

Ensuring Validity of Information in TP

- Validity

  is 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.

Ensuring Validity of Information in TP

The probability of falsifying the results of the sensitive information processing in TP is linked to the possibility of the existence of *"hidden switches"* in the TP design.

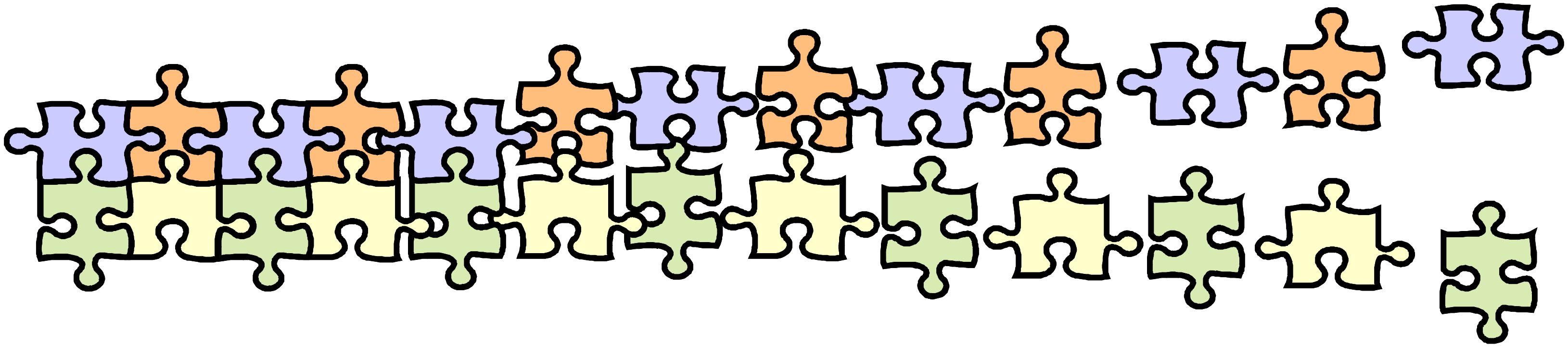
A "hidden switch" is anything that could selectively affect the results of the fissile material verification.

The hidden-switch problem is divided into two components:

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

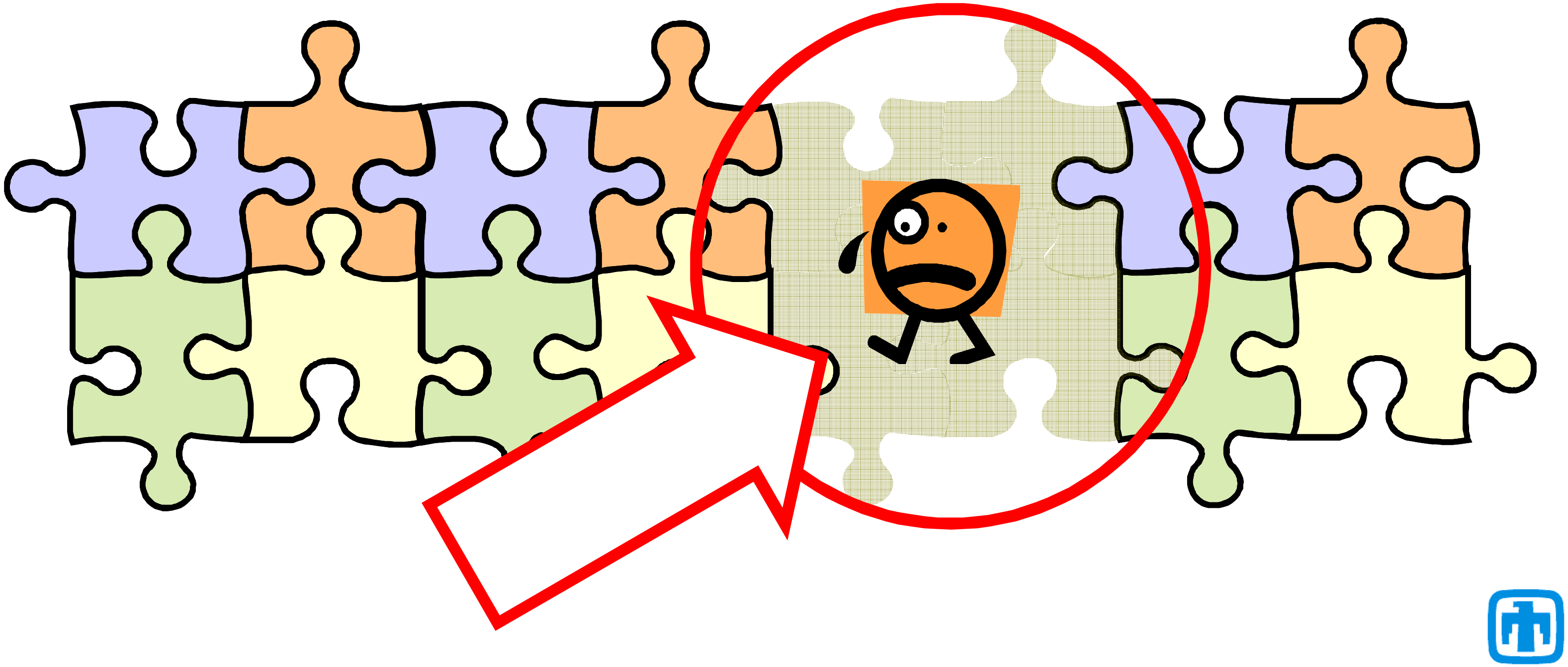
Ensuring Validity of Information in TP

In analyzing the TP hardware and software for the absence of hidden switches, one must inspect the structure of the hardware and the software to the smallest indivisible component.



Ensuring Validity of Information in TP

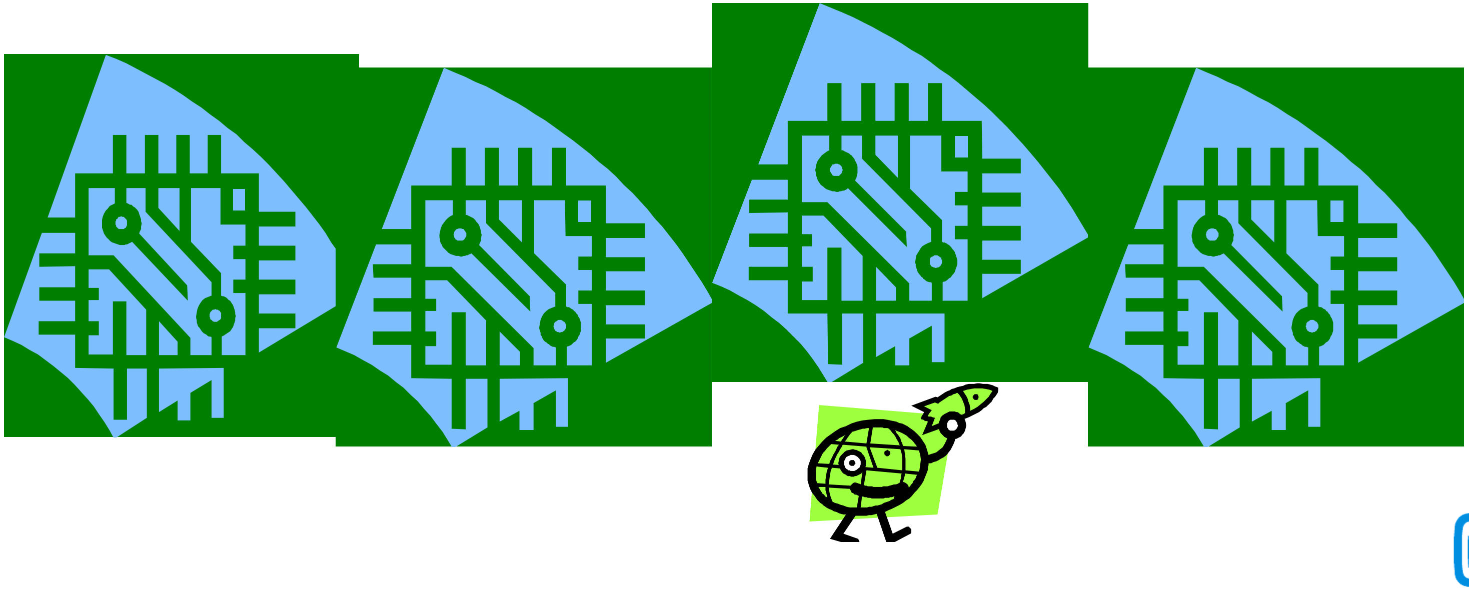
For the software, this indivisible component is the processor command to which the assembly language instruction clearly corresponds. If there is comprehensive documentation on the software being used, the *software-based hidden switches* are unavoidably detected.



Sandia National Laboratories

Ensuring Validity of Information in TP

The presence of documentation for the TP hardware 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.



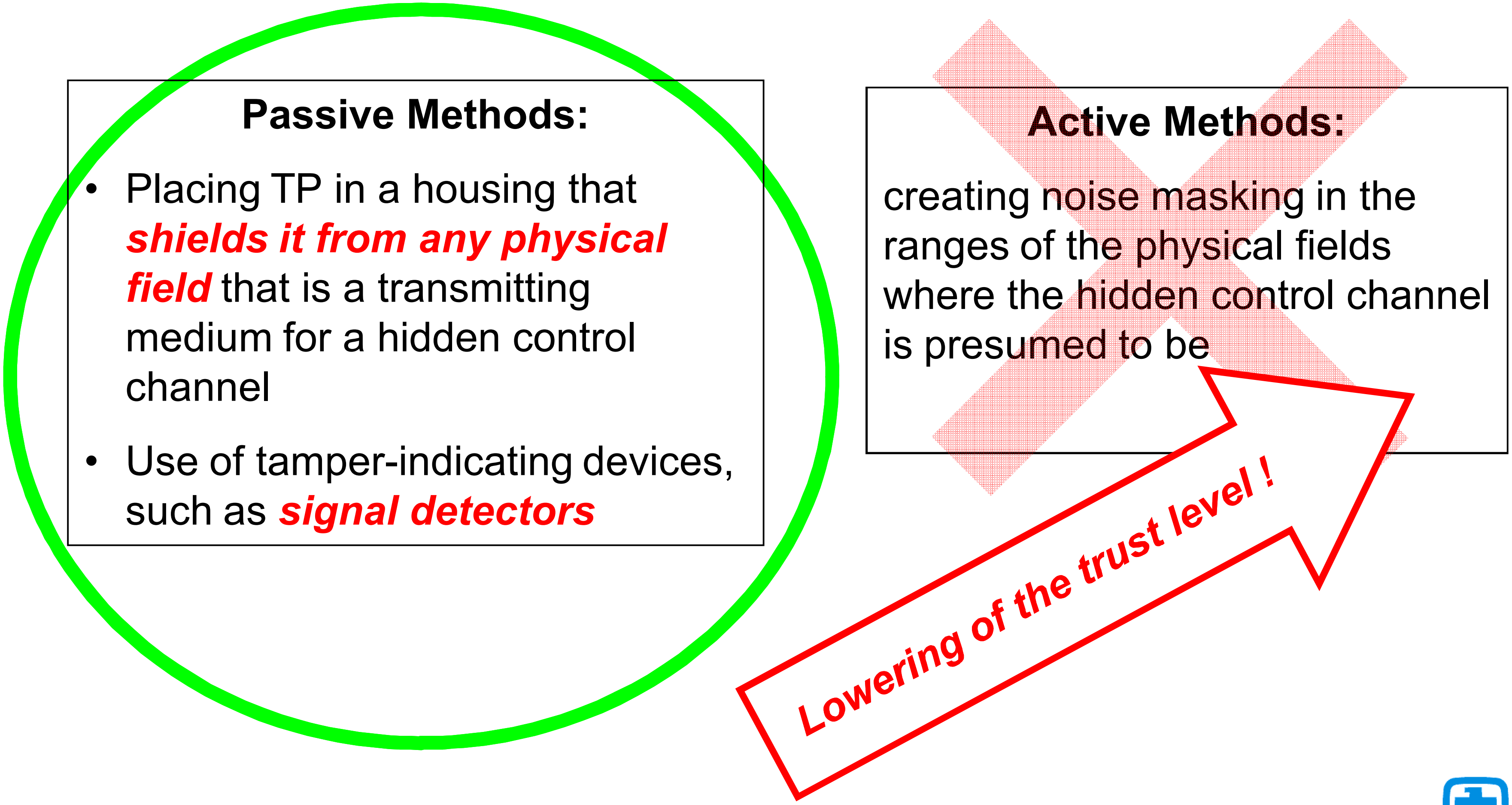
Ensuring Validity of Information in TP

Possible measures that can be taken to ensure trust in the hardware part of TP:

- Use *publicly accessible* microelectronic items acquired on the *free* market from *different* makers.
- Use microelectronic components that support the IEEE 1149.1 boundary-scan standard (JTAG), to enable non-destructive testing of the TP modules.

Ensuring Validity of Information in TP

TP protection against hidden control channels:



Passive Methods:

- Placing TP in a housing that ***shields it from any physical field*** that is a transmitting medium for a hidden control channel
- Use of tamper-indicating devices, such as ***signal detectors***

Active Methods:

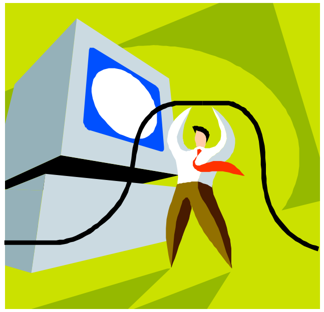
creating noise masking in the ranges of the physical fields where the hidden control channel is presumed to be

Lowering of the trust level !

Ensuring TP Transparency

Transparency

is 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.



Ensuring TP Transparency

Analysis of the transparency should consider the following:

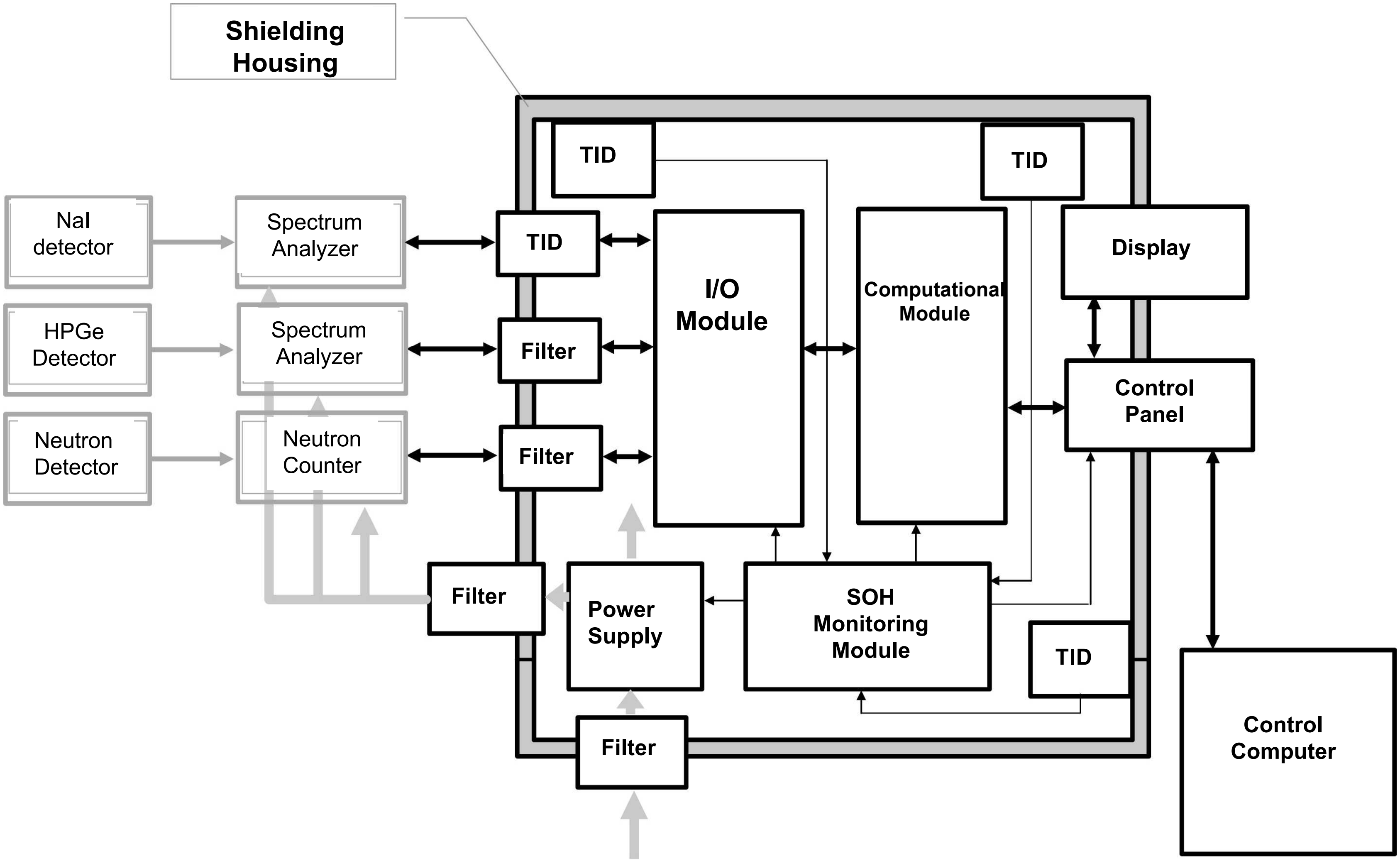
- transparency of the *principle of operation of the system* as a whole and of the interrelationship among the components
- transparency of the *structural design of the system* as a whole and of its components, to the level of the smallest indivisible component
- transparency of the smallest *indivisible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

Ensuring TP Transparency

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
- 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)

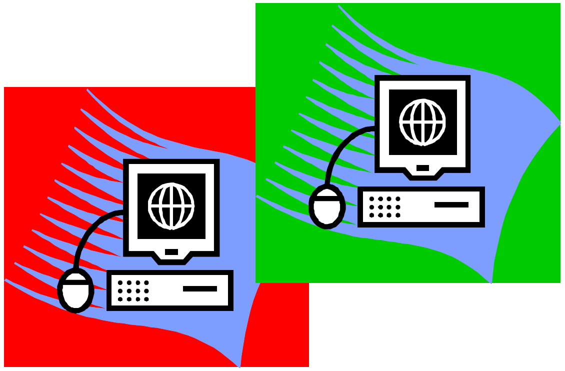
TP Structural Diagram



Ensuring TP Authenticity

- Authenticity

  is the conformance of a given device to an agreed-upon reference standard, and to it only.



Ensuring TP Authenticity

Authentication is a check to determine that a system conforms to a given reference standard.

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.

Ensuring TP Authenticity

Functioning of the TP is to be done in two modes.

- In *“open” mode*, radiation measurements are tested both from a panel and a connected personal computer on reference sources that have known characteristics.
- The *“closed” mode* corresponds to measurements of the FM sample being tested. The triggering of any tamper-indicating device results in the destruction of sensitive information in the TP 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 TP when the mode changes.*

Requirements for TP Computer Resources

In terms of functions performed, the TP’s software can be divided into two fundamental sections:

- the controlling program (monitor)
- 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 TP tasks is made by the *programs for processing the results* of the measurements.

Requirements for TP Computer Resources

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.
- *Sensitive information* in the measurement equipment and TP must be *destroyed* after the final non-intrusive results are prepared.

Characteristics of TP Computational Module's Processor

1. For interaction with external equipment and the control panel:
   - Timer for controlling the stages for the performance of measurement procedures
   - Serial port for linking to the panel and/or the controlling computer
   - Parallel port for linking to the input/output module

Characteristics of TP Computational Module’s Processor

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

Characteristics of TP Computational Module's Processor

3. For ensuring specific properties of the TP:
   - Support of the IEEE 1149.1 boundary-scan interface (JTAG)
   - Flat pack (PQFP, TQFP)
   - Presence of the sync signal frequency multiplication circuit
   - Supply voltage must not exceed 3.3 V

Overview of Hardware Platforms for TP Implementation

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*.

Overview of Hardware Platforms for TP Implementation

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 design.

Overview of Hardware Platforms for TP Implementation

A TP based on programmable logic integrated circuits (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.*

A shortcoming of the PLIC option is the *lengthy period* for the in-house *development* of the TP's nucleus.

Overview of Hardware Platforms for TP Implementation

Implementing the TP on the basis of digital signal processors (DSP) is preferable due to the following DSP properties:

- The size of the *internal memory* allows mass storage of *sensitive data*.
- *Phase-locked loop frequency control* makes it possible to employ *low-frequency clock signal generators* to *reduce emitted electromagnetic interference (EMI)*.
- *The accuracy* in the performance of *operations* is *sufficient* for *processing* the measurement results.
- External devices (RAM, ROM, I/O) can be connected to DSP directly.
- Hardware mechanisms for speeding up computations ensure a *high level of performance.*

Conclusion

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 does not satisfy the *high-priority principle of system requirements*. Implementing a TP requires *specialized development*.