Functional Basics of Third-Party Alarm Notification Systems

Bridget A. Moorman and Tim Gee

About the Authors

Bridget A. Moorman, CCE, is president of BMoorman Consulting, LLC. Email: bridget@bmoorman.com

Tim Gee is a principal with Medical Connectvity Consulting. Email: tim@medicalconnectivity.com

Interest in third-party alarm notification systems continues to increase as clinicians work to improve alarm response and reduce adverse events in an increasingly busy and distracting patient care environment. These systems promise to unburden the clinician from the many portable devices they carry for communication and alerting purposes as well as to provide management of both alarms and clinicians. However, these systems have daunting infrastructure requirements as well as clinical workflow requirements. From a technical viewpoint, a basic understanding of the different functional components as well as required underlying infrastructure will better prepare clinical engineering professionals to assess the different vendors' systems as well as provide for proper implementation, support, and clinical expectation management.

Communication and Paging Systems

See Figure 1 for a functional diagram of a generic third-party alarm notification system. Each of the system's components is described in the following sections.

Signal Input Systems

There are different types of signal input systems. One is a medical device gateway, which facilitates communication with external systems such as alarm notification servers. This gateway can be supplied by a medical device vendor, a third-party medical device integration vendor (example vendors: CapsuleTech, Nuvon, iSirona) and/or a third-party alarm notification vendor. Device gateways send HL7 messages or proprietary messages to the alarm notification server. Both third-party medical device integration systems and alarm notification systems can acquire data from multiple medical device manufacturers' devices. Lastly, a nurse call gateway aggregates nurse call information and sends a proprietary message (often using a variation of the session initiation protocol [SIP] or telocator alphanumeric input protcol [TAP] communications protocols) to an alarm notification server.

Some might argue that these input systems are basically the same; however, based on actual interfacing capability and signals gathered at some of the interfaces, these are different types

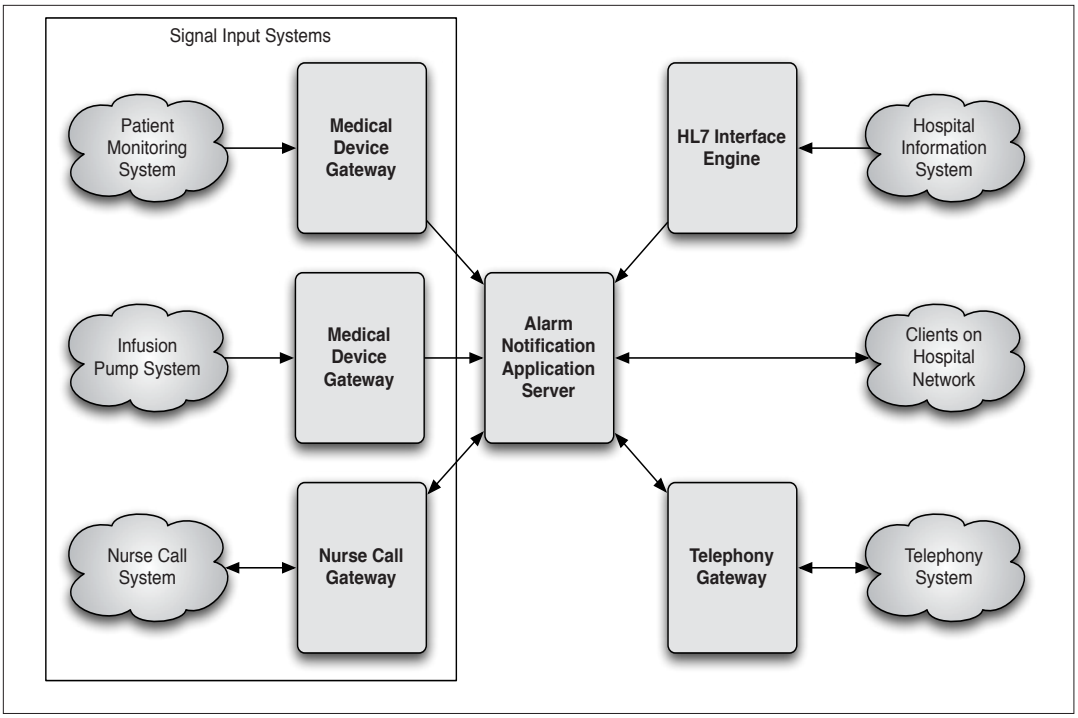

Figure 1. Block Diagram of Alarm Notification System, High-Level Functional View

of systems. For example, a nurse call system may use a simple on/off switching and signaling mechanism which minimizes the specificity of the information that can be propagated. In another example, a medical device gateway may send a 'snippet' of an arrhythmia waveform with the alarm notification.

Some medical device system interfaces are capable of two-way communication, such that a clinicians can remotely "silence" an alarm with acknowledgement at their communication device; usually this functionality is not implemented due to regulatory risk issues. The nurse call system interfaces are capable of two-way communication as well, such that acknowledgement by the clinician with the communication device will reset the nurse call system at the gateway and/or at the bedside annunciator.

The common data element providing context among data from various signal input systems is the patient. The association of patient identification with data from a signal input system is referred to as patient context. All of these components—both the signal input systems and the alarm notification server—must establish patient context to associate a patient with their data before sending information to the next component in the overall alarm notification system. Establishing patient context must be done by the signal input systems.

Common methods for establishing patient context include manually entering a patient's name and identification (ID) into the signal input system, using a barcode reader to capture the patient's name and ID, or having ADT (Admission Discharge and Transfer, a common information service available in hospital information systems) interfaces to the different gateways from which a clinician selects the patient demographic information. How patient context is established depends upon the vendors of each of the systems and how the provider configures their system at installation.

Alarm Notification Application Server

This server receives patient-identified information from the signal input systems. The alarm notification application server then looks up the assigned clinician for that particular patient as well as the assigned communication device for the clinician. This server may also filter an alarm by the signal input system generating the alarm because alarms from some devices, such as a ventilator or portable dialysis, may be routed to a technologist or clinician other than the patient's assigned caregiver. It then sends messages directly to the specific communication device specified by the alarm notification application. Messages sent to wireless phones are sent via the telephony gateway.

Most of the alarm notification application servers have a set of "rules" which are applied to the incoming signal. These rules allow message addressing and prioritization and are customized based on customer preference. Typically, the prioritization is based on alarm severity. In addition, triage scenarios can be defined such that message receipt and acknowledgement accountability can be attained. Moreover, there are some vendors in this space who offer decision support functionality in which multiple medical device inputs are analyzed and alarms messages are generated on a set of algorithms regarding the combined physiological information. A prototypical alarm notification server architecture is depicted in Figure 2.

This sample, high-level alarm notification server architecture diagram shows the main components of the server. The software architecture of alarm notification servers is similar across manufacturers. More mature systems, such as Amcom's CommTech Wireless solution, are mostly coded software; while more current platforms like Extension use highly configurable software "engines" for most of their functionality. All alarm notification servers include a database management system that stores data from input systems and logs all of the internal server transactions and interactions with endpoint devices and users.

In computing, an enterprise service bus (ESB) is a software architecture component that provides basic services for complex architectures via an event-driven and standards-based messaging engine, the bus. Some alarm notification systems utilize an ESB or may implement a Service Oriented Architecture (SOA) component. Systems based on SOA, such as Emergin, package server functionality as a suite of interoperable services defined by the SOA. Because SOA does not include the concept of events, systems using SOA include a separate messaging engine. The ESB or messaging engine performs message triage, routing, and escalation based on how it is configured. A rules engine may be included to provide clinical decision support in processing input system data, generating and managing messages.

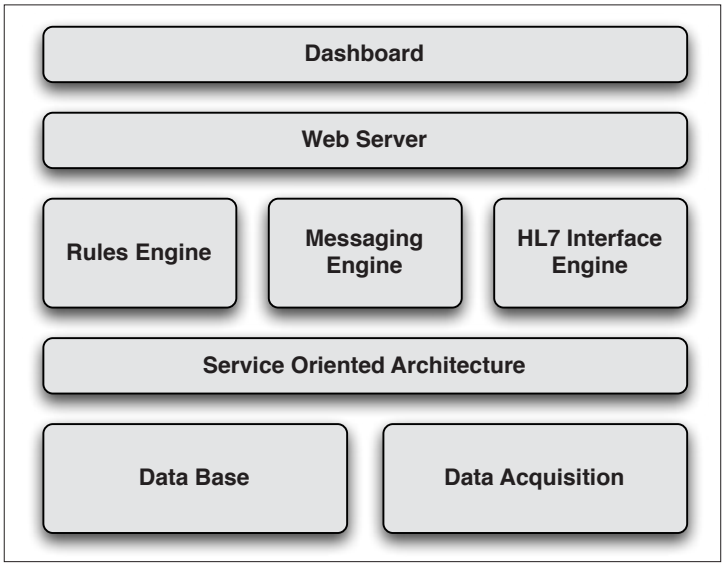

Figure 2. Prototypical Alarm Notification Server Architecture

A key advantage of these engine-oriented software components is that scripting rather than writing software code defines their specific use. Depending on the system's design, technicians or trained end-user system administrators can modify message routing and escalations or the appearance or content of a display of data. The usability and accessibility of scripting and/or configuration tables is highly variable from product to product. Scripting on some systems are not suitable for, or accessible by, customer personnel.

Current best practice for software architectures is to implement features and functions as independent modules, or plug-ins. When this approach is used, a framework for supporting plug-ins is required. A web server is used for deploying client applications on endpoint devices. A relatively new addition to this kind of modular "engine" architecture is the dashboard. A patient monitoring central station display is a dashboard for patient monitors. Many healthcare IT applications also include dashboards to summarize data. By using a dashboard, manufacturers can quickly configure displays of summary data that are updated automatically by the system.

HL7 Interface Engine

An interface engine provides HL7 integration capabilities for ADT feeds to support patient context, and may include results reporting for receiving diagnostic reports that may generate messages.

Telephony Gateway

This system provides the messaging to handsets which can be via VoIP, cellular, digital

enhanced cordless telecommunications (DECT) or paging frequencies. Most telephony gateways use a version of the SIP protocol to communicate with external systems like alarm notification servers. Telephony gateway compatibility does depend upon alarm notification vendor. Telephony gateways are designed to operate with specific handsets, so compatibility depends upon the telephony gateway vendor as well. Ascom, Cisco, Polycom, Voalte and Vocera are vendors in this product space.

Integrating System Components

Alarm notification systems are often multi-vendor solutions by necessity. The number of vendors involved, and which vendor provides what blocks in the system diagram, is highly variable. Current examples of alarm notification solutions available from two medical device manufacturers are Welch Allyn's AcuityLink Clinician Notifier and Masimo's Patient SafetyNet. These are effective systems, but only support the manufacturers' medical device products. Patient-centric systems that support products from multiple medical device and nurse call manufacturers are only available as third-party solutions.

Third-party alarm notification system vendors include Amcom CommTech Wireless, Ascom Unite, Cardiopulmonary Corporation, Cerner AlertLink, Extension, GlobeStar Connexall, and Philips Emergin.

The medical device signal input system component can be provided by the medical device manufacturer, as is the case for patient monitoring network gateways and infusion pump gateways. A third-party medical device signal input system, also known as a medical device data system or MDDS, can integrate medical devices that do not include any network capability or a gateway, and are often used to implement electronic clinical documentation for electronic medical records (EMRs). Many alarm notification systems also include medical device signal input system capabilities. If medical device data acquisition requirements are only to be used to drive the alarm notification solution, the MDDS features offered by the alarm notification vendor should provide sufficient functionality and may eliminate the need for a separate MDDS vendor. When additional medical device connectivity features are desired, such as pushing data for clinical documentation in the EMR, the MDDS features provided by an alarm notification vendor may be inadequate and should be validated as suitable for both messaging and clinical documentation applications.

Any interface is made up of two halves. For example, nurse call integration is provided by an interface or application programming interface (API) in both the nurse call system and alarm notification system. Both vendors may sell their side of the interface as a gateway, or offer the interface as an option on another generalized system component. Currently, there are no third-party gateway manufacturers that handle the signal input system side of an interface.

When additional medical device connectivity features are desired, such as pushing data for clinical documentation in the EMR, the MDDS features provided by an alarm notification vendor may be inadequate and should be validated as suitable for both messaging and clinical documentation applications.

Because no standards are used, signal input system vendors must actively participate in and support the integration of their products with any third-party system, including alarm notification systems. The availability of interfaces between alarm notification system vendors and third-party medical device and system vendors is highly variable. The availability of interfaces should be a key factor in vendor selection.

As mentioned earlier, patient data moving through the alarm notification system must be identified with the correct patient, and should be established in the system closest to the patient—ideally at the patient's bedside. When a third party provides the MDDS, patient context must be established in that system before data is passed to the alarm notification server. If the alarm notification vendor provides the MDDS, the alarm notification solution provides the patient context function.

The scenario where a third-party MDDS passes patient data associated with a physical location rather than a patient identity is not best practice. Patients sometimes change their location frequently during an inpatient episode, and systems tracking patient location can be out of sync with the patient's actual location,

and can result in misidentification of the patient. When patient location is used, the alarm notification system must associate a patient with that location. This approach introduces an unnecessary level of abstraction that can result in a misidentified patient.

Availability of Interfaces

As noted earlier, the availability of interfaces between system components is a key purchase criterion for the components that encompass an alarm notification system. Interfaces to medical device systems are especially limited. Nurse call system interfaces are also somewhat limited. Unlike medical device and nurse call manufacturers, whose "open" interfaces require approval from the company (which is often withheld), and signed non-disclosure (NDA) and license agreements, most telephony gateway interfaces are truly open. One can go to the telephony manufacturer's public website and download all required documentation in a software developer's kit; there are no NDAs or license agreements to sign. Engineering support is also available from telephony gateway vendors for a modest cost.

The availability of interfaces between system components is a key purchase criterion for the components that encompass an alarm notification system.

Selecting an alarm notification solution that does not have all the complete and operational interfaces required for a specific deployment is problematic. Should the input system vendor (typically medical device or nurse call) be unwilling to work with the alarm notification system vendor to create the necessary interfaces, it is up to the system purchaser to attempt to create sufficient incentive for the recalcitrant vendor to support an interface development effort. Creating such interfaces may result in additional charges for the purchaser from the input system vendor, alarm notification vendor, or both. Worst case, the input system vendor refuses to cooperate in the development of a needed interface, and another alarm notification vendor must be selected.

The preferred method for making disparate systems interoperable, as between signal input systems and alarm notification systems, is through industry standards. The organization Integrating the Healthcare Enterprise (IHE, www.ihe.net) was created to facilitate test and certification of standards based integration between disparate systems. The IHE has made considerable contributions to the industry in diagnostic imaging and cardiology, markets where manufacturers have widely adopted industry standards. In 2005, the IHE created a new domain, Patient Care Devices (IHE-PCD) to foster similar standards-based interoperability among common medical devices and systems found at the point of care. Because manufacturers in the PCD market have not adopted standards, the work of the IHE-PCD has been difficult and slow. The IHE-PCD has defined an alarm communication management (ACM) profile.[1]

As of this writing, only two manufacturers have published conformance statements with the ACM profile on the IHE product registry site (http://product-registry.ihe.net/PR/home.seam). Presently, it is not possible for a provider to purchase an alarm notification system based on the ACM profile. Providers are encouraged to push manufacturers to support standards, and to achieve approved integration statements from IHE. But ultimately, hospitals cannot buy a standards-based alarm notification system that is tested and certified by IHE because none yet exist.

Communication Devices

Communication devices can be general-purpose computers running client software on desks or carts, personal data assistants (PDAs), tablet computers, smart phones, or VoIP handsets. These devices can be broken down into those suitable for stationary or portable use (desktop computers and computers or tablets mounted on carts) and mobile devices carried by clinicians (PDAs, handsets and some tablets). Communications can also be divided into two groups, closed-loop two-way messaging, and open-loop one-way messaging.

Most contemporary devices provide two-way communications with message receipt and possibly responses or end user messaging back to the alarm notification system. One-way devices merely receive the alerting message and function similarly to a pager. A limitation of one-way devices is that the alarm notification server has no way to verify if the communications device or the user has received a message. Two-way devices may allow for other types of

communication: text messaging, voice messaging, and access to email and other services, assuming the functionality has been enabled.

Communication devices can use paging frequencies, shared or dedicated wireless frequencies, or even cellular frequencies. Currently the majority of communication devices operate on Wi-Fi networks. Communication device functionality can also vary due to more vertically integrated product offerings using proprietary mechanisms across the data communications path. For example, one can buy an Ascom middleware solution along with Ascom handsets and the resulting functionality of the handset with regards to types of messages received at the handset can be "richer" compared the use of the Ascom middleware solution with another vendor's communication device. Similarly, some systems (like the system from Voalte) enable rich communications using iPhones and iPod Touch devices, devices that are not currently supported by enterprise telephony systems.

Infrastructure

All of these alarm notification systems—and their related signal input and access to communications devices—rely upon the enterprise network infrastructure which provides means for sending messages throughout the integrated system. Cisco, Meru, and Aruba are vendors in this product space. Some network manufacturers also offer telephony systems, and some do not. Depending on the frequency used for signal propagation to the handsets, the vendor chosen for the messaging/middleware solution, wireless network infrastructure, and communication devices may be the same. This vertical integration can be beneficial in providing tight coupling and signal propagation; however, it also may lead to incompatibilities with other system-alerting products.

The servers and core network used to deploy an alarm notification solution should use redundant and high-availability configurations in order to minimize unscheduled down time. The end-to-end system, from point-of-care medical devices to wiring closets and server farms, should have appropriate backup power supplies, cooling and ventilation, and physically controlled access. Life-critical system components should be clearly labeled as such, with color coding for network cable runs and patch panel cabling. Many providers have policies and procedures covering these topics for patient monitoring systems and other life-critical medical device systems. These policies and procedures should be extended to alarm notification solutions, especially if the system is being used for applications such as medical device alarm notification and/or critical test results management.

A meaningful level of testing is required to ensure that changes and upgrades to infrastructure do not introduce latent defects in the operation of the overall alarm notification system that could result in failure. Most provider test labs are limited to a very small selection of network and other systems. Proper testing for an alarm notification system, or any networked medical device system, includes the use of an end-to-end test system, including a selection of medical devices and simulators to generate test data that represent the actual enterprise network environment. Wireless network infrastructure should include at least a couple of controllers and a half dozen access points. Subsequent to a successful test in the lab, network upgrades should be deployed in phases, starting with the least complex and demanding environments. Over three or four phases, the deployment of network upgrades should be extended into more demanding network environments. As many hospitals have learned, jumping from a very limited test lab to house-wide deployment is a recipe for disaster.

Alarm notification systems rely upon an institution's information technology infrastructure for communications. To ensure the continued safe and effective operation of alarm notification systems, it is the opinion of these authors that the IT governance in most hospitals must be enhanced.

Alarm notification systems are typically installed in an IT infrastructure that meets the alarm notification manufacturer's specifications. These specifications often include wired and wireless networks, computer hardware and system software, and the physical operating environments of infrastructure equipment. Providers may chose to not meet certain infrastructure specifications, but manufacturers are likely to require providers to sign an agreement stipulating that the provider understands they are assuming responsibility for modifying a regulated medical device.

Governance and Regulatory Considerations

Alarm notification systems rely upon an institution's information technology infrastructure for communications. To ensure the continued safe and effective operation of alarm notification systems, it is the opinion of these authors that the IT governance in most hospitals must be enhanced. This need impacts biomedical and clinical engineering because they are the best resource to provide an appropriate life-critical perspective to what is currently a mission-critical IT perspective. How documents are controlled, risk management, change management, configuration control, and verification testing are often the IT operational areas most in need of revision. Providers deploying alarm notification systems are advised to adopt a risk management process as described in IEC 80001[2] or ISO 14971.[3] Unfortunately, there are no industry standards providers can adopt to guide them in defining and implementing the kinds of IT governance enhancements that are required for life-critical applications. Industry best practices are just now emerging in this new level of IT governance.

Alarm notification systems are regulated medical devices that are designated Class II in risk and require FDA clearance prior to sale (via the 510(k) process). FDA has exercised limited regulatory discretion toward alarm notification system manufacturers, i.e., not pursued enforcement actions provided they refrain from displaying physiological waveforms. Some alarm notification solutions are FDA-cleared medical devices (e.g., Cardiopulmonary Corporation's Bernoulli system), and FDA has recently signaled that manufacturers without FDA clearance may face enforcement action in the near future.[4] Providers should determine an alarm notification manufacturer's regulatory status. A quick search of the FDA's 510(k) database can accomplish this, or alternatively providers can request documentation, e.g., a copy of the FDA 510(k) clearance letter, from the manufacturer. Manufacturers without clearance should not necessarily be excluded from consideration provided they are pursuing a path to bring them into regulatory compliance in a timely period. The FDA rarely pursues enforcement actions that would be unduly disruptive to providers, especially against manufacturers that are actively engaged with FDA and making progress towards compliance that is acceptable to FDA. Providers should be warned that in the event the FDA pursues enforcement actions against a manufacturer without clearance, the manufacturer could be forced to recall their alarm notification systems from customers.

Enterprise IT infrastructure is made up of products with relatively short product life cycles. New software releases and hardware obsolescence necessitate frequent verification and validation testing by the medical device and alarm notification system manufacturers before it can be safely deployed in customer sites. Providers must allow the manufacturers of medical devices, including the alarm notification system, to complete verification testing prior to installing IT upgrades. Providers that modify IT infrastructure that makes up part of a medical device system, without the medical device manufacturer's approval, are modifying a regulated medical device and may bear additional liability as a result.

As providers and industry begin to enter a period of increasing levels of systems integration and eventually interoperability with medical devices, it is important to follow practices that will ensure sufficient levels of patient safety and system effectiveness.

As providers and industry begin to enter a period of increasing levels of systems integration and eventually interoperability with medical devices, it is important to follow practices that will ensure sufficient levels of patient safety and system effectiveness. The evaluation and selection of alarm notification systems is a process of discovery, starting with a thorough needs assessment and in-depth understanding of the prospective alarm notification solutions. ■

References

1. **Integrating the Healthcare Enterprise Patient Care Domain Profile.** Alarms Communication Management. Available at http://wiki.ihe.net/index.php?title=PCD_Profile_Alarm_Communication_Management.

2. **IEC 80001-1:2010.** *Application of risk management for IT-networks incorporating medical devices - Part 1: Roles, responsibilities and activities.*

3. **ISO 14971:2007.** *Medical devices - Application of risk management to medical devices.*

4. **Gee T.** FDA Final MDDS Rule Signals FDA Shift to Enforcement. Available at http://medicalconnectivity.com/2011/02/17/fda-signals-enforcement-with-final-mdds-rule/.