Addressing the Corrections Crisis with Software Technology

Patricia O'Hagan and Edward Hanna, *Core Systems*
Roy Sterritt, *University of Ulster*

Faced with rising costs and rampant overcrowding, correctional facilities are turning to software technologies for help.

More than 2.3 million people currently live in US prisons or jails—25 percent of the world's total inmate population—a comparatively much higher rate than in other Western countries. Denmark only incarcerates 66 of every 100,000 citizens, compared to 760 in the US (www.kcl.ac.uk/depsta/rel/icps/worldbrief/world_brief.html). This situation results from tough sentencing policies that focus on drug use and habitual offenders. Over three decades, these policies contributed to high incarceration rates.

While most states have stopped enforcing these policies, the legacy remains, with high recidivism rates perpetuating the cycle. This situation has resulted in rampant overcrowding, with facilities operating at levels above design capacity and inmates frequently housed on bunks in recreational areas.

STAGGERING COSTS

Keeping so many people in the correctional system, excluding parole and probation, cost a staggering $52 billion in 2008. This is an 8.7 percent increase from 2007. One in every 15 dollars of state funds goes to corrections, making it among the fastest growing public services in the US—second only to Medicaid, a program for eligible individuals and families with low incomes and resources. Jointly funded by the states and federal government, Medicaid is managed by the states. To compound this situation, most states face their worst fiscal crisis in years.

In FY2009, 43 states faced a combined budget shortfall of $100 billion. This will affect several essential services, including healthcare, education, and public safety. Most states respond by making cuts to correctional budgets. Faced with this situation, operational costs are the first to be cut. In some situations, facilities have made staff cuts of up to 10 percent. Combined with overcrowding, this poses a serious safety threat.

Departments of corrections (DoCs) are implementing a range of strategies to address the situation, including efficiency savings. Several waves of such savings occurred during earlier cycles of fiscal constraint in the 1990s. Because the corrections industry typically has a low level of technology uptake relative to other sectors, the opportunity exists to achieve further efficiency savings.

Staffing costs can account for up to 80 percent of operating costs. A significant proportion of corrections officers' time goes to answering inmate queries and undertaking mundane administrative tasks that relate to inmate needs, such as visitation, purchasing commissary items, queries about the inmate's funds, and healthcare requests.

On average, a corrections facility requires more than 20 systems to manage the wide range of inmate needs. These run on administrative networks operated by staff. Hence it is the corrections staff's responsibility to answer queries and seek information on the inmates' behalf. This is labor-intensive, inefficient, and a source of inmate frustration. Instead, we propose providing inmates with ways to directly seek information and make service requests though self-service kiosk applications interfacing with existing inmate management systems.

 Published by the IEEE Computer Society 0018-9162/09/$26.00 © 2009 IEEE

SELF-SERVICE

Self-service kiosks in corrections facilities are a relatively new but growing phenomenon. In 2006, the Corrections Technology Association conducted a survey on the use of computer-based kiosks to help corrections agencies make decisions on implementing kiosk-based systems. The results indicated considerable interest in using kiosks for a range of applications, including distribution of general information, display of inmate account balances, purchase of goods from the commissary, and depositing inmate funds.

A wide range of applications are possible. Current efforts focus on existing services, but digital technology creates possibilities for new service types that can exploit the direct distribution model, such as a law library and the digital media distribution of music, literature, films, and images managed through the kiosks and downloaded onto appropriate secure devices, such as MP3 players.

Electronic messaging

Another new service on the horizon is electronic messaging, which provides a mechanism for enabling two-way communication between inmates and their friends and family. Letters are a traditional communication method within prisons. However, processing paper mail is labor-intensive and requires that each item be opened and checked for contraband. This is not an issue with digital messaging, which offers additional benefits such as automated screening tools that highlight suspicious communications.

Further, the Federal Bureau of Prisons has cited the application of intelligence gathering as a key advantage of the pilot system they have implemented in 14 facilities. New, chargeable services provide the opportunity to generate revenue that can pay for the technology, saving taxpayer funds.

Direct to inmates

Demand also exists for direct-to-inmate technology, supported by several requests for proposals for commissary or inmate accounts services that specify kiosks for inmate use. Takeup has been low to date, with some departments of correctional services noting that vendors lack a proven product or adequate experience.

Electronic messaging provides a mechanism for enabling two-way communication between inmates and their friends and family.

Among the innovators, the Colorado DoC aspires to improve direct-to-inmate services while developing plans for a new state penitentiary. The facility will house dangerous inmates kept in their cells most of the time. The plan will provide information and services to the inmates through a kiosk platform that will facilitate TV, communications, video visitation, and inmate requests. This will save money by keeping costly prisoner escort overhead to a minimum. The technology can also support the rehabilitation process by enabling inmates to actively engage in positive activities such as taking courses or completing instructional programs. Incentives can also be used to reward positive behavior by providing more choice and responsibility to responsive inmates.

Providing services

The market is currently driven by service providers who seek mainly to sell their particular service. Additional functions are offered as value-added components, a practice that raises issues of compatibility. What happens if the customer wants several services sourced from different suppliers?

Conceivably, multiple kiosk networks would support a range of disparate services. The way forward must be for a single open platform that can accommodate the applications and services of choice. This approach offers the best return on investment and flexibility for the customer. It is a familiar story of early technology at the prospecting stage when suppliers compete to win market share.

SEEKING A COMMON PLATFORM

Providing direct electronic services to inmates presents several challenges, including user interface design, security, and availability. With a high proportion of inmates having a lower-than-average literacy level and using a mix of languages, the user interface must be easy to use. Security must be addressed at two levels: protecting information on the system and securing the system from inmates' abuse or attack.

The number of technology-based systems used directly by inmates is currently low, but usage is increasing for several reasons. Traditional paper-based systems such as service requests and ordering goods from a commissary are being replaced by end-to-end computer-based systems that can improve delivery efficiency to inmates and increase the supplying companies' profit margins.

The other main increase in system numbers will occur through introduction of new services such as electronic messaging and media delivery to inmates. These services are typically provided to inmates on a shared-access touch-screen kiosk with limited access time for each inmate. More modern and advanced

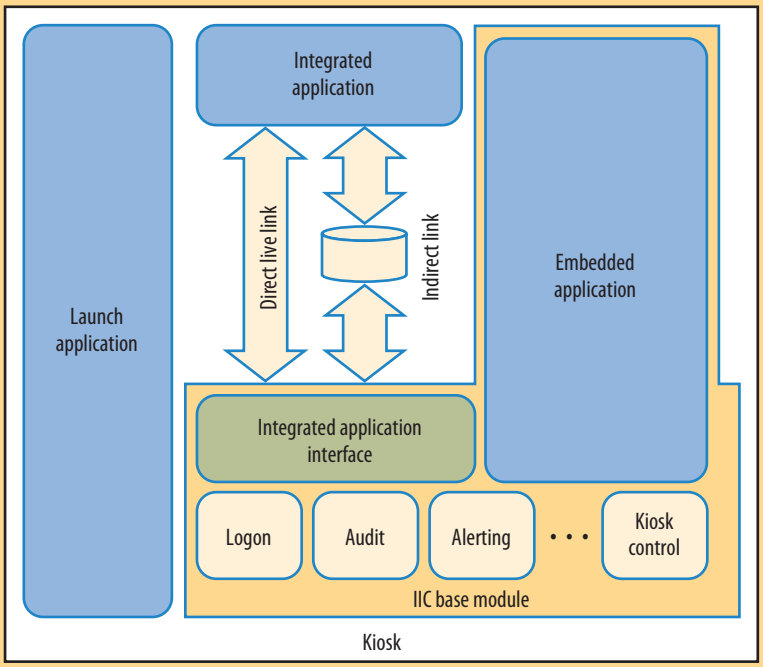

Figure 1. Inmate Information Centre architecture. The IIC platform provides a common base functionality and tailored options for specific inmate service applications.

prisons are tapping the next generation of systems that will be provided to inmates in-cell, increasing both the range of services that can be offered and the amount of access time to those services.

In the short- to medium-term, most prisons will use shared-access kiosks. As service provision companies compete in the marketplace for supply contracts, each will seek to develop, sell, and install its own kiosk system to provide such services. This multisystem approach causes several problems for the prison, however. For example, when a service contract ends, the supplier typically removes the equipment and the new supplier must reinstall a system to replace it.

Further, the prison staff must maintain inmate accounts on all the different systems. Bearing in mind the limited amount of space for installing kiosks in each prison wing, inmates must deal with several different systems, each of which may have different logon credentials. Providing a common platform owned by the prison only solves some of these problems.

SIMPLIFIED ACCOUNTING

The prison's ownership ensures that when contracts replace suppliers, the only thing that must be changed is part or all of the software that provides a given service. The prison staff has only one inmate account to maintain and, by having a long-term system in place, it will be more likely to integrate with the prison's inmate management system. The number of kiosks on each wing can then be tailored to the number of inmates, not the number of discrete services being offered. This in turn lets inmates deal with a more consistent interface.

Developing a common platform that lets inmates access applications through a common interface has driven Core Systems to develop the Inmate Information Centre (IIC) platform shown in Figure 1. This provides a common base functionality and different options for supplying service applications.

The IIC platform's base application provides services such as security, single sign-on, biometric logon, multilanguage support, alerts, audit event recording, remote session monitoring, and kiosk management and control. These service applications can be integrated with the base module through one of three distinct methods.

Launch

This is the least interactive layer and is a means for launching a separate application for which the IIC has little or no control. The IIC can monitor the task list to observe the life of the application but cannot provide it with any information or record events or statistics on use that occurred within the application. This option is provided to extend the life of legacy applications.

Integration

The IIC can communicate with integrated modules using some type of data transfer, such as XML messages over TCP, UPD, a shared database, or a regularly transferred file. This data transfer lets IIC have some two-way communication with the application.

If using a live link, IIC can provide, on application start-up, information such as inmate logon credentials, language, account balances, and so forth. IIC can also receive information about how the inmate interacted with the service, such as transactions performed, which can then be recorded in the IIC central audit trail. This type of application requires writing an application-interface module within the IIC for the specific application being integrated.

Embedded

These modules reside fully within the IIC. An audit trail records actions within the module and offers a wide range of reporting possibilities. The IIC manages sessions and privileges within the application, giving full

control to the system administrator. This application type can fully utilize all facilities the IIC base module provides.

SYSTEM AVAILABILITY

With the move to provide existing and new services through kiosks, there is a risk that the kiosk or other critical parts of the system might eventually fail, with several consequences. For example, the service provider could lose the interface to the inmates. Should this occur, the service availability level will be reduced, which in turn might invoke contract penalties and reduce the opportunity to generate revenue. Alternatively, some or all of the inmates might be deprived of these services until the fault is repaired. This might sound like a trivial inconvenience, but the volatility of prison environments can cause frustrations that swiftly spark violent reactions.

The key step for maintaining system availability involves ensuring that the entire system has few if any points of failure. For hardware this means installing redundancy in as many parts of the system as practically possible—most critically the database and webservers. Within the software application, an autonomic approach to system monitoring and self-healing is appropriate (R. Sterritt et al., "Survivable Security Systems Through Autonomicity," *Proc. 2nd NASA/IEEE Workshop Radical Agent Concepts*, LNAI 3825, Springer, Dec. 2006, pp. 379-389).

Reliability software

To address this issue, each of the software modules within the base Core IIC platform and embedded application modules contains a reliability software element that interacts with a watchdog service. The watchdog monitors all software elements and looks for failures. When it detects one, the watchdog can be configured to take varying actions depending on the failure's nature.

For example, the watchdog will first attempt to restart the software service. If this fails after a fixed number of attempts, the watchdog will restart the hardware on which the service runs. If this step fails, the system manager will be alerted that a component could not restart.

Multifunctionality

The reliability software element within each module has two functions. The first replies to the watchdog poll messages with the module's current state so that the watchdog can maintain a system overview. The second interprets the data sent within the watchdog poll message. This data contains the state information about all other software modules within the defined groups of modules needed to provide each specific service. For example, providing the commissary service on a kiosk requires the following running modules: commissary database, commissary Web services, and commissary webserver. If any of these services are idle, the kiosk can disable the commissary service entry point for the user with a message saying the service is currently unavailable.

The system then prevents users from accessing the service and getting error messages, but leaves the kiosk functionality unaffected. Meanwhile, the watchdog service seeks to restore the commissary service and, as soon as the service becomes available again, the kiosk module automatically reenables the commissary service.

These service dependency groups can be defined for each available kiosk facility. The base IIC module itself can have dependencies for its own operation—for example, the biometric logon will have a dependency group containing the biometric server as well as other services. If any of these are not available, the kiosk can revert to an alternate logon method such as inmate number and PIN.

This form of software monitoring, used in conjunction with other load balancing and redundancy techniques, can provide a highly available system.

To help succeed in these aspirations for a common platform, prisons and suppliers must agree on a set of protocols for data exchange and communication methods. This framework and the base kiosk functionality will enable developers to produce better applications, which can be used in more prisons without having to rewrite all the base functionality.

To this end, an IEEE TC-ECBS and TC-AAS industrial working group is being established and launched at the 17th IEEE Engineering Computer-Based Systems (ECBS 2010) and 7th IEEE Engineering of Autonomic and Autonomous Systems (EASe 2010) conferences, Oxford University, from March 22 through 26.

Patricia O'Hagan *is managing director at Core Systems. Contact her at patricia@coresystems.biz.*

Edward Hanna *is a technical director at Core Systems. Contact him at edward@coresystems.biz.*

Roy Sterritt *is a faculty member in the School of Computing and Mathematics and a researcher in the Computer Science Research Institute at the University of Ulster. Contact him at r.sterritt@ulster.ac.uk.*

Editor: Mike Hinchey, Lero—The Irish Software Engineering Research Centre; mike.hinchey@lero.ie

Selected CS articles and columns are available for free at http://ComputingNow.computer.org.