

RECEIVED  
JAN 30 1995  
OST 1

ISSUES ASSOCIATED WITH A TOTAL SYSTEMS APPROACH  
TO DESIGNING DEPENDABLE SYSTEMS

G.H. Chisholm

Argonne National Laboratory  
9700 S. Cass Avenue  
Argonne, IL 60439  
chisholm@mcs.anl.gov

MASTER

Abstract: A total systems approach, developed by the nuclear-reactor-safety community, is extrapolated to the design of complex, critical systems. The essential properties of these systems are described, and a generic paradigm for subsequent designs is proposed.

Keywords: complex systems, fault-tolerant systems, system architecture, system integrity, system models, systems design, reliable

1 INTRODUCTION

A nuclear power station is a classic example of a dependable system. Fielding such a system requires close communication among many disciplines to ensure that the specifications and implementation of the system are conducive to certification. This paper introduces a total systems approach to managing this process. This approach, used in the nuclear industry, is also generally applicable to the design of complex, dependable systems.

The total systems approach is based on developing multiple layers (commonly referred to as "defense in depth"). The control system occupies the innermost layer of the design and is made up of two subsystems: the continuous control subsystem and the safety subsystem. The safety subsystem has ultimate control over safety-related functions. It is trusted to perform these functions when required and certified to provide its functionality during design-basis events. Digitization of the safety subsystem mandates compliance with the precepts of the overall safety policy for the facility.

The total systems approach consists of the following steps:

- Identify critical functions and properties.
- Conceptualize architectures that implement the required functions and have the stated properties

- Evaluate the architectures for system constraints, and select a candidate for continued decomposition.
- Repeat steps 1, 2, and 3 until the design is complete.

This paper describes three complex systems: a commercial nuclear power generating station, a fault-tolerant computer, and the Battle Management/Command, Control, and Communications (BM/C3) element of the Strategic Defense Initiative Office's Global Protection Against Limited Strike (GPALS) system. These three systems have the following properties in common:

- Dependable systems are composed of multiple layers. The inner layer represents a minimal, or degraded, functionality, whereas the outer layer represents the fully evolved functionality.
- The inner layer is made up of critical and trusted functions. Subsequent layers perform less critical, but more complex functions with successively lower levels of trust.
- No single point of failure impairs the functionality of the most critical layer (diversity, recovery blocks, and/or partial

proofs of correctness combined with testing are recommended).

- Firewalls ensure that a failure in a less critical layer does not affect a more critical layer.
- Acceptance tests may provide a mechanism for graceful degradation and trust enhancement.

A total systems approach has been applied to the design and certification of critical systems. It has also been extended to a complex, computer-based system with similar design constraints. The essential properties of such systems are described, and a generic paradigm for design is proposed.

## 2 COMMERCIAL NUCLEAR POWER STATIONS

Designers of commercial nuclear power stations must consider two "mission critical" functions: power production and public safety. Power production is enabled by a multilayered control system:

- Corporate (i.e., establishing goals for station operation, such as megawatt production levels);
- Administrative (i.e., system goals that accomplish station goals, such as reactor power level);
- Continuous (i.e., subsystem goals, such as optimal control laws applied to primary flow rate); and
- Safety (i.e., protective goals, such as fuel temperature upper limit).

Layering is predicated on the ultimate authority of the safety system to ensure proper action. This authority is established by carefully analyzing the system to determine the least acceptable functionality that provides adequate protection.

Public safety is ensured by a defense-in-depth philosophy in the design of radiation containment. This philosophy is realized by both passive and active features. The passive features include the following:

- Fuel cladding (metallic jacket surrounding the fuel),
- Primary coolant boundary (coolant containment), and
- Reactor containment building.

The active features include safety subsystems, such as the following:

- Coolant injection systems,
- Dual negative reactivity insertion systems, and
- Safety control subsystems.

These features, individually or in combination, address possible failure scenarios that have the highest probability of affecting safe operation of the plant (e.g., an earthquake).

The safety control subsystems have the authority to curtail power generation if necessary to ensure public safety. However, spurious misuse of this authority has large negative effects. Likewise, failure to exercise this authority in the event of a real need is a serious design flaw. For these reasons, great care is taken in identifying critical functions.

Stringent requirements are placed on implementing critical functions and critical properties (e.g., ultrahigh reliability and availability). These requirements are realized by the use of redundancy and voting to detect a failure, isolate this failure, and reconfigure the system. These realizations are predicated by a strict independence among the layers of the control subsystems. For example, the continuous layer cannot obviate the functionality of the safety layer. The safety subsystems are considerably less complex than the total system, and their functionality is ensured by independence and fault tolerance.

## 3 A DEPENDABLE COMPUTER BASE

A reactor safety control subsystem is designed on the basis of the critical properties of failure detection, isolation, and reconfiguration. A general approach depends on establishing that the computer base has these properties and does not introduce faults into the application. A digitized system must have similar properties. Thus, both qualitative (no single point of failure) and quantitative (Markov) analysis are used to establish the reliability of a computer base. Each application is then required to establish its reliability. (One approach would be to establish claims respective to the application by applying formal methods and asserting that the functionality is provided with the reliability established for the computer base. Further research is required to support this concept.)

The Charles Stark Draper Laboratory Fault-Tolerant Processor (FTP) was designed to tolerate Byzantine faults. For example, the FTP protects against a type of Byzantine fault that occurs when a fault is perceived differently by different system components. This design feature was highly desirable in the intended critical application. Another benefit of the FTP design is that one

need not provide a direct proof of the fault tolerance of the software. Rather, formal analysis must show only that the software meets its *specification*. This specification is sufficient to demonstrate that the total system (hardware and software) is tolerant to faults in the hardware and input sensors. In this specific application, the software itself is *not fault tolerant*. The fault tolerance of the *hardware* allows the software to meet its specification. (Note also that no claims are made about the *correctness* of the *functionality* of the software; this is a separate issue.)

The claim of fault tolerance is linked to the manner in which the FTP operates. Each of four processors is assumed to be executing the identical program. Further, all processors are executing the same instructions in lock-step synchrony. Data are transmitted bit serially in the FTP. When a processor computes a data value, it distributes its value to the other processors via the data distribution network (a *voted exchange*). The voting mechanism not only guarantees that each processor stores congruent data, but it also ensures that identical data are stored, even in the presence of a single failure in the system.

One can examine the flow of control of the software to understand how it is linked to the behavior of the FTP hardware. The first time the application software is executed, local variables are initialized. Then, the software initiates, reads, and stores the sensor data from its own node. (Identical software is being executed on each node. At this stage, the nodes simultaneously read data from redundant sensors.) Next, the software distributes the data from each node to the others in such a manner that

- The data in each processor are the same if there are no hardware faults.
- The data in a majority of the processors are the same (but not necessarily correct) if there are hardware faults.

All application software performs a standard signal validation test (a sequential probability ratio test) on the sensor signal data. The results for each test from each node are distributed to the other nodes, compared, and distributed back to each node. Again, the hardware ensures that the data returned to each processor are the same in most of the processors, but not necessarily correct. Each node then generates an appropriate control signal and sends it to the reactor shutdown system. Thus, the application program can be structured so that its results can be proven to be correct, even in the presence of a single fault.

Single-fault tolerance is a special feature of the FTP. If the hardware in a single-fault containment region malfunctions, at most a single error is generated. The single error could be the result of several failures within the faulted region. However, the failures still result only

in the propagation of a single error to the other regions. The error is detected during the voting process, and the malfunctioning region is masked out of further voting until it is repaired.

The FTP design was carefully analyzed, and compliance with the failure detection, isolation, and reconfiguration paradigms for nuclear reactor safety subsystems was confirmed.

#### 4 GPALS BM/C3 — A CASE STUDY

The total systems approach to the management of complexity to facilitate a safe design was also applied to the BM/C3 element of the Strategic Defense Initiative Office's GPALS system. Designing GPALS BM/C required a multistep approach:

- Determine critical functions and properties. A critical function is defined as follows: a function is critical if the system will not achieve its objective if the function is removed.
- Develop alternate strategies for implementation.
- Evaluate each strategy for compliance with design constraints.
- Select the superior strategy, and repeat steps 1 through 4 until the design is complete.

In developing a complexity management scheme for this software, one essential assumption was made about the enabling computer resources (i.e., hardware, operating system software, and network): the computer resources are designed and implemented commensurately with the BM/C3 trust objectives (e.g., reliable, available, coordinated, tolerant of single points of failure).

Figure 1 depicts a multilayered design alternative for GPALS BM/C3. The representative properties of the layers are as follows:

- Inner layer (critical functions)
  - Most trusted,
  - Minimum accepted functionality,
  - Highest reliability and availability, and
  - No single point of failure.
- Outer layer
  - Least trusted,
  - Optimal functionality, and
  - Lowest reliability and availability.

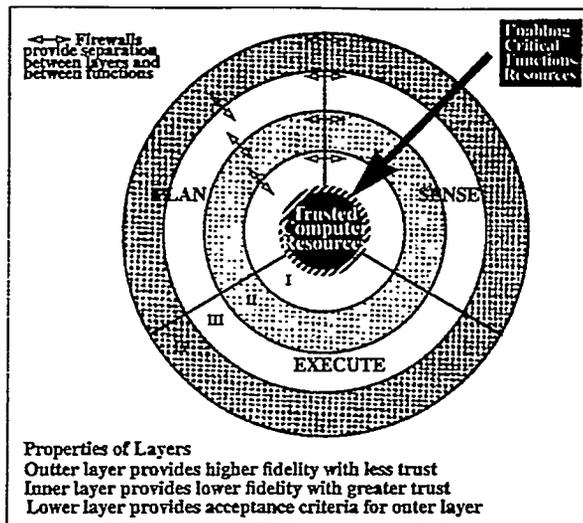


Figure 1 A Multilayered Design Alternative for GPALS BM/C3

An essential feature of this strategy is that each layer is separated by a firewall. These walls ensure that the failure of one layer will not impede the functioning of another, more critical layer. Because of their importance, firewalls must be implemented at the highest trust level. Independence of control and data is ensured by formal specification, formal verification, and testing.

An important side effect of this strategy is support for the graceful degradation of the BM/C3 functionality. Failures are anticipated to occur in the outer layer. When such a failure is detected, the system can degrade gracefully, that is, recover to a configuration that is free of failure. This configuration may perform the same function, but with a lower degree of fidelity. Figure 2 depicts an acceptance test performed at the firewall. Agreement between two layers implies that the data resulting from the calculation of the outer layer are at least as good as those from the more trusted inner layer.

## 5 CONCEPTUAL DESIGN OF AN ACCEPTANCE TEST

One approach for graceful degradation of the functionality allocated to the computer resources of the GPALS BM/C3 is presented. The following results are from an analysis of those functions:

- The Sense, Plan, and Execute functions are critical to the GPALS mission.
- A function is composed of multiple layers. The inner layer represents a minimal, or devolved, functionality, whereas the outer layer represents the fully evolved functionality.

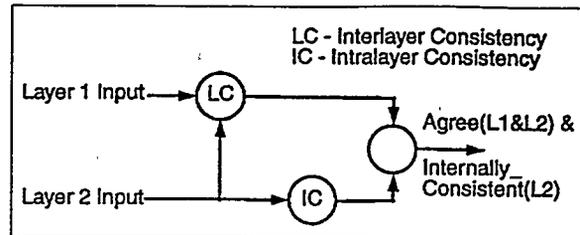


Figure 2 GPALS BM/C3 Acceptance Test

The inner layer is made up of critical and trusted functions. Subsequent layers perform less critical, more complex functions with diminishing trust.

- The following design paradigms provide an initial approach to complexity management:
  - No single point of failure will impair the functionality of the most critical layer (diversity, acceptance test, and/or partial proofs of correctness combined with testing are recommended).
  - Firewalls will ensure that failures in less critical layers do not affect a more critical layer.
- The enabling computer resources are assumed to be reliable, available, coordinated, and tolerant of single points of failure.

## 6 DISCUSSION

The three systems described here must perform under predetermined conditions. Such systems can be certified only when a convincing argument is presented that the system performs as required, only as required, and wholly as required. In the nuclear community, this argument is supported by qualitative and quantitative analyses. The qualitative arguments are similar to those postulated by the fault-tolerance communities (e.g., performance in the presence of all postulated single failures). The quantitative argument is exemplified by a probabilistic risk assessment or a Markov analysis. The total systems approach focuses on functions and properties (e.g., security or fault tolerance). This focus stems from the observation that a single failure may obviate any component of the system, yet must not affect the performance of the required function. Likewise, a security breach may occur at any point in the system, yet must not obviate functionality. From another perspective, functions are envisioned as decomposable, from some top-level capability to a least reducible function. Properties of systems must permeate this decomposition structure (i.e., each component must be secure or fault-tolerant to support operation in the presence of the initiating event).

This conceptual approach provides a mechanism for composing critical properties. That is, the essence of such composition is formulating an argument that the system performs the required function while demonstrating that critical properties are preserved. The rationale for such an approach centers on the precept that properties such as safety or security are indigenous to individual, nonidentical applications. This rationale justifies unique formulations in support of system certification.

## 7 CONCLUSIONS

The following conclusions can be drawn from this study: A total systems approach to dependable system design requires communication among diverse disciplines.

- Fault tolerance permeates the totality of the system.
- Complexity management leads to a multilayered implementation of critical functions (e.g., safety, security, system).
- Formal specification, verification, and testing are manageable when complexity is managed.

## ACKNOWLEDGMENT

This work was sponsored by the National Security Agency.

## BIBLIOGRAPHY

Chisholm, G.H., J. Kljaich, B.T. Smith, and A.S. Wojcik, 1987, *An Approach to the Verification of a Fault-Tolerant, Computer-Based Reactor Safety System: A Case Study Using Automated Reasoning*, Interim Report NP-4924, Electric Power Research Institute, Palo Alto, Calif. (Jan.)

Kljaich, J., 1985, *Formal Verification of Digital Systems*, Ph.D. Dissertation, Department of Computer Science, Illinois Institute of Technology, Chicago, Ill. (Dec.)

Kljaich, J., B.T. Smith, and A.S. Wojcik, 1988, "Verification of Fault-Tolerance Using Dependency Lists," in *Proceedings of the 1988 International Conference on Advanced Science and Technology*, Chicago, Ill. (Feb.)

Winter, V.L., G.H. Chisholm, B.T. Smith, and A.S. Wojcik, 1992, *A Formal Model for Verification of Abstract Properties*, Technical Report ANL-92/10, Argonne National Laboratory, Argonne, Ill. (April).

The submitted manuscript has been authored by a contractor of the U. S. Government under contract No. W-31-109-ENG-38. Accordingly, the U. S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for U. S. Government purposes.

## DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

