

A Framework for Proactive, Automated and Continuous E-commerce Control and Assurance

Wenli Wang • Andrew D. Bailey • Zoltán Hidvégi • Andrew B. Whinston

Decision and Information Analysis, Goizueta Business School, Emory University, Atlanta, GA, 30322

Department of Accounting, University of Illinois at Urbana Champaign, Champaign, IL 61820

Center for Research in Electronic Commerce, Department of MSIS, The University of Texas at Austin, Austin, TX 78712

Wenli.Wang@bus.emory.edu • jabaila@uiuc.edu • hzoli@ede02.bus.utexas.edu • abw@uts.cc.utexas.edu

September 17, 2001

SUMMARY

In electronic commerce, proper operations of e-processes are crucial to an e-business' economic well-being. We suggest that due to the complexity and characteristics of e-operations, the only viable approach for rigorous control and assurance relies on mathematical and computational methods to represent and analyze e-systems. Traditional auditing methods, based on manual verification, piecemeal analysis and post-audits, are insufficient. An innovative set of methods is proposed: 1) Applying economic reasoning, e.g., mechanism design, to design correct e-commerce trading rules and policies; 2) Applying the concept of atomic transactions to define e-system properties and specifications; 3) Applying formal verification, e.g., model checking, to ensure correct implementation; and 4) Applying agent technology to monitor real-time execution. These four methods should be embedded within the System Development Life Cycle. They complement each other, and their proper applications can refine e-systems and enhance the relevance, completeness and reliability of control and assurance.

KEYWORDS: Electronic Commerce, Internal Control, Assurance Services, Auction, Formal Verification, Distributed Computing

INTRODUCTION

Internet-based business operations offer many benefits, but also bring a broadened range of risks, some of them unprecedented. The actual and perceived lack of system security and reliability are significant deterrents to the rapid growth of the digital economy. While daily progress is being made in reducing Internet computational risks through a variety of software patches and cryptographic algorithms, these efforts solve only a small piece of the larger puzzle. To solve the puzzle, systematically managing e-business operational risks is particularly important.

To manage e-business operational risks we need to look into the e-commerce infrastructure. Distributed Internet computing is fundamentally changing e-market structures and e-business models. This is a mixed blessing. While the flexibility of distributed e-operations supports open accessibility and dynamic interactions, it also intensifies problems arising from e-market information asymmetry and e-business operational uncertainty. These problems prevent, or at least restrain, innovative e-commerce transactions. For example, although e-commerce

offers the opportunity for e-businesses to build network-based ad hoc partnership, many e-businesses still choose to operate in a more familiar and stable market scope through traditional means because of the increased difficulty of assessing information asymmetry in real-time and the heightened risks from operational uncertainty among unfamiliar business partners.

Because of the distributed nature of e-transactions, the potential for information manipulation and operational fraud by a disguised or dishonest Internet party is quite high. Also, most unfortunately, due to the increased complexity, even legitimate and honest parties may unknowingly introduce errors if effective business controls are not in place and functioning. Recognizing that trust services are needed, the auditing profession is beginning to provide a broad range of information services. The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) have introduced WebTrust, WebTrust-ISP and SysTrust products to support such a demand (Ame 1996).

However, the auditing profession has not yet provided practitioners with new and effective tools adapted to e-business con-

trols and assurance. In effect, it suggests that practitioners carry over the traditional control and auditing principles and methods to provide new assurance products. Providing e-commerce assurance services only need audit-like skills (Nagel and Gray 1999). Unfortunately, traditional means are insufficient and auditors need to expand their skill set.

We argue that due to the complexity of e-business operations, the only viable approach for systematic control and assurance is to use rigorous mathematical and computational methods to represent and analyze e-systems. To be proactive and more effective, these methods should be applied from the early stages of the System Development Life Cycle (SDLC). We introduce a Proactive, Automated, Continuous Control and Assurance Framework (PACCAF, pronounced pə-ˈkäf), involving four suggested methods that should be used at the various stages of SDLC: economic reasoning, atomic transaction design, formal verification and real-time monitoring. PACCAF takes into account many issues Kinney, Jr. (2001b) considered as research barriers to internal control quality and quality assurance: organization design and measurement, process verification, and the complexity of both the subject systems and the control and assurance processes.

INFORMATION ASYMMETRY AND OPERATIONAL UNCERTAINTY IN E-COMMERCE

Market Information Asymmetry

Information asymmetry exists in any market (e.g., securities, used cars, software). Most of us have neither the time nor inclination to investigate the “quality to price” characteristics of every product or service we purchase online. As consumers, we tend to rely on the market to be information efficient and thus permit us to act as a simple price taker. In a benign environment, this may cause us no systematic harm. Unfortunately, the openness and anonymity of the Internet allow for easy misrepresentation and thus is not so benign. Digital markets are far from being information efficient. Information asymmetry in e-commerce has shown itself to be particularly problematic due to the breadth of access and processing speed. The easy access to a large number of potential victims has shown that some small and short lived misrepresentations can be profitable. This is one of the reasons why online scams or inaccurate e-business claims are common practices.

Business Operational Uncertainty

Operational uncertainty results from the unforeseen difficulties that can occur and disrupt the efficiency of business operations. Unlike in traditional businesses where business models are established, task divisions are defined, operations are standardized, and partnerships are limited, e-businesses operate much more dynamically and at a much faster pace. Unfortunately, change brings in risks. Because e-business operations are computing processes running over the Internet, they are, by nature, distributed across different computing systems and further across different organizational domains. This distribution

can have devastating side effects. To be more specific, the following characteristics of e-business operations introduce unwelcomed uncertainty and are potentially harmful if not properly controlled:

Interconnectivity

Networking technology and client-server applications allows the flexible integration of digital operations across different vendors. E-businesses often outsource Web hosting to ISPs, banner ad operations to advertisement dot coms and payment collection to credit card companies. In the extreme cases of flexible and dynamic integration, two major types of e-firms result:

- *Creativity firms*: firms that produce commodities, such as news, MP3 music, streaming videos and knowledge.
- *Process firms*: firms that provide business processes, such as advertising, inventory management, to other firms.

Creativity firms supply new commodities and process firms help channel them to support demand. Consequently, information, even information that can be considered a crucial business asset, may frequently flow in and out of a firm to its business partners and consumers in order to fulfill a single transaction. An error or attack at one location may trigger a domino effect resulting in catastrophic failures across many e-processes. These concerns arise naturally from the intense interdependency and interconnectivity of e-business operations, coupled with the usual moral hazard problems commonly associated with outsourcing and contracting.

Automation

Because of dramatically increased cost-efficiency and computing capability, business operations that traditionally require human involvement are becoming computerized. A good example are the Goldman Sachs traders who are assisted by sophisticated information technology. Secret algorithms guide 20,000 a day trades in the equity derivative market. Trade prices are updated 200 times per second and 100 million deals are executed without any human intervention (Weinberg 2000). In general, e-business operations can be fully implemented by a cluster of e-processes. Users may generate initial inputs from Web browsers, while programs running on servers automatically process inputs and generate outputs.

One side-effect of the heavy reliance on computing is an increased vulnerability to problems that can arise from the varying quality of the software supporting or implementing business processes. When and how a latent bug will be triggered and how the bug will affect business operations are difficult to predict. Uncertainties caused by the most recent “Code Red” worm exemplify such concerns. Therefore, e-processes should be designed to react properly in as many potential situations as possible. Controls should be executed when exceptions occur.

Speed

Computing power, coupled with automation and interconnectivity, makes for speedy e-business transactions. Transactions taking several business days in the physical economy can be completed in seconds. Unfortunately, such speed generates new possibilities for failure and the enhanced impact of failure. A small disturbance may rapidly resonate throughout the system, causing large waves and subsequent chain reactions that can only occur in an environment of complex interconnectivity. “Code Red” infected more than 359,000 computers in less than 14 hours (Meinel 2001). With the proliferation of global e-operations, similar quick catastrophic failures can be anticipated.

As we have implied, the above characteristics of e-business operations – interconnectivity, automation and speed – can interact and intensify each other’s effects of any failure. To help understand the increased complexity and risks of e-operations, we introduce the following example.

An E-business Example

/Insert Figure 1 here /

Figure 1 is a specific example, but it illustrates a more general e-business model – selling customized, sophisticated digital products. To satisfy each customer’s need in a highly responsive manner, such an e-business integrates various components in real-time, many of them might not be in stock and have to be obtained externally from their creators. Because digital products can be, and in many cases, should be, frequently refined or updated (e.g., software needs to be patched and online educational packages should be integrated with new real-world cases), the business’ digital inventory needs a faster turnover and the e-business needs frequent and dynamic involvement from content creators. For each customer request, the list of potential content suppliers may differ; hence, the e-business may even have to build ad hoc partnerships.

A concrete example of such an intermediary is a Red Hat-like distributor providing customized Linux packages. A customer submits her hardware configuration and software requirements. The Linux distributor searches its digital inventory and the Internet for necessary compatible components and presents the customer a package catalog with lists of choices and prices. After the customer picks her final order, the distributor fetches all necessary components, integrates them into a coherent package and delivers it to the customer. Occasionally some suppliers may need to directly contact the customer and then report their services to the distributor for payment purpose.

Such a customized sale takes about 23 steps. Each step may involve one or several e-processes, each being implemented by a list of interacting computing procedures which may reside on servers dispersed all over the globe. Not to mention that the customer may expect to order and receive delivery in a single Web session. The pressure is largely on the distributor to carry out these processes seamlessly and quickly. However, any mistake

in the system may lead to a failure. The secret of e-business success – “... knowing and fulfilling customer need, ... and building network-based alliances and partnerships” (Barua and Whinston 2000) – is easier said than done.

Many e-businesses aim to provide customized and responsive e-services. But the implementation can be complicated and risky. The challenge is, given such complexity, how to control and assure e-services to gain customers’ trust?

NEW SCOPE OF TRUST SERVICES

Information asymmetry and operational uncertainty are stumbling blocks in e-commerce development. The need to manage them has generated a demand and supply for trust products and services. Trust services in e-commerce are not restricted to financial information, but regard any decision-making information, including: 1. Operational inputs and outputs; 2. Digital products and services; and, 3. Business claims and reporting. Table 1 illustrates the new scope of assurance services in the digital economy, compared with the traditional auditing services.

/Insert Table 1 here /

	Traditional Auditing	Assurance Services
Concern processes related to	Accounting Information	Any Information
Provide assertion about relevance and reliability of	Financial Reporting	Any Information Reporting
Play the role as the guardian of	Capital Market	Any Market

Table 1. Expanded scope of assurance services in e-commerce

Trust services related to information and its processing are needed for e-commerce. We now address the limitations and potentials for several trust products and services created by different industries.

LIMITATIONS OF EXISTING TRUST PRODUCTS AND SERVICES

Trust Products and Services from Computer Scientists

Security products in computing are trust products because they aim to reduce computation risks, part of e-business operational uncertainty. Cryptographic protocols, firewalls, digital watermarking, and software patches all contribute to the reduction of operational uncertainty, and, to a limited extent, information asymmetry. But, the contribution is limited. For instance, Secure Socket Layer (SSL), a popular security protocol applied by almost every e-business to authenticate Web servers through digital signatures and certificates is optional to authenticate Web clients. Hence, SSL cannot prevent false names. Relying on

technical solutions as the sole basis for claiming e-business security, is far from a complete solution.

Trust Products and Services from Entrepreneurs

Several firms have recognized the market niche for a more fundamental approach for e-business security – process design. These process firms introduce specialized e-business functions that reduce certain aspects of operational uncertainty. Secure Electronic Transaction (SET) is such an example. It surpasses SSL in securing online credit card payments by discouraging individual vendors from keeping customer credit card information. Another examples are InterTrust's Digital Rights Management (DRM) to manage digital products and Certificate Authorities (CAs) certifying public-key as a promising solution to Internet authentication problems.

The above trust services are important additions to e-commerce and can be used together to substantially improve system security and reliability. In the nature of trust layering, e-commerce users face the same trust problem when using trust services: Do they perform as claimed? CA businesses are not rigorous as the Social Security bureaus, which discount their importance. If DRM services have security holes or errors, creativity firms relying on InterTrust's DRM may lose their digital assets and InterTrust's failure could, in its extremity, result in the "going concern" issues for its business customers.

Trust Products and Services from Auditors

The infinite regression of layered trust concerns cannot be resolved in principle (Gerlach, McAfee, Bailey, Jr and Whinston 1981). However, a competent and independent third party trust provider with no objective other than assuring product reliability can contribute to product credibility and reduce user risks. The underlying contribution of auditors is their competence and independence. By building a reputation for competence in business, accounting, and auditing, and by demonstrating an independence from management, auditors contribute to an efficient and productive economy. Now auditors are developing competencies intended to secure clients in the new e-commerce domain. The AICPA/CICA have introduced several trust products and services: WebTrust, for the B2C market focusing on e-business disclosure, transaction integrity, and customer information protection; WebTrust-ISP, for examining the integrity of Internet Service Provider (ISP) services; and more recently, SysTrust, for providing assurance of basic computer information systems supporting firm operations and reporting. On another track, the auditing profession has also introduced eXtensible Business Reporting Language (XBRL) to facilitate Web financial reporting. Its future development should consider the security and reliability of online financial reporting.

Although the trust products and services offered by the auditing profession are appropriate and timely, the profession's implementation guidelines fail to meet the desirable requirements for such products. SysTrust (Ame 2000) is an exemplary of our concern.

SysTrust Definition

According to the auditors, a business system consists of five key components organized to achieve a specified objective: infrastructure, software, people, procedure and data. While such a definition is valuable, it does not capture the essence of a functioning and evolving system. The definition is static and hence it is difficult to embody the characteristics of a system in operation. In order to transform inputs to valuable outputs, a system carries out processes characterized by motion and change. From the Merriam-Webster dictionary, a system is defined as "a regularly interacting or interdependent group of items forming a unified whole." This definition focuses on the motion and change of an operational system and brings the necessary interactions of the AICPA/CICA's definitional components into focus and is more useful for analysis purpose.

While we emphasize the fluidity of a system, we do not wish to discount the importance of regularity in the interactions. It is the regularity that supports the fulfillment of the common purpose. Therefore, to control and assure an e-commerce system, we need to focus on its functions, assembled by the operations and interactions of distributed digital processes. We will expand on this point shortly.

SysTrust Objectives and Criteria

To evaluate whether a system fulfills its objectives, we need to set up clear and proper criteria that can be measured empirically. The SysTrust principles and criteria set forth by AICPA/CICA provide a positive set of overall guidelines and can be adapted to the process orientation suggested. However, for the purpose of implementation and measurement, these criteria are too general to be immediately useful. Our suggested control and assurance framework below can be of use in developing the process focus when addressing field practice guidelines. We will also address a set of objectives that are critical for implementing and measuring distributed systems.

SysTrust Methods

The AICPA/CICA discuss the recommended methodology for SysTrust, which is the same as that used in financial auditing. Unfortunately, the five traditional auditing procedures – physically observing system behavior, inquiring of employees, examining documents, reprocessing data and analyzing information through analytical procedures – will not be adequate for verifying e-business systems.

Physical observation. Since e-operations have largely replaced manual operations, not many physical activities are left to observe. Many e-operations occur in milliseconds and are impossible to observe in any meaningful physical sense. Nevertheless, observation will continue to be an important activity, but based on "computer intelligent observation."

Inquiry. Similarly, although auditors can still query employees to see if they understand policies and procedures, it will be

more important for auditors to know how to observe and question e-processes than to quiz employees.

Examination. When examining e-operations, auditors face a paradox of “general information overload” and “relevant information scarcity.” Computation trails generated by operating systems and applications, the sheer volume of processing, and the lack of automated examination and reporting tools challenge auditors with overloaded computation trails. But there is also a lack of relevant information for verifying business properties. Over the years a set of data has been defined for verifying correct accounting systems, however, no consensus or standards exist on what data should be retained for verifying correct e-operations. Furthermore, information regarding an e-business event may be alive for only a fraction of a second and the “need for speed” also creates an incentive to omit information retention on e-business processes.

Reprocessing. Reprocessing is essentially reactive as are post testing and simulation. As we explain in detail in (Wang, Hidvégi, Bailey, Jr. and Whinston 2000), testing and simulation is useful but limited in checking a complex reactive system. Proactive verification and on-the-spot analysis along with system execution are be much more meaningful and reliable than reprocessing.

Analysis. Analytical procedures are widely used to analyze aggregated data to find exceptions. Analytical approaches help to identify interesting testing vectors and hence belong to the testing and simulation arena. As we explain in (Wang et al. 2000), for a complex system, it is impossible to identify all interesting testing vectors, therefore, analytical approaches have their inherent weaknesses.

The above approaches will continue to have value, however, e-commerce assurance requires a methodological paradigm shift from these traditional methods to those that can support proactive, automated and continuous control and assurance.

Point-in-time Auditing vs. Continuous Assurance

Some limitations of the traditional methods come from the fact that traditional auditing is a point-in-time assurance. Although the auditing profession has recognized the potential of continuous auditing, it has been very cautious about its development, partially because of liability risks. SysTrust serves as an intermediate step toward continuous assurance, however, many open questions remain to be addressed before SysTrust becomes an effective operational product (Bailey, Jr. 2000). Despite of the difficulties, we believe that in the future there will be a paradigm shift from the point-in-time, historical assurance over static states toward the continuous, forward-looking assurance over processes. Advancing control and assurance methods is a prerequisite for this shift.

A PROACTIVE, AUTOMATED AND CONTINUOUS CONTROL AND ASSURANCE FRAMEWORK (PACCAF)

We define an *e-commerce system* as a network of distributed digital processes, interacting in an established manner to serve business objectives. An e-business is a system of such systems. The analysis of an e-business decomposes a high level entity into its sub-systems that follow the same rules used to analyze a single system.

To control and assure an e-system, auditors must thoroughly understand the subject system. To do so, auditors should investigate the entire life cycle of the system.

System Development Life Cycle (SDLC) is a popular systems approach to problem solving. It has long proven itself to be a disciplined approach to developing information systems (Laudon and Laudon 2001). SDLC remains one of the design models for developing e-business applications; for instance, parts of the IBM e-business framework are designed to work within SDLC (Harvey 2000). Similarly, our methodology framework PACCAF is also embedded within SDLC because we believe that control and assurance should be an inimitable process running in parallel to the entire life cycle of a system.

There are six phases in SDLC: system analysis, definition, design, development, implementation and maintenance. We embed an innovative set of methods – economic reasoning, atomic transaction design, model checking and real-time monitoring – in SDLC, with each of them to be applied respectively in different phases of SDLC (Figure 2).

/Insert Figure 2 here /

Using Mechanism Design in SDLC Phase I: System Analysis

The major task in system analysis is to obtain an in-depth understanding of the present system and of the problems and limitations inherent in it. Analysis is particularly critical in e-commerce because many digital firms, when transitioning to e-commerce, have simply carried over the traditional policies and trading rules by “redressing” them to execute in the Web computing environment, but, unfortunately, policies and trading rules that function well in the brick-and-mortar commerce may fail in the digital setting. Fraudulent or malicious traders may exploit the resulting structural weaknesses.

Designing a robust process structure, safe against fraud and attack, falls into the realm of traditional internal controls. However, reinterpretation is needed for handling special issues that appear in e-commerce. For example, separation of duties should be applied not only to divide responsibilities among personnel who design, implement, operate or monitor an e-system, but also to direct how to divide functionalities among e-processes.

More importantly, the fundamental soundness of e-business policies and trading rules should be examined. For example, on-line auctions have become pervasive and successful because of their inherent advantages of price discovery and the convenience offered to traders. However, their increased popularity has been

accompanied by growing pains. Online auction fraud has become the number one Internet fraud over the last three years (The Internet Fraud Watch 2001). In 1999, it accounted for an overwhelming 87% of the reported incidents, soaring from 68% in 1998. In 2000, it increased 23% and accounted for 78%.

One major attraction of conducting auction fraud resides in the inherent vulnerabilities caused by e-auctioneers applying traditional auction mechanisms in an untraditional trading environment. Examples have shown why traditional auction structures are vulnerable to shill bidding (Wang, Hidvégi and Whinston 2001b) and false-name bidding (Wang, Hidvégi and Whinston forthcoming, Wang, Hidvégi and Whinston 2001a). Shill bidding in English auctions is the deliberate placing of bids by the seller under a fictitious bidder identity to artificially drive up the price of the seller's item. False-name bidding is when a bidder creates and colludes under multiple fictitious bidder identities to reduce the bidder's expected payment. The lack of strong binding between an Internet identity and its real-world counterpart makes false-name registration possible and easy. Moreover, the policies of e-auction houses are not designed to prevent these fraud. For instance, they require minimum information for bidder registration, and they charge sellers low commission fees, which actually creates an incentive for shill bidding.

Preventing and detecting shill and false-name bidding are difficult. Most e-auctioneers do rely on some computing and statistical technologies for authentication, such as monitoring IP addresses or data mining on false-name registration. However, dishonest agents can still easily maneuver against them (Wang et al. 2001a). Duh, Jamal and Sander (2001) suggest that in order to control buyer-side integrity, e-auctioneers require buyers to provide credit card numbers and trade using their real names. But most e-auctioneers omit credit card information in their buyer registration because they fear this may hinder buyer participation and hence reduce market competition and liquidity. Authentication through digital signatures and encryption causes similar concerns but it is a much stronger authentication method. However, it will take years for cryptography to become a part of general Web users' daily operations. Instead of relying on immature technology to detect and react upon fraud, we should accept its existence, but design trading rules to eliminate its negative effects. In other words, e-auctioneers must accept the fact of false-name registration but redesign their auction protocols so that bidders and sellers cannot gain advantages by using false identities.

Redesigning auctions requires an analysis of how problems can occur. Shill bidding is, in fact, the seller secretly resetting her reserve during the bidding process after observing and knowing that there is a high probability of squeezing "extra juice" out of bidders with high valuations. Although Riley and Samuelson (1981) and Myerson (1981) have shown the revenue equivalence among common auction formats and how to calculate the seller's optimal reserve, they did not consider the case where an English auction can be more profitable to the seller than any other auction format when the market has different types of bidders

and hence the seller's expected profit curve has multiple local maximums. When there are multiple humps in the seller's expected profit curve, the global best solution of optimal reserve varies with respect to the number of bidders and the bidders' value distribution, observable in English auctions. A shill bidder can obtain this information during the bidding process and then maximize her expected profit accordingly by resetting the optimal reserve through shill bids.

To prevent the seller's manipulation over her reserve price, we focus on the role of an auctioneer as a trusted third party. The auctioneer can control the seller's behavior, such as the honest disclosure of the reserve before an auction starts, through the intermediation fee schedule he charges. We design a Shill-deterrent Fee Schedule (SDFS) (Wang et al. 2001b) where an auctioneer charges the seller as the following: 1) a listing fee, which is a function of the seller's reserve; 2) a commission fee, which is a function of a commission rate and the difference between the final sale price and the seller's reserve. Commission rates in different auction markets are mathematically determined to ensure the non-profitability of shill bidding.

In cases of buyers' false-name bidding, despite of the "bid shielding" in English auctions, another incentive for a bidder to false-name bidding in sealed-bid auctions is to possibly reduce his final payment by splitting his bid for bundled goods into several bids for smaller bundles (Wang et al. 2001a). To solve this problem, Yokoo et al. described a sealed-bid combinatorial auction protocol called Leveled Division Set (LDS) that discourages a bidder splitting up his bid (Yokoo, Sakurai and Matsubara 2000). This solution does not come without a price; LDS provides inefficient allocation and hence is not practical to use. To simplify, Wang et al. (forthcoming) modified LDS into a Leveled Partition Set (LPS) protocol for multi-unit auctions. Furthermore, Wang et al. (2001a) introduce a Binary Vickrey Auction (BVA) protocol, selling identical goods in bundles of power-of-two. BVA provides a more efficient allocation and is still robust against false-name bidding. All of the above new auction protocols achieve robustness against false-name bidding by determining the final allocation and payment in multiple steps, where bids for a bundle are considered more favorably than bids for partitions of the bundle. This selling strategy discourages a bidder from splitting a bid for a bundle to several bids under false identities.

As we have discussed above about e-auction markets, dealing with the inherent problems and limitations of the present system is crucial for evaluating an existing system or designing a new system. Technology changes force the changes of e-business policies and trading rules. These changes in process structure can modify traders' incentives. They function as proactive controls, which can contribute substantially to the achievement of system objectives.

Defining System Boundaries, Assurance Dependencies and Atomic Transactions in SDLC Phase II: System Definition

In SDLC phase II – system definition – detailed business requirements are further defined in terms of the overall system objectives. Based on these requirements, the designers prepare a conceptual design of the system. These business requirements also determine the properties and specifications that the system should satisfy. To define them, the designers first need to bound the system. This is an easier task for a brick-and-mortar system than an e-commerce system because of the dynamic and real-time interconnectivity and interdependence of e-processes within and across firms.

Drawing System Boundaries

The drawing of system boundaries must consider both vertical and horizontal dimensions. The digital content distributor model in Figure 1 illustrates the horizontal expansion of system boundaries. Unlike the traditional economy, where companies rely on physical assets to create value and have often owned the value chain to minimize the risk of relying on others, in the digital economy, companies relinquish ownership of most of the value chain activities. Instead, in order to do business in the most productive and efficient manner, e-companies rely on real-time information, and leverage Internet-based partnerships with suppliers (Barua and Whinston 2000).

The vertical dimension is depicted in Table 2, modified from the Barua and Whinston (2000) framework.

/Insert Table 2 here /

Layer Four	Internet Commerce
Layer Three	Internet Intermediary
Layer Two	Internet Application
Layer One	Internet Infrastructure

Table 2. Layers of Internet business operations

The bottom two layers represent the networking and computing services needed by an e-business to support its market or commerce operations. The Internet Infrastructure layer is the underlying platform for an e-business. An e-business needs to subscribe online services either from ISPs (e.g., AOL) or directly through Internet backbone providers (e.g., AT&T). It also needs to be equipped with online devices, e.g., routers, modems and fiber optic cables, purchased from manufacturers of networking and “last mile” access devices (e.g., CISCO). The Internet Applications layer involves software products and services. An e-business can develop its e-processes through Web development software and integrating functions of search engines, databases, multimedia and e-commerce applications. It can purchase consulting services that help design, build and maintain its e-processes.

The top two layers represent the Internet market and commerce activities. Internet Intermediary players are market makers or intermediaries, such as e*Bay, e*Trade and VeriSign. This layer covers online brokerages, auction houses, content aggregators, portals, e-advertisement brokers, trusted third parties, and so on. The Internet Commerce layer includes the companies that generate online sales directly to consumers or businesses, such as online retailers, the Web version of traditional corporations, and many “mom and pop” shops. An e-market operates at the bottom three layers and a commerce e-business can operate at either all four layers or at the bottom three, depending on how critical the commerce e-business relying upon an intermediary.

Drawing system boundaries, that is, identifying both horizontal and vertical operational dependence among digital processes, is necessary to create a sufficient system requirement list. Because the dependence is often reflected in business contracts, which provide a substantial portion of requirements, figuring out who are the important business partners is crucial for defining a system.

Determining Control and Assurance Dependencies

Drawing system boundaries is also important for understanding the extent of the vertical and horizontal assurance dependence. The quality assurance of lower-layer players’ products and services is the prerequisite for control and assurance of higher-layer businesses. If a lower-layer player provides computing and networking services for high-layer e-business processes, the integrity of its support is important to higher-layer businesses.

The lack of this vertical assurance is often a part of many e-commerce failures. Many high-profile news stories regarding Internet risks highlight viruses and attacks at the networking and computing levels, such as the “Code Red” worm. The reason that they become headline news resides in the fact, or the fear, of the devastating consequences for businesses. Since the operational success of an e-business is highly dependent upon the security and reliability of the underlying information systems, the design and implementation of e-business systems must overcome the weaknesses inherent in the Internet-based distributed computing. Assurance over the lower-level services, which should involve code level review, needs to be further emphasized and developed.

Horizontal assurance dependence also exists. For example, a credibility check is needed when interacting with a new business partner. The dynamic nature of business relationships and the desire for real-time interactions demand real-time quality assurance. This is why we regard an “Assurer” necessary in Figure 1. The “Assurer” can help establish the credibility of content providers to the distributor. Likewise, to create customer trust, the distributor also needs to purchase external assurance services to independently assess and certify its service quality. This service quality not only involves the intermediary’s own operations but also those of its content providers. A customer goes to the intermediary not only for one-stop shopping convenience but also

for service quality.

Control and assurance dependence requires auditors to have knowledge about security tools and schemes applied at the lower layers and by business partners. Auditors also need to disentangle control and assurance sensitive factors from detailed technical implementations. They may choose to outsource some supporting assurance services to other auditors or specialists. For example, they may outsource the bottom two layers technology verification to computer specialists and accept the assurance level they provide.

Analyzing Distributed Systems Through Atomic Transactions

Since e-business processes are indeed distributed computing processes, it makes sense that we look into how computer scientists manage distributed computing processes and improve their integrity. We learned that in order to disentangle the web of digital processes, we must group processes into controllable units called transactions. A *business transaction* is a collection of operations on the business' physical and abstract state. The physical state is the real state of a business (e.g., the actual assets) and is represented by the abstract state in computation (e.g., the database records of the assets). A business transaction transforms business states.

The pervasive use of distributed computation today implies that the integrity of such systems must be accepted as effective. The achievement of the reasonable integrity should be subject to the ACID properties, i.e., atomicity, consistency, isolation, and durability (Gray and Reuter 1992), because these properties have emerged as the unifying concepts for distributed computing. Achieving the integrity of distributed e-commerce systems must also follow these established concepts. Moreover, an e-business must protect its assets and privacy not addressed directly by ACID. Thus, we add authorization, authentication and confidentiality, resulting in the ACID-AAC property list:

- **Atomicity.** A transaction's changes to the state are atomic: either all happen or none happen.
- **Consistency.** A transaction is a correct transformation of the state. The operations taken as a group do not violate any of the integrity constraints associated with the state.
- **Isolation.** Even though transactions are executed concurrently, it appears to each transaction that, others executed either before it or after it, but not both.
- **Durability.** Once a transaction completes successfully (commits), its changes to the state survive failure.
- **Authorization.** A transaction is only executed upon proper approval.
- **Authentication.** Entities involved in a transaction are proved as what they claim to be.
- **Confidentiality.** A transaction is kept secret from unauthorized observation.

A simple and common example for explaining ACID relates to bank transactions. A cash withdrawal is atomic if it both dispenses money and reduces your account. It is consistent if the cash dispensed equals to the account reduction. It is isolated if the withdrawal is unaware of other transactions accessing your account concurrently (e.g., a deposit). And it is durable, if, once the transaction is complete, the account balance is sure to reflect the withdrawal.

The atomicity of a state transition ensures that a transaction is not out of control no matter whether the involved processes function normally, abnormally, or crash. This is crucial for Internet transactions as many things can happen before a transaction can commit: e.g., the connection may be broken, the server may be overloaded or crash, the buyer may decide to cancel. If a system is defined in the units of atomic transactions, the system can return to the previously committed state no matter what may occur.

The integrity of each transaction (governed by atomicity and consistency), the seamless integration of transactions (isolation), and the fault-tolerant acknowledgement of each transaction (durability), help to ensure the integrity of a system, that is, the satisfaction of system properties and specifications, after each transaction.

Traditional control principles reflect some of the ACID concept. For instance, the rule of "every event is properly recorded" is implicit in its design of atomic and durable transactions. However, traditional accounting transactions often assume the involvement of only two parties: the sender and the recipient. Operations requiring multi-parties' engagement are often serialized into two parties' transactions. This "delay" enhances controls but sacrifices efficiency. However, the *two-phase commit protocol* in distributed computing allows for the achievement of all-or-nothing agreement among multiple independent but concurrent processes. A coordinating process collects votes from participating processes and coordinates the commit action. Isolation ensures the sequential logic execution of competing transaction related to the same resource although it may appear to end users that they are concurrent. In this way, both control and efficiency are achieved.

Although ACID aids in the fight against errors, unexpected faults, or crashes in e-systems, computer designers have often assumed the benign behavior of involved entities. We know this assumption to be false. Given a potentially malicious e-commerce environment, the added AAC properties further emphasize the need for ensuring the appropriateness and privacy of certain business transactions. Although achieving AAC is not a new concept for e-commerce, its importance remains.

In sum, drawing system boundaries and determining control and assurance dependence support the definition and scope of system properties and specifications. Furthermore, defining atomic transactions allows for design specifications at the level of manageable units. Defining ACID-AAC properties guides the detailed implementation in the following phases.

Applying Model Checking in SDLC Phases III, IV, and V: System Design, Development and Implementation

System design, development, and implementation realize the conceptual design in information systems, including hardware and software. Our main concern here is with software quality. As we discussed previously, e-system designers and assurers need the quality assurance at the Internet infrastructure and application layers, choosing reliable networking products¹ and services, robust operating systems², reliable databases, and qualified Web commerce development tools. We wish most of these quality assurance can be purchased in the market in the near future. If so, the correctness of an e-business system will primarily depend upon the design and coding of e-business processes. This is not easy. For instance, on June 8, 2001, trading at the New York Stock Exchange halted for one hour and twenty minutes due to some software changes made in the NYSE's computing system. How to ensure the coding of business software or any change in the existing system actually implement intended functionalities?

We suggest that e-commerce designers and developers run a formal verification process similar to how computer scientists implement critical software and design chips. Such a quality assurance process should start at the very beginning of programming. Otherwise, a late remedy will be much more costly and difficult. The traditional approach relies upon testing and simulation, which often occurs only after software implementation and just prior to product delivery. It not only occurs too late but also has inherent limitations. Testing and simulation can only cover a small portion of all possible executions, but dynamic and real-time interactions in e-commerce have substantially enlarged the execution space. Moreover, effective testing and simulation require the development of test benches that can execute crucial execution paths. This development not only demands in-depth expertise, but is also inefficient and error-prone.

In contrast, formal verification is the most rigorous quality assurance method for software. "Formal verification conveys a promise of mathematical certainty . . . If a model is formally verified to have a given attribute, then no behavior or execution of the model ever can be found to contradict this" (Kurshan 1995). The formal verification spectrum ranges from manual proofs, computer-aided theorem-proving, to automated model checking. Due to its high level of automation and efficiency, model checking is the most suitable method to verify e-business systems.

The traditional auditing approach is a very distant from formal verification; it largely depends on post testing and simulation in the sense that it samples after-the-fact data and applies computer programs, commonly based on a spreadsheet or similar technology, to facilitate data collection and analysis. Even the most advanced EDP auditing techniques continue to extensively rely on the fundamental reasoning power of the auditors to construct tests and assess evidence. Extant techniques still primarily qualify as manual forensic testimony. For complex e-business systems, this can be extremely tedious and error-prone. Error is

almost assured due to the long list of properties and specifications to check. This problem is not unique to auditors. Chip designers and telecommunication software developers have already encountered these same problems. They have turned to the combination of intensive testing and simulation together with formal verifications. Their experiences suggest that it is not realistic to expect manual observation, testing and simulation, and judgment based on the auditors' experience and knowledge to result in credible assurance over nonstop, large-scale and highly interactive e-business systems. But formal verification can help.

Several of the current authors have previously advocated an alternative, automated approach to reasoning about business systems, particularly accounting internal control systems (Duke, Gerlach, Ko, Meservy, Bailey, Jr and Whinston 1985, Gerlach et al. 1981). The basic idea is that certain important properties associated with business transactions are verifiable by automated reasoning through computation. Model checking is a further extension and efficient fulfillment of this idea.

We demonstrate how to apply model checking in (Wang et al. 2000). The main concept is that system properties and specifications can be automatically translated from human language into rigorous temporal logic, and process models can be automatically interpreted as automata. Computation between mathematical logic and process automata can verify whether these processes satisfy the described properties and specifications. We programmed an online ticket-sales prototype and verified the correctness of its design and implementation by using VeriSoft and SPIN model checkers. In our example, model checking has been proven to be a rigorous control and assurance tool for e-businesses. It found errors, such as deadlock, which are often missed by designers but exploited by hackers to launch Denial of Service attacks. Model checkers can show how these errors can occur, which helps designers to fix the problems.

Although, in current industrial practice it rarely occurs that a software package, whether for e-business or others, is thoroughly examined before its delivery, we believe that this practice will have to change, especially for software that carries out crucial business functions. Model checking can serve as a popular tool for this thorough examination.

Introducing Real-time Monitoring for SDLC Phase VI: System Maintenance

In the system maintenance phase, the new system is placed in a real-world execution. While economic reasoning, atomic transaction design, and model checking aim to ensure system integrity from design to implementation, how the system actually performs remains a real concern.

We suggest that embedded sensors be included in the system and monitors be used to collect real-execution information in order to coordinate transactions and verify system properties in real-time. For instance, vector clocks can be embedded in e-processes and the real-time analysis of events and their associated vector clock value can provide meaningful system snapshots (Coulouris, Dollimore and Kindberg 1994).

/Insert Figure 3 here /

Figure 3 illustrates the design model of a Real-time Assurance Monitor (RAM). Sensors are embedded in the monitored system and report the occurrence of events and their associated vector clock value to the RAM server. These event notifications and vector clock values are accumulated in a buffer to wait for further processing. The causal delivery monitoring process scans the buffer for events that are ready to be analyzed. An event is ready to be analyzed only after all of its preceding events have already been analyzed. Vector clock values help determine the causal relationship among events, which depicts the logical ordering among process executions rather than the actual occurrence. Every time a new event is analyzed, a snapshot of the global state of the monitored system is updated. Predicate evaluation on global states checks whether system properties are satisfied in the actual execution. Assurance reports are automatically generated and presented on the Web to authorized auditors and managers. Exceptions found by RAM are processed by the warning system. Feedback is given to the monitored system and if necessary, alarms are sent to the proper personnel in real-time.

The RAM server and the communications between RAM and the monitored system must be administered with high level security and reliability. Any fraud of them circumvents the independence and credibility of assurance results. Sensors and monitoring processes can be implemented in agent technology like Java. No matter what technology is chosen, again, the security of the technology must be warranted.

Summary of PACCAF

Since model checking cannot verify every system property due to its cost and inherent complexity, some of the system behavior has to be verified through other means like real-time monitoring. Model checking can handle non-determinism and verify every possible execution path, however, real-time monitoring only needs to verify what the actual execution is. Each of these two methods has its own advantages and their combination can deliver more complete assurance. In fact, all of the four suggested methods complement each other and should be applied iteratively in SDLC to enhance the completeness, relevance and reliability of controls and assurance.

Alan MacCormack and Iansiti (2001) discuss a more flexible system development process for Internet applications. Actually, this new process is essentially SDLC but allows its phases overlapping to certain extent to encourage earlier user feedback and hence better respond to new or changing system requirements. Such variation to SDLC, as well as other system methods (e.g., prototyping), require some adjustments on how to use PACCAF. It is not difficult. Developers can simply apply our methods whenever feel appropriate.

THE ROLES OF THE AUDITORS

Providing trust services for the digital economy is a competitive arena. Controllers and assurers must be clear on what sys-

tem properties and specifications are relevant to decision making and what cannot be omitted. Auditors are more experienced in judging such relevance and completeness than any other potential trust provider, such as IT vendors. In general, auditors have more understanding about business decision contexts and know better what to observe and how to report. Auditors have the “knowledge of the individual and aggregate effects of alternative standardized measurement and reporting structures” (Kinney, Jr. 2001a). Based on auditors’ knowledge and judgment on the criticality of a property, auditors can choose appropriate verification methods for measurement. Although our methods are supporting tools to refine system specifications to be more relevant and complete, auditors’ industrial and business domain expertise can serve as a credible starting point and a useful knowledge base that cannot be easily replaced by others.

Auditors should be the best advocates in promoting proactive, automated and continuous controls and assurance to top managers. Auditors’ traditional roles as trustworthy guardians and consultants to the board of directors and high-level managers have earned them a strategic position in advising firms. They impact “the tone at the top” and can potentially revolutionize e-business system development practices.

CONCLUSION

Risks are heightened in e-commerce due to the complexity, interconnectivity, automation and speed of digital processes. Applying the methods in our PACCAF control and assurance framework, namely economic reasoning, atomic transaction design, model checking, and real-time monitoring, in the System Development Life Cycle, will lead to proactive, automated and continuous control and assurance services. Only such services can prevent an e-business from experiencing errors, fraud, hacking, or even catastrophic failures. Successful operations of these methods will be a prerequisite for delivering the envisioned continuous, forward-looking assurance services in the future. Auditors, if equipped with these new methods, together with their credibility, independence and expertise, will contribute substantially to the integrity of the digital economy.

Notes

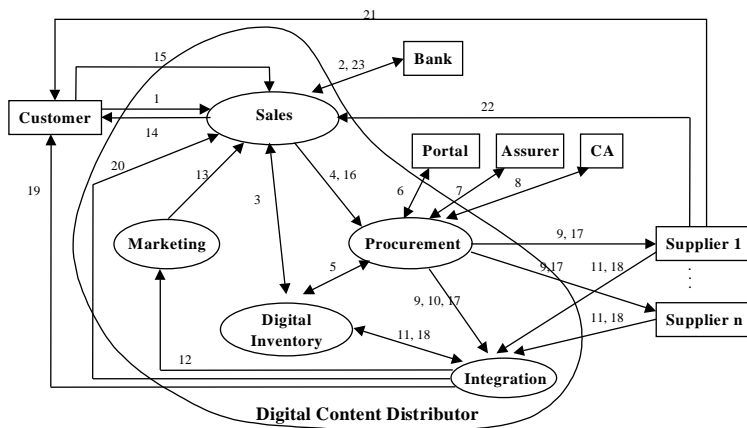
¹New York Stock Exchange, the biggest equities market in the world, was halted for 59 minutes on October 26, 1998 due to a faulty switch in the network.

²“Code Red” worm and the like exploit weaknesses in Microsoft Internet Information Servers.

REFERENCES

American Institute of Certified Public Accountants, *Report of the Special Committee on Assurance Services*, <http://www.aicpa.org/assurance/index.htm>, 1996.

- ____, *AICPA/CICA SysTrust Principles and Criteria for System Reliability* April 2000. exposure draft, version 2.0.
- Bailey, Jr., Andrew D.** “AICPA/CICA SysTrust Principles and Criteria for Systems Reliability – Discussion and Remarks.” *Journal of Information Systems*, 2000.
- Barua, Anitesh and Whinston, Andrew B.** *Measuring the Internet Economy*, www.internetindicators.com, 2000.
- Coulouris, G.; Dollimore, J. and Kindberg, T.** *Distributed Systems: Concepts and Design*, second ed., Addison-Wesley Publishing Company, 1994.
- Duh, Rong-Ruey; Jamal, Karim and Sander, Shyam.** “Control and Assurance In E-Commerce: Privacy, Integrity and Security at eBay,” April 2001. working paper.
- Duke, G.; Gerlach, J.; Ko, C.; Meservy, R.; Bailey, Jr, A. D. and Whinston, A. B.** “TICOM and the Analysis of Internal Control.” *The Accounting Review*, April 1985, pp. 186–201.
- Gerlach, J.; McAfee, R. P.; Bailey, Jr, A. D and Whinston, A. B.** “Internal Accounting Controls in the Office of the Future.” *IEEE Computer*, May 1981.
- Gray, J. and Reuter, A.** *Transaction Processing : Concepts and Techniques*, Morgan Kaufmann Publishers, 1992.
- Harvey, Ernest.** “Building Your E-business Applications.” <http://www.developer.ibm.com/devcon/augcc00.htm>, August 2000.
- Kinney, Jr., William R.** “Accounting Scholarship: What Is Uniquely Ours?” *The Accounting Review*, April 2001, 76 (2).
- ____. “Research Opportunities in Internal Control Quality and Quality Assurance,” 2001. working paper.
- Kurshan, R. P.** *Computer-aided Verification of Coordinating Processes*, Princeton University Press, 1995.
- Laudon, Kenneth C. and Laudon, Jane P.** *Essentials of Management Information Systems: Organization and Technology in the Networked Enterprise*, fourth ed., Prentice-Hall Publisher, 2001.
- MacCormack, Roberto Verganti Alan and Iansiti, Marco.** “Developing Products on ‘Internet Time’: The Anatomy of a Flexible Development Process.” *Management Science*, January 2001, 47 (1), 133–150.
- Meinel, Carolyn.** “Code Red: Worm Assault on the Web.” <http://www.ScientificAmerican.com/explorations/2001/073001codered/>, July 30, 2001.
- Myerson, Roger B.** “Optimal Auction Design.” *Mathematics of Operations Research*, February 1981, 6 (1), 58–73.
- Nagel, Karl D. and Gray, Glen L.** *Electronic Commerce Assurance Services – Electronic Workpapers and Reference Guide*, San Diego, New York, Chicago, London: Harcourt Professional Publishing, July 1999.
- Riley, John G. and Samuelson, William F.** “Optimal Auctions.” *The American Economic Review*, June 1981, pp. 381–392.
- The Internet Fraud Watch.** “2000 Internet Fraud Statistics.” <http://www.fraud.org/internet/lt00totstats.htm>, 2001.
- Wang, Wenli; Hidvégi, Zoltán and Whinston, Andrew B.** “BVA – A Protocol Against False-name Bidding in Multi-unit Auctions,” June 2001. working paper.
- ____; ____ and ____ . “Shill Bidding in English Auctions,” April 2001. working paper.
- ____; ____ and ____ . “Designing Mechanisms for E-Commerce Security: An Example from Sealed-bid Auctions.” *International Journal of Electronic Commerce*, forthcoming.
- ____; ____; **Bailey, Jr., Andrew D. and Whinston, Andrew B.** “E-process Control and Assurance Using Model Checking.” *IEEE Computer*, October 2000, 33 (10), 48–53.
- Weinberg, Neil.** “Fear, Greed And Technology.” *Forbes Magazine*, May 15, 2000.
- Yokoo, Makoto; Sakurai, Yuko and Matsubara, Shigeo.** “Robust Combinatorial Auction Protocol against False-name Bids,” in “The proceedings of the 17th National Conference on Artificial Intelligence” August 2000, pp. 110–115.



1. Customer fills in request forms with specifications, preferences and credit card information.
2. Sales checks the customer's credit through banking systems.
3. If the customer has good credit, sales checks the digital inventory to see if it has all the necessary components.
4. If further purchase is needed, sales forwards the corresponding requests to procurement.
5. Procurement queries digital inventory about who are the existing suppliers that can potentially supply the components.
6. If new suppliers are needed, procurement launches search agents, who search portal sites, find best match, and make up a list of URLs of new suppliers.
7. Procurement obtains assurance of suppliers.
8. If the supplier has good credit, procurement obtains assurance and the certified public key of the supplier from a creditable certificate authority.
9. Procurement makes requests to suppliers, both existing suppliers and new ones, and notifies the integration department.
10. Procurement provides assurance and public key information to integration.
11. Suppliers provide product and service information, including price and availability etc., to integration. Integration obtains existing component information from the digital inventory.
12. Integration briefly bundles component information into different final product packages with corresponding costs, delivers the package information to marketing.
13. Marketing decides price, creates a catalog customized to the customer's request and forwards the catalog to sales.
14. Sales delivers the catalog to the customer.
15. Customer selects and orders.
16. Sales notifies procurement of the final order.
17. Procurement notifies necessary suppliers and guarantees future payment to them.
18. Suppliers provide components to integration and integration obtains other necessary components from the digital inventory.
19. Integration bundles components into the package that the customer ordered and delivers the final package to the customer.
20. Integration notifies sales about the successful delivery.
21. This step is needed in case there is a need for the supplier to directly offer its services to the customer as part of the order fulfillment.
22. This step is needed if step 21 is executed. The supplier notifies the sales of the fulfillment of its direct services.
23. Sales receives payment from customer's bank.

Figure 1. An e-business model of a digital content distributor

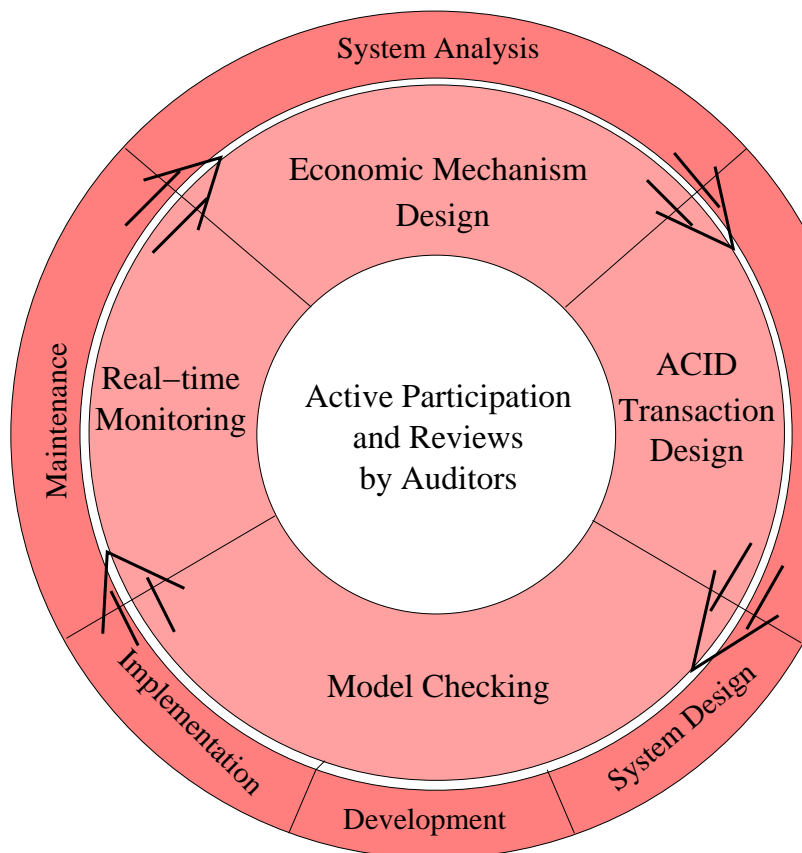


Figure 2. A Proactive, Automated, Continuous Control and Assurance Framework (PACCAF)

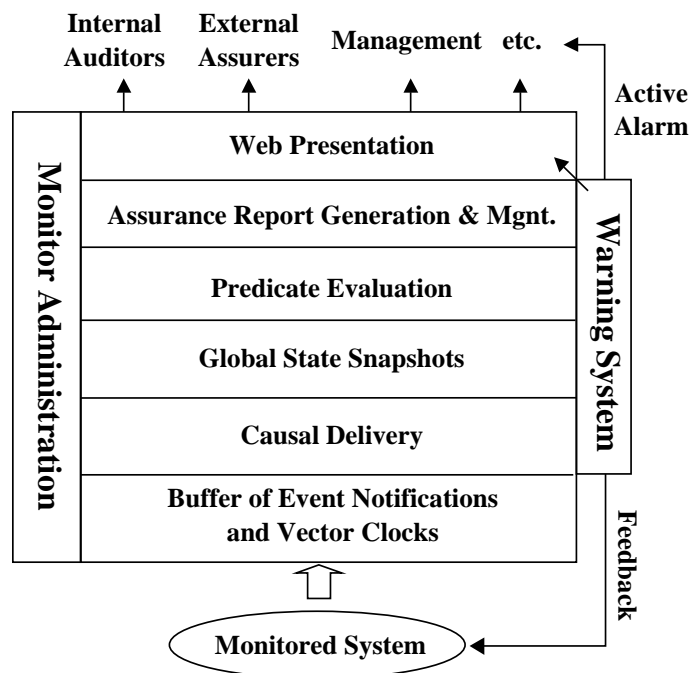


Figure 3. A model of a Real-time Assurance Monitor (RAM)