Cyber Infrastructure for Effective Deployment of Environmental Management Systems

Andy Srinivasan, Bayer Material Sciences (Baytown, TX)
Tim Aldredge, Eastman Chemicals (Longview, TX)
Jeremiah O'Brien, Process Data Control Corp (Arlington, TX)

Introduction

Title V of the Clean Air Act, as amended in 1990, changed the way industrial plants and other sources of air emissions were regulated in the past. First, it requires most industrial facilities to obtain a federal operating permit and agree to report all deviations from applicable regulations at least twice per year. A responsible company official must certify compliance with all rules each year. Second, it imposed significant penalties for non-compliance, including the shutdown of plants, criminal penalties, and fines. It has been said that companies trying to comply with their Title V permits are "guilty until proven innocent." For many permit holders, the standard of "proof" for Title V compliance is virtually 100% documentation of the data needed to confirm that all requirements were met during all operations subject to the permit.

The Sarbanes-Oxley Act of 2002, which was passed by Congress in response to public calls for corporate accountability following the demise of WorldCom, Enron, and others, raised the stakes of compliance management even higher. It requires public companies to disclose information that could affect potential environmental liabilities. Inaccurate reporting of environmental liabilities can lead to a false assessment of corporate value, which may cause problems for investors, insurance underwriters, lenders, taxing authorities, and others who depend on this information. According to a U.S. EPA report published in 1998, 74% of companies failed to disclose on their Form 10-K's one or more environmentally related legal proceedings that could result in fines in excess of $100,000. This widespread failure to report liabilities is in violation of Securities and Exchange Commission regulations that require full disclosure of "material effects of compliance with environmental laws" on a business, as well as "any known trends, demands, commitments, events or uncertainties" that are reasonably likely to have a material effect on a company's bottom line.

So what does this new, heightened level of environmental compliance and reporting mean to the design, operation, and support of computer systems that facilitate compliance? Among other things, it means that the infrastructure underlying these systems must be reliable, flexible, and fully capable of meeting stringent performance requirements. Access to the information that proves compliance, and the ability to incorporate the effects of changing requirements in the management system, are also key requirements. To meet this demand, infrastructure must be web-centric– i.e., robust and efficient within a cyber (web) infrastructure. This paper reviews these requirements in detail to evolve a vision of the cyber infrastructure that meets the needs of industrial facility managers.

What is Cyber Infrastructure – and Why Do We Need It?

Cyber infrastructure refers to the supporting elements that underlie computing systems and the "glue" that enables efficient interfacing of systems and databases to solve problems. It is analogous to the foundation and framing of a house – i.e., building elements that are unseen in the finished product but critical to its success. "Success" related to Title V compliance is measured by the effective and efficient functioning of management systems that assure all requirements have been met within defined cost and manpower parameters. Cyber infrastructure is a network of components and policies that support a positive outcome of the

company's environmental compliance program, including web components (Intra- and Internet) and e-mail.

In her keynote address to the Supercomputing 2002 conference in Baltimore, National Science Foundation Director Rita Colwell said that a "robust, flexible and comprehensive cyber infrastructure will give us the foundation we need to make rapid progress… [and gain] access to high-performance computing, high-bandwidth networks, very large data stores, and sophisticated tools for knowledge discovery." Examples of cyber infrastructure mentioned by Director Colwell included the Grid Physics Network, Earthquake Engineering Simulation, and the Human Genome project. The power of cyber infrastructure is especially germane to life sciences, where Director Colwell mentioned that the folding of proteins used to take 20 months to simulate, but may today be done in one day at 1 trillion operations per second. "We will need the power of supercomputing and the integration and insight that a comprehensive cyber infrastructure provides to untangle these complex interactions," she said.

The monitoring, reporting, and recordkeeping of data needed to confirm compliance with environmental rules might not approach the complexity of the human genome. However, there are several parallels. For example, in many areas of the country, the right to emit certain types of chemicals – oxides of nitrogen and volatile organic compounds, in particular -- may be banked, traded, bought, and sold under a novel "cap and trade" strategy supervised by the state regulatory agency. The idea is to create a "cap" for an area that comprises site-specific allocations of pollutant emissions across a broad spectrum of industries. The amount of emissions discharged from specific facility locations are not viewed as a problem so long as the total emissions in the area remain below the "cap."

Although cap and trade programs offer flexible alternatives to companies that must comply with air emission limits, they require considerable computing resources to simulate the economics of compliance under all available options. These projections must also take into account the decrease in allocations that are mandated by air quality modeling conducted by regulatory agencies. Companies subject to cap and trade programs must consider plant decommissioning and construction projects (schedule, scope, etc.), emission rates of selected equipment affected by plant changes, site-wide emissions, the expected economic value of emission allocations, production requirements, and market demands – perhaps not the 500 million trillion sequence comparisons required to identify the human genome, but more complex than traditional environmental measurements.

The calculation of short-term air emission rates is another area where computing power, networking, and database integration is required. Some industries are required to perform complex emission calculation formulas every hour to confirm that emissions from regulated equipment did not exceed a specified limit. The inputs for these calculations include operating parameters such as pumping rates, fuel usage, and material throughputs – all of which may be available from process historian databases that record data continuously from process control systems. Cyber infrastructure can efficiently support the retrieval of these parameters, emission calculations, comparisons of results to regulatory limits, and pager or e-mail notifications to designated staff members when problems are identified. Figure 1 describes how information flows through a Title V Compliance Assurance System, from applicable rule determinations and task definitions, to confirming and certifying compliance.

Federal operating permits usually encompass numerous local, state, and federal citations, as well as other types of requirements that are “federally-enforceable,” such as cap and trade programs. All states are required to submit State Implementation Plans (SIPs) to the U.S. EPA that summarize the methods and strategies that will be used to meet the ambient air quality standards established by the Clean Air Act. Because SIPs are “federally-enforceable,” virtually all rules and regulations imposed by state agencies fall into the same category. Consequently, federal operating permits tend to be extremely thorough and comprehensive with respect to air quality, and may even include rules related to wastewater and solid waste disposal to the extent that air emissions may occur from these types of operations.

In a typical oil refinery or integrated chemical plant, the number of governmental rules that apply to plant equipment and processes often exceeds 50,000 discrete regulatory citations and permit conditions. Each of these rules has the potential of requiring one or more actions to achieve or demonstrate compliance. The capability of environmental compliance systems to track the performance of these tasks will determine, more than anything else, the ultimate success or failure of a Title V compliance program. It is, therefore, advisable for companies to understand what constitutes a compliance task (see Glossary at end for a definition of this and other terms), and how best to manage data resulting from the performance of tasks over time. Cyber infrastructure will play a key role in supporting computer systems that are responsible for defining, scheduling, and tracking the results of these tasks.

Cyber infrastructure is more than technologies and systems. It also encompasses policies developed by system managers to facilitate smooth operations. The importance of policies on determining the effectiveness of cyber infrastructure cannot be overstated. Computer systems may define what is possible, but policy makers define goals and strategies. Frequent reviews and updates of company policies should be a formal part of any cyber infrastructure deployment plan. Required services for cyber infrastructure operations, such as training and support services, are essential to efficient functioning of compliance systems and should be included in the overall plan for implementing and maintaining cyber infrastructure.

Profile of Cyber Infrastructure Requirements for Environmental Compliance

In a press release dated February 13, 2004, entitled “Cyber Infrastructure Poised to Revolutionize Environmental Sciences and Other Disciplines,” Margaret Leinen, head of National Science Foundation Geosciences directorate, explained how cyber infrastructure is being used to solve real world problems. "New instrumentation, data-handling and computation capabilities will expand the horizons of what we can study and understand about the environment," she said. "Cyber infrastructure is empowering [us] to unravel how the world around us works." Other researchers were quoted in the press release as saying that ”the convergence of information and communication technologies... is poised to revolutionize the environmental sciences and many other disciplines in the coming years. In environmental science, cyber infrastructure combines computation, information management, networking and intelligent sensing systems into powerful tools… to investigate the natural world and the human-built environment in their full complexity.”

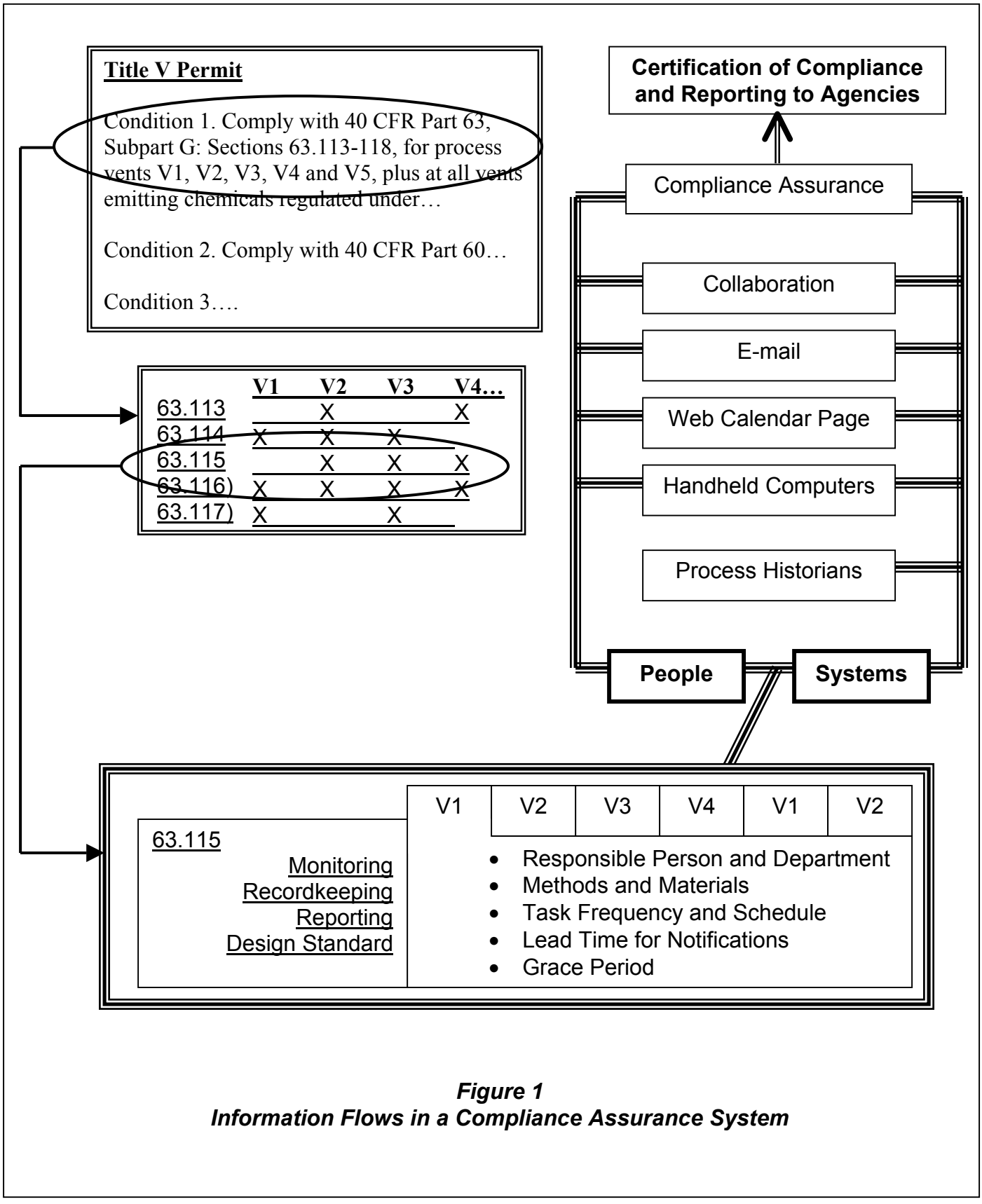

Figure 1
Information Flows in a Compliance Assurance System

This view of cyber infrastructure, i.e., as a merger of computing, networking, and intelligent sensing, is especially pertinent to Title V compliance. Computing resources are needed to cope with the large volumes of data that must be collected to assess and prove compliance. Networking and distributed databases that utilize web technologies are necessitated by the fact that input is often required from operations, maintenance, legal, management, accounting, and other parts of an organization. Intelligent sensing is increasingly being employed by facilities that utilize sophisticated control systems and process historians to track data from instruments, gauges, and other sensors in the manufacturing environment. Bringing all of these technologies and resources together to achieve compliance is both the definition and mission of cyber infrastructure.

Standard operating procedures (SOPs) are often used to define tasks for operations and maintenance of plant equipment in the same way that airline pilots use take-off checklists, i.e., to make sure that all steps are followed and nothing is left out. While many compliance tasks may also be effectively managed under an SOP, there is an important difference between this and other types of SOPs, namely: the regulatory requirements that "drive" each task must be an integral part of the management system. Otherwise, tasks defined at one point in time may continue to be performed regardless of whether the related regulations have been amended by the agency, or eliminated altogether for specific equipment or processes due to a change in rule applicability.

The applicability of rules is rarely a static element of the system because equipment and manufacturing processes are continuously being modified and upgraded, which, in turn, have the potential of dropping some requirements and adding new ones. Thus, compliance tasks are subject to change at any time. The speed with which the need for modifications is identified and changes are implemented is an important aspect of Title V compliance. Title V permits require that compliance tasks be updated within 30 days of a rule amendment, or immediately if updates are needed because of a process modification. Cyber infrastructure should enable system administrators to detect when updates are needed, define the changes that are required, and make changes efficiently and reliably without jeopardizing historical data that has been collected from the performance of compliance tasks.

Applicability determinations often involve a myriad of factors, each requiring specific data about the design and operation of plant equipment. For example, a storage tank may be subject to a certain rule only if it contains organic liquids, was built after a certain date, is larger than a certain size, or has a certain type of roof. To effectively manage changes in equipment and processes that may impact applicability, the compliance system should provide logical rules for interpreting how equipment and process parameters affect regulatory applicability. This perspective can be characterized as a chain with three links, as shown in Figure 2, below.

Figure 2

Figure 2 describes the basic system elements involved in defining all of the tasks that will be needed to assure and maintain compliance. Cyber infrastructure must support these three elements effectively and reliably in order for the tasks to be identified, defined, assigned, scheduled, and kept up-to-date. Compliance documentation will flow directly from these task assignments and from actions taken to correct or minimize the impact of deviations from applicable rules. Important cyber infrastructure components for defining compliance tasks and schedules are:

- Database Platform – consisting of data tables and the content stored in them
- Text Parsers – to intelligently break down regulatory text into tasks
- Networks – to maintain connectivity between the database, web server, mail server, applications, and other critical components, for local and remote users
- Web Page Hosting – to disseminate information about rule applicability and tasks
- E-mail Notifications – to enable collaborators to exchange information
- Services – primarily training on how to use software and web pages that have been provided to determine rule applicability determinations and define tasks
- Policies – management-level guidance on the level of detail and staff assignments

Not all compliance tasks will be assigned directly to individuals or systems for routine updates. Companies usually group tasks with similar compliance periods and assigned staff in order to streamline recordkeeping and reduce the volume of data updates to a manageable level. These task groups are an important part of the "set-up" process.

Once tasks have been defined, grouped, scheduled, and put into a production system that manages the results obtained from performing tasks over time ("history"), a second three-link chain emerges. This chain reflects the collection, processing, analysis, and reporting of task results to regulatory agencies, as shown in Figure 3, below.

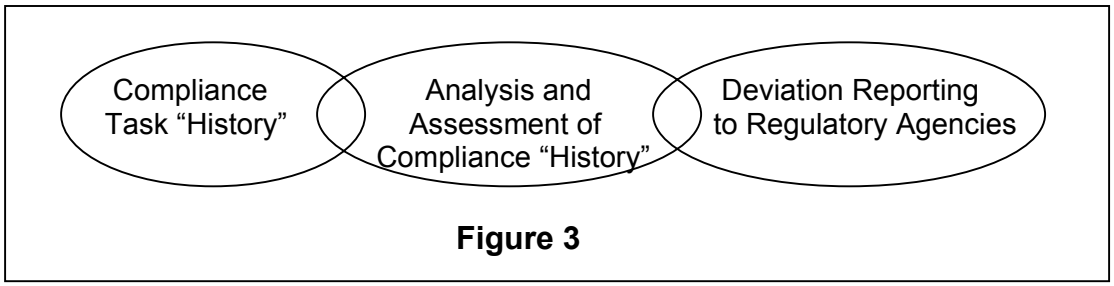

Figure 3

Important cyber infrastructure components for managing task "history" are:

- Database Platform – as stated above plus web page hosting
- Networks – as stated above plus connectivity with process historian server, handheld computers, software applications for reporting and analysis.
- Web Page Hosting – as stated above plus to enable users to view calendar pages showing upcoming tasks, review task "history," and produce reports
- Remote Sensing Devices – to update task "history" directly from instrumentation
- Hand-held Computing – to enable users in the field to access and update compliance data, as needed, using portable data entry devices
- Process Historian and Distributed Control System Interfaces – to launch queries for data stored in process historians and other on-line data sources

- E-mail Notifications – to advise company staff when tasks are due, or to notify staff of late/missing tasks and potential deviations that have been recorded
- Services – primarily training on how to use software and web pages that maintain task "history" and manage change in applicable rules and task definitions
- Policies – management-level guidance on how "history" should be collected and assessed to enable Title V deviation reporting and tracking of corrective actions
- Job Scheduling – i.e., to manage components that will operate at a specified time
- Security and User Authentication – to ensure that date is viewed and altered by approved staff members only, and that system backups are done reliably

Because many industrial facilities employ the same types of equipment located in several areas of the plant, compliance task definitions derived from the same applicable rules will be applied many times across the facility. Equipment-specific tasks are usually similar, but not always the same, because of subtle differences in equipment size, age, type of service, and other factors. To ensure that compliance is maintained, these differences must be respected in the definition, method, schedule, and other task attributes. Cyber infrastructure can assist in this area by enabling managers to identify those tasks likely to be affected by specific rule changes and process modifications, and enabling prompt implementation of needed updates to the compliance management plan.

Defining "generic" tasks for applicable rules is often an advisable first step in the process of developing a facility compliance management plan. Generic tasks, which provide a "default" definition of the compliance activities for a regulation, can accomplish several objectives. First, they reduce unnecessary variations in the way compliance tasks are performed. Second, they allow the use of systems to identify tasks that may need to be updated when a rule or its applicability is altered. Third, if the initial set of task modifications is made at the generic task level, managers can modify equipment-specific tasks selectively based on generic task updates. Figure 4, below, shows how changes can affect the components of a compliance management system. The main "layers" and components of cyber infrastructure are shown in Figures 5 and 6, respectively.

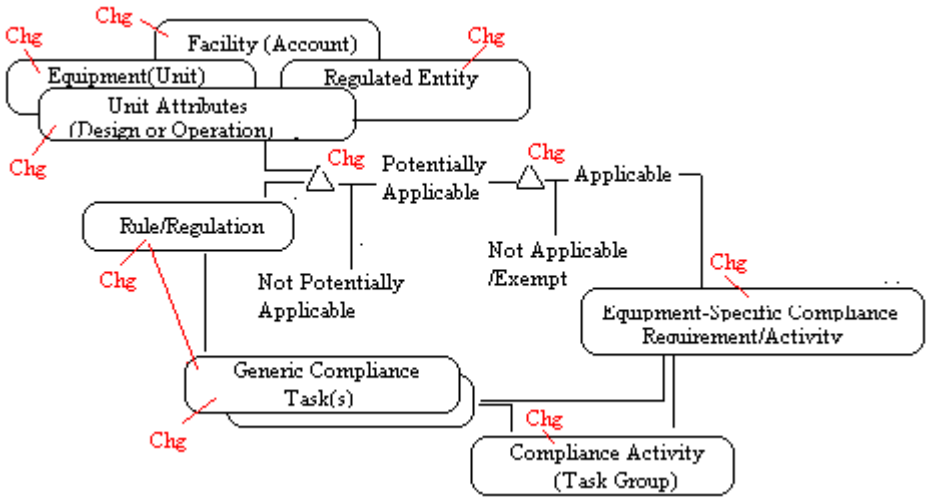

Figure 4

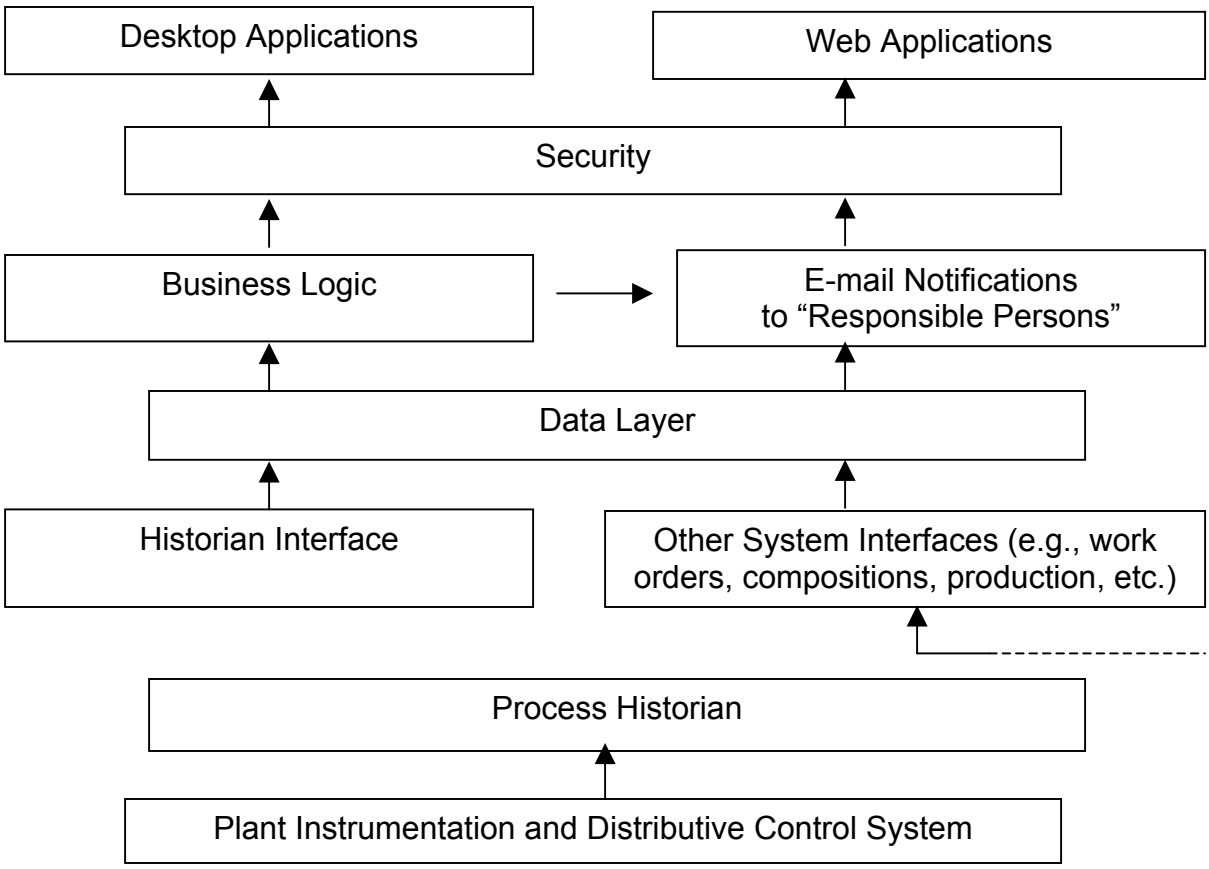

Figure 5
Cyber Infrastructure Layers

Documenting the chain of custody of compliance "history" data is extremely important to the future use of this information, and must, for that reason, be well supported by cyber infrastructure. Admissibility of electronic evidence in a legal proceeding is dependent upon the ability of a company to establish when data was collected, updated in the database, and modified, and by whom. Consequently, multiple persons and action dates may constitute the chain of custody information that must be documented. The individual's names, action dates, and relevant comments on why changes were made are crucial data that must be stored and verified in a manner consistent with the generally accepted standards.

Future Demands on Cyber Infrastructure

As compliance systems and databases become more powerful and efficient, cyber infrastructure must continue to provide reliable and effective operations in all areas, e.g., mass data storage, networking, access to computing resources, and interfaces with on-line data and systems. Training and other services, as well as policy guidance, must keep pace with the growing power and extent of compliance systems.

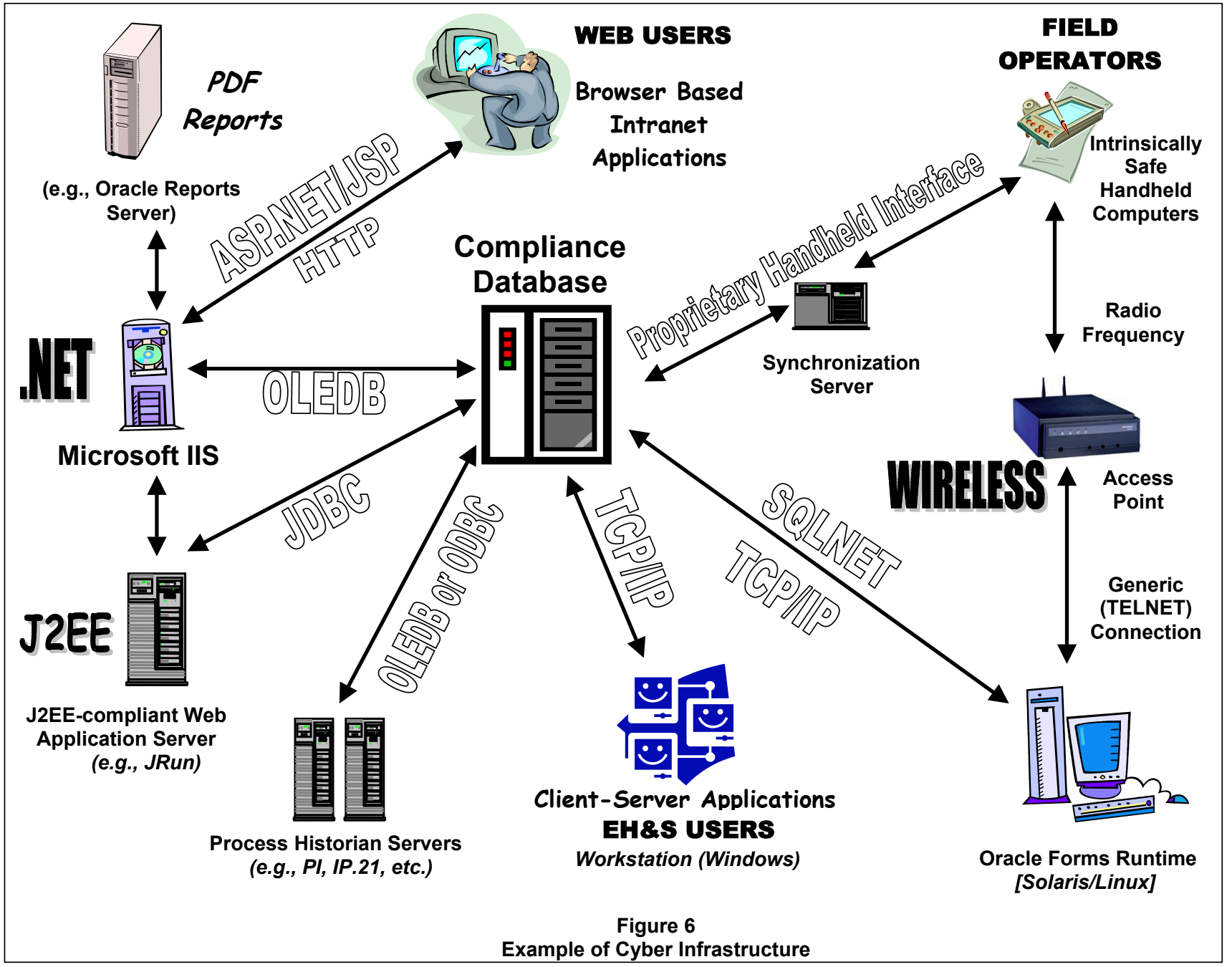

Figure 6
Example of Cyber Infrastructure

Processing of database updates is a resource-intensive operation requiring a significant amount of bandwidth to transfer all of the data needed for each transaction. Viewing task ”history,” especially over web connections, requires extensive bandwidth due to the fact that many plants compile millions of “history” records each year. Figure 7, below, shows how the volume of “history” records can increase based on a hypothetical distribution of compliance tasks and equipment. In the future, bandwidth will need to be utilized much more efficiently or made available in much greater supply, or both, to meet these requirements.

Equipment and Number ()	Compliance Tasks	Task Frequency	“History” Records/Year
Boilers (4)	Monitor op. hours	Daily	1,460
Boilers (3)	Monitor fuel usage	Hourly	26,280
Tanks (75)	Monitor Throughput	Daily	27,375
Tanks (30)	Perform Seal inspections	Quarterly	120
Vents (50)	Monitor composition	Every 15 min.	1,752,000
Scrubbers (9)	Monitor water circ. rate	Hourly	78,840
		Total	1,886,075

Figure 7

Remote sensing of environmental data with little or no human effort is already an important part of Title V compliance in many plants, and all indications suggest that it will continue to evolve and mature. For example, new technologies will enable emissions from leaking valves, flanges, and pumps to be measured remotely (e.g., Fourier transform infrared spectrometry). “Smart” equipment is becoming available that will allow direct read-out of critical data, such as “smart valves” that inform a technician of the condition of the valve seals and maintenance history. Cyber infrastructure must support these new technologies when they reach the point of acceptance by industry and regulators.

Management of change will continue to be critical to compliance systems. Task lists must be constantly adjusted to reflect current compliance requirements based on rule applicability, operating status, and other factors. Any changes that are deemed necessary must be implemented without delay. Cyber infrastructure will be called upon to deliver up-to-date requirements for each piece of equipment, with all potential sources of change fully considered, evaluated, and reflected in these requirements. In addition, systems must be capable of rigorous audits with respect to any changes made to tasks and “history.”

Compliance management systems produce information that must interpreted by a company’s regulatory experts before the results are reported to regulatory agencies. For this reason, it is essential for compliance systems to provide information that can be understood and interpreted with minimal effort, thereby freeing up managers to focus on why compliance deviations have occurred and how they can be prevented in the future. Translating “raw” data into usable information for decision-makers is a crucial function of compliance systems.

Title V deviation reporting illustrates the inherent complexities of supporting compliance programs. The first step in preparing a deviation report is to retrieve “history” records for a six-month time frame, say, from January 1 to June 30. Should “history” be

retrieved only for tasks that were actually completed during this period, or should records for tasks completed later, but entered into the database during the period, be included? How about “history” for tasks that were started in March and completed in July, or started in November and completed in January? Should annual tasks that were completed in June be included in this deviation report, or in the next one?

Even when the data retrieval has been properly defined with regard to task completion dates, etc., there is also the important question of what constitutes a “deviation” from applicable rules. Should it include task results that were undetermined as to compliance, for example, or only to non-compliance results? How about tasks completed late, or “missing history” – such as when only four “history” records are found for a monthly task (instead of six)? Should the data retrieval exclude apparent deviations that may be excused due to an operating condition, such as a unit shutdown? How should deviations over an extended time period for very frequent tasks be shown and “counted?” These are only a few of the complexities involved in executing a very common retrieval of Title V compliance data.

Conclusions

Dr. Michael Nelson, Director of Internet Technology and Strategy at IBM, stated in a recent presentation that the infrastructure of the future “will be fast, everywhere, always on, natural, easy, intelligent, and trusted.” He argues that speed and pervasiveness have been the focus so far, but “incorporation into business activities means that computing systems must be easier to manage because there will not be sufficient human resources to ‘tend’ them. Systems will be self-configuring, self-optimizing, self-healing, and self-protecting.”

An evolving element of cyber infrastructure, called a “grid,” will hasten the day when cyber infrastructure is transformed into a self-managed and self-directed entity. According to Dr. Nelson, cyber infrastructure evolved from one-to-one connectivity characterized by e-mail communications, to one-to-many access via the web, and finally to many-to-many connectivity through collaborative tools and technologies. A grid extends many-to-many architecture to a level in which, when connecting to the grid, users have full access to a series of many-to-many systems. In academia, grids are evolving as a virtual supercomputer with distributed databases, applications, and services.

Web portals offer a user-friendly point of access to grids and other types of system configurations, enabling users to choose which applications to connect to and what data to display on portal screens. Cyber infrastructure will need to keep pace with web portals and grids that infuse organizations with almost limitless access to data, services, and resources, as well as the expanded security that will be required.

In an article entitled “Integrating the Human Infrastructure,” which appeared in a recent issue of Envision magazine, Rich Wolski (UC Santa Barbara) argues that human input is also crucial to cyber infrastructure. Advances in computing environments and utilization of resources "doesn't happen by itself," Mr. Wolski said. "You have to have experienced, dedicated people managing the system. It is the human infrastructure that is key to making cyber infrastructure work successfully." Thus, facility managers must strive for the best combination of effective software applications, flexible and reliable cyber infrastructure, and enlightened system administrators to meet the many challenges they will face to comply with Title V and other environmental regulations.

Glossary of Environmental Compliance Terms and Concepts

This section provides an expanded definition of the key terms paper for the benefit of readers who are not familiar with the jargon of environmental compliance systems.

1. Applicable Rule -- A local, state, or federal regulation, term, or condition from an environmental permit, air emission limit, Permit-by-Rule, agency directive or order, or any other requirement or restriction that applies to equipment or processes located at a facility.

2. Compliance Task -- A Compliance Task ("Task") is one of the following:

- an action that must be performed to maintain or achieve compliance;
- an informational item that is helpful in understanding a compliance requirement;
- a contingent action that must be performed when a deviation from a rule occurs; or
- an activity that comprises several discrete tasks (see Task Groups, below).

3. Generic Task -- A task can be described as being either a "generic" version or an "equipment-specific" version. Generic tasks have been defined directly from the text of a rule, with no consideration given to the details of equipment to which it may apply, or to the personnel that may be performing it. A rule can have only one set of generic tasks. Another way to look at generic tasks is that they contain the "default" attributes of a task.

4. Equipment-specific Task -- Equipment-specific tasks are generic tasks that have been assigned to specific equipment or units in the site. They may be identical to the generic version in all respects, or nearly identical with only one or two attributes that differ from the generic version, or quite different with even core attributes like Task Description and Frequency changed from the generic version.

5. Compliance Management Plan, or "CMP" -- The CMP for a site is the set of tasks that have been assigned to specific equipment or units which comprises all actions that, when performed as scheduled and using the methods and materials specified, will enable site managers to assess compliance with all applicable rules.

6. Compliance History, or "History" -- The "history" for a task refers to the results that were obtained after a task was performed during a specified time period. "History" is only collected for equipment-specific tasks (never for generic tasks), and always refers to a specific date range, such as the "task history for the last six months."

7. Deviations -- "History" records that indicate potential non-compliance with a term or condition contained in a Title V Permit are referred to as "Title V Deviations," and a report summarizing these events is required at least every six months. Additional data that must be reported for deviations include corrective actions taken and duration of the events.

8. Compliance Period -- The "history" for tasks that are periodic in nature (e.g., daily, weekly, annual, etc.) may be viewed as a record of compliance within a time frame that is determined by the task frequency. For example, the Compliance Period (date and time) for a calendar-year annual task in 2004 would be 01/01/04 00:00:00 - 12/31/04 24:00:00, regardless of when the task was actually performed.

9. Task Group -- Most site managers do not wish to collect "history" for each task. To streamline the collection of "history," it is often more convenient to group several tasks under a single Primary Task for which "history" will be collected on a routine basis. The term Secondary Task is used to describe those tasks that have been grouped under a Primary Task. A good example of a task group is a "unit walk-through," which is often performed at the beginning of each shift. The walk-through may be defined as a "Primary Task," while each of the sub-tasks performed during the walk-through may be defined as "Secondary Tasks."

10. Non-Periodic Tasks -- Not all tasks are performed on a recurring or periodic basis. Some tasks are continuous in nature, while others are performed only under specific conditions, such as the filling of a storage tank, or at start-up of a unit. "Non-periodic" refers to the fact that history cannot be expected to be have been collected at a recurring frequency, such as daily or weekly. They are, for that reason, among the most difficult tasks to track from a compliance standpoint -- precisely because the lack of history does not imply compliance, or non-compliance, with an applicable rule.