

## Implementing Secure Remote Diagnostic Access (SRDA) With Audit Capability For Equipment Telemaintenance



Teleconsole™

**F**or many decades, telemaintenance has been a well established 'best practice' for Information Technology (IT) operations. However, most recent independent surveys still suggest that the concept of telemaintenance is virtually non-existent, or not an enterprise-wide capability, in equipment operations outside the realm of IT services, such as healthcare, utilities, communications, and other sectors.

Telemaintenance is accomplished by a Secure Remote Diagnostic Access (SRDA) capability that enables a remote technician to perform diagnostic tasks on equipment without having to be onsite, or the ability for the local maintainer to collaborate with remote Subject Matter Experts (SMEs) assisting in the troubleshooting and repair of the equipment.

The purpose of this whitepaper is to first examine the current medical equipment operations model to better understand the challenges of implementing SRDA for equipment telemaintenance and audit of the technicians' activities during the SRDA session for regulatory compliance; and then to present a unique solution, the Teleconsole, that was specifically developed for military applications through R&D funding from the Department of Defense. The Teleconsole currently has a DoD-wide Authority to Operate (ATO) certification, along with multi-national certifications such as FIPS 140-2, Level2 and Common Criteria EAL-3. The Teleconsole has been commercialized and some of the security accreditations have relevance or satisfy some industry-specific regulatory compliance standards.

While this paper is written in the context of medical equipment, the concept, methodology, and technology mentioned are applicable to other industries, including utilities (SCADA equipment), retail (Point of Sales devices), manufacturing, and conventional IT (branch office and remote site infrastructure support).

### **Current Biomedical Maintenance**

Biomedical facilities face a number of challenges when confronted with maintaining a diverse set of sophisticated and complex medical equipment. The current maintenance model is on-site and physical, rather than remote and virtual, requiring a technician to travel to the medical facility to perform equipment diagnostics, calibrations, and other maintenance task.

Historically, the maintenance of medical equipment requires an on-site technician to connect his/her laptop directly to the equipment with a physical cable for diagnosis and repair. Almost all types of computerized medical equipment are outfitted with a console port for diagnostics. However, most often, the original equipment manufacturer (OEM) does not provide any native SRDA capability in their equipment. Without any remote accessibility to the equipment, telemaintenance cannot be achieved. This is inefficient as on-site maintenance prolongs downtime, increases operational costs, and impacts quality of care and safety for patients. Furthermore, with the growing concerns of security threats and related industry regulatory compliance, accountability becomes a necessity to document or record all the activities of the technician. When a company is considering or developing an SRDA strategy for its equipment operations, it is therefore necessary to also include an audit function in order to comply with security regulations.

## **The SRDA Challenges**

In the IT world, console access has been standardized with the RS-232 protocol. Whether a DB25 (outdated), DB9 or RJ45 console port is on the device, the same software and methodology is used to access network devices or servers. There are standards for operating procedures, access protocols, and even software interfaces.

### **Proprietary Software and Communications Protocols (No Standardization)**

It isn't the same for medical equipment. Each piece of equipment may have a different communication interface, as well as different software required to perform the maintenance. OEMs use proprietary software for the console access, placing dependencies on the manufacturers to provide management and diagnosis capabilities, often times for different makes and models within their own product lines. This is good for their bottom-line as they provide managed services offerings across their product line.

### **Non-disclosure by OEM (No Interoperability)**

Adding to this vendor "lock-in" is the fact that they are reluctant to release proprietary hardware and software specifications, access protocols, application programming interfaces (API), or software development kits (SDK) to allow independent development, integration, and support for telemaintenance. Without the ability to integrate or consolidate these individual and diverse management points, from various OEMs, the enterprise does not have a standardized and centralized management platform on which complex data-mining can be performed and analyzed.

### **IT and Biomed Operational Gaps (Need Alignment / Convergence)**

Some of the more complex medical equipment are partially available via remote access, due to the fact that they have two management points. The first is a 'computer' part that runs a specialized OS, such as Microsoft XP Embedded, along with custom software used by the technician to operate the equipment. The second is a 'mechanical' part that is controlled by circuit boards and is accessible by the technician via the serial console and running proprietary diagnostic software. To implement full RDA for medical equipment, the IT organization assisting the efforts often does not understand the dual management points. If the IT engineers recommend some in-band access solutions, such as virtual network computing (VNC), remote desktop protocol (RDP), or virtual private network (VPN), then the solution negates the management point on the medical equipment that can only be accessed via out-of-band console. Conversely, if the suggested solution is serial console access, then the equipment cannot be accessed via in-band services as mentioned above, or other out-of-band console such as those using USB and KVM interfaces. As such, IT organizations' recommended solutions, based on products designed for IT operations, generally do not meet the requirements of biomed telemaintenance, such as form factor, in-band versus out-of-band access, serial console versus USB console, and text-based console versus graphical console (KVM products).

## Lack of Accountability

In all remote access implementations, one important aspect is having visibility to the users' activity during the access sessions. Most COTS access products on the market today provide basic logging and reporting of the users' sessions. General logged and reported information mainly contains the authenticated user name, time of initial connection, session duration, time of connection termination, and devices accessed and duration within the session. This set of information provides very basic data about the session itself, but does not provide any real visibility to what he/she is doing within the active connection to a particular medical device.

In order to gain access to the user's actual activities within an access session, most COTS solutions on the market today employ a variety of session recording methods, such as video recording of the user's desktop, recording of user's keystrokes, protocol-specific recording, and others. These types of solution are not practical for a number of reasons:

1. Video recording requires massive storage capacity to store large video files. The recorded data is not searchable, and thus it is of little use because one has to view the entire video session in order to search for something. In the non-IT equipment operations, massive storage repository is unlikely to be available, such as in an isolated medical-centric network.
2. Keystroke logging alone doesn't provide sufficient context of the user's actions. When a user's key strokes are recorded, the string "reboot" can be a word in the document or it can be a command issued in a console session to restart a device, for example. Without context, the recorded keystrokes have little use in terms of forensic discovery.
3. Protocol-specific recording usually requires software to be installed in the back-end system. In the case of biomedical equipment, which are FDA certified, installing 3<sup>rd</sup>-party software is prohibited. This method is not a popular "audit" feature because there are countless protocols, both open and closed, that are in used today. A protocol-based recording capability can't be used in situations where the manufacturers dictates the protocols they want to use in their diagnostic connectivity between the software and hardware components.

## The Teleconsole Solution

The Teleconsole solution is a unique platform that has quantified all possible SRDA methods and integrated them into a single solution – one with a comprehensive set of access capabilities that can transform virtually any legacy medical device with no built-in remote diagnostic capability into one that is fully telemaintenance-ready.

This new solution provides technicians with the ability to remotely perform diagnostic tasks and resolve problems without any time and physical constraints. With such a new SRDA capability, a local maintainer can collaborate with subject matter experts (SMEs) via the "over the shoulder" view of the medical device; or a remote technician can "reach in" via secure access to calibrate

machine components, retrieve error logs, or upgrade configuration files – all of which can be achieved through an extensive set of RDA functions that are agnostic to the brand, make, and model of the failing medical equipment.

### **Convergence with IT Practices**

IT support personnel are accustomed to having the ability to access all equipment remotely, including the console ports necessary for ‘out-of-band’ access. The latter piece has been solved in the IT world through the use of a serial console server – a device which accepts communications over the network and transfers them to the standardized RS-232 protocol and out the physical console port connected to the network device or server. By combining standard in-band access with the functionality of a serial console server, it provides alignment with the typical access methods that IT is familiar with. Convergence occurs when the same diagnostic solution can be used for telemaintenance of both IT and non-IT or specialized equipment. In this case, IT support personnel has no issue supporting the Teleconsole which is deployed to enable telemaintenance on medical equipment.

### **Comprehensive RDA Capability for Interoperability**

Equipped with 6 DB9 serial ports and 4 USB ports – as well as network interfaces, it can provide in-band and out-of-band access methods in a single platform to both management points on even the most complex medical equipment. The in-band allows remote access to devices with an integrated ‘computer’ component, while the out-of-band access is used for the ‘mechanical’ component of the medical equipment.

OEM supplied diagnostic software has been developed to communicate directly with the console port on the medical equipment. The Teleconsole allows the software to think it is doing so even though the technician’s laptop is not directly connected to any medical equipment. To accomplish this, a few steps are needed. First, a virtual communications port needs to be created on the technician’s computer so the application thinks that it is speaking directly with the device via the COM port and a physical cable. Next, a piece of software running on the same computer needs to accept the traffic from the virtual COM and transmit it over the network to the serial console server physically connected to the medical equipment. Lastly, the serial console server transfers the communication directly to the console port on the medical equipment using the raw serial protocol. The same process using a virtual port and software transmitting communication over the network to the console server is also applicable for USB access.

### **Standardized Operating Platform**

With a distinctive Application Hosting and Distribution feature, it will also host and serve out the necessary software to create and run the virtual communications port and network transmitter on the client machine – as well as the proprietary software necessary to access the medical device. This eliminates the need to roll out any proprietary software required to access the equipment, and creates interoperability by consolidating access through a single, unified platform.

## Implementing Audit Capability

Concepteers has integrated known recording methods to develop a new recording method that is suitable for biomedical equipment operations. The patent-pending “multi-dimensional” recording method includes:

- a. An efficient visual capture function that doesn’t require a massive storage capacity – the captured visual information is not based on 30 frames per second (FPS) as found in conventional video session recording. And the recording is user-triggered rather than the traditional time-based continuous recording method. These two differentiations enable the Teleconsole to effectively and visually document a user’s activities with a minimal storage requirement.
- b. A context-based keystroke logging that simultaneously captures keystrokes and mouse input actions, as well as, recording visual data. Subsequently, these data sets are associated and aggregated to form a single data set. This representation adds visual context to the recorded keystrokes.
- c. The visual data is further processed by using an optical character recognition (OCR) engine to extract additional context that can be made searchable. In today’s graphical-intensive user interfaces, a person can manipulate the equipment via software commands and controls without ever touching the keyboard. This image extraction technique enables the Teleconsole to transcribe what the user sees, on the screen, to text that can be searched or evaluated.
- d. The Teleconsole also employs a protocol-based capture of individual connections within each SRDA session. This context-rich data set can be exported and processed by external protocol-based interpreters / reporters.

Collectively, the accountability documentation function of the Teleconsole encompasses what the user sees, types, and the responses from the device that user is interacting with. The result is a comprehensive visibility of the users’ activities during the SRDA sessions, and the data has context and highly searchable.

## Conclusion

The Teleconsole solution solves the shortcomings of existing telemaintenance as outlined above. It provides a centralized and standardized SRDA method in a single platform to virtually any device regardless of the complexity, brand, make or model. This complete telemaintenance solution can significantly improve the availability and resiliency of the medical equipment, reduce costs associated with unscheduled repairs, and increase visibility of the technicians’ activities, which in turn provides the physicians with the ability to deliver quality health care to their patients. The Teleconsole uniquely delivers efficiency, security, and compliance for any equipment operations.