

Welcome to a world where technology flows
through the heart of your business environment

Welcome to CDC



Security MANAGER

Powered by **Integra**

Contents

Overview	4
Security Management	5
Security Manager	6
Key Features and Benefits	7
Benefits	8
Powered by Integra	9
Integra applications	10

Overview

Security management is a broad field of management related to asset management, physical security and human resource safety functions. Historically the various aspects of security were addressed separately - notably by distinct and often non-communicating departments for IT security, physical security, and fire, life & safety systems. Today there is a greater recognition of the interconnected nature of security requirements, an approach sometimes known as holistic security, "all hazards" management, and other terms.

The challenge is the effective integration into a single management interface for:

- Administrative
- Environmental design.
- Access control.
- Incident detection.
- Surveillance video monitoring and
- Response
- Analytics
- Rules Based Logic
- Group Collaboration.
- Communications.
- Stakeholder & Media

CDC's **Security Manager** meets the challenge of integrating environmental design, access control, intruder detection, surveillance, life safety, and communications into a single management user application allowing for efficient and effective functional management of all sub-system devices, data and images from the Security Control Room or anywhere. CDC **Security Manager** is able to provide integration of all existing and future systems and provides a fully integrated operational environment in accordance with defined cause and effect response plans.

CDC **Security Manager** provides a demonstrable consistent approach to security management, allowing for centralised operational control and easier implementation of security policies. It provides consistent real-time monitoring, a wide range of communication options, scenario planning, controlled responses and an auditable record of events and responses.

CDC **Security Manager** is powered by CDC Integra™ software - a uniquely flexible interface and control system, designed to allow for integrated communication and operational control between the different sub-systems that support the operation of any type of facility.

CDC **Security Manager** is provided by CDC, an employee-owned company specialising in the application of intelligent building solutions since 1988, with offices in London, Dubai, Istanbul and Beijing.



Security Management

Security management is a broad field of management related to asset management, physical security and human resource safety functions. It entails the identification of an organisation's information assets and the development, documentation and implementation of policies, standards, procedures and guidelines. It is supported by management tools such as information classification, risk assessment and risk analysis that can be used to identify threats, classify assets and to rate system vulnerabilities so that effective monitoring and control can be implemented.

Security policy defines what it means to be secure for a system, organisation or other entity. For an organisation, it addresses the constraints on behaviour of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and walls.

Historically the various aspects of security were addressed separately - notably by distinct and often non-communicating departments for IT security, physical security, and fire, life & safety systems. Today there is a greater recognition of the interconnected nature of security requirements, an approach sometimes known as holistic security, "all hazards" management, and other terms.

Major factors in the recent convergence of security disciplines include the development of video surveillance technologies and the digitisation & networking of physical control systems.

There are at least five layers of physical security:

- Environmental design.
- Mechanical and electronic access control.
- Incident detection.
- Video monitoring.
- Communications.

Commercial office and retail properties in particular exhibit the greatest challenges in implementing and maintaining technical systems because they reflect a great deal of diversity with owners, brokers, managers, and tenants typically being from different organisations with disparate interest and priorities

There are a wide range of sub-systems that impact on security management and thus costs and some of the more common systems in which operational efficiency can be improved, are listed below:-

- Access Control
- Asset Tracking
- Automated Number Plate Recognition

- Cameras Analogue & Digital
- Car Park Entry / Exit Barriers
- CDC Integra Operating System
- CO Monitoring & Extract
- Conference Room Systems
- Contamination Monitoring
- Control Room Displays
- Control Room Systems
- Digital Image Recording
- Digital Signage
- Emergency Lighting
- Explosive Particle Detection
- Facial Recognition
- Fingerprints & Biometrics
- Fire Alarm & Detection
- Fire Suppression
- Intercom
- Intruder Detection
- IT Assets & Network
- Leak Detection
- Lifts & Escalators
- Lighting Control
- Paging
- Panic Alarms
- People Counting
- Perimeter Intruder Detection
- Power over Ethernet
- Presence Detection
- Public Address
- Queue Management
- Remote Management
- RFID Tagging
- Seismic Detection
- Smart Card
- Standby Generators
- Surveillance Cameras
- Tamper Detection
- Telephony
- Under Vehicle Scanning
- UPS Uninterrupted Power Supply
- VESDA
- Voice Evacuation

CDC Security Manager

CDC's **Security Manager** is licensed as **VIEW, ANALYTICS** and **CONTROL** and integrates monitoring and control of each technology "silo" of operations, proving easier to design, update, and operate a portfolio wide security and environmental control plan.

The CDC **Security Manager** is a network-based information management system that is specifically designed to manage security with proven crisis/incident communication practices. It is powered by the CDC IntegraT software solution, a uniquely flexible interface and control system, designed to allow for integrated communication and operational control between the different sub-systems that support the operation of any type of facility.

The CDC **Security Manager** comprises the following core management modules listed on page 4 :-

Administrative Management Module

This module can be used to create the security and environmental control plans. It utilises CDC Integra's™ real time automated response plan concepts to capture security and other management scenarios as templates to individually identify the performance thresholds and required automated / manual actions required to maintain operation within the desired threshold.

Environmental Design Management Module

The graphical interface can present all monitored "points" such as controlled doors, sensors, surveillance cameras and ID scanners in a geographic display that allows for areas to be zoned and monitored from a single command station.

Mechanical and Electronic Access Control Management Module

Interfaces provide integrated connection to all access control systems which allows for centralised monitoring, management and occupancy control. Geographical zones can be created to control access within time of day and authorisation limits. Assets can be centrally monitored and tracked.

Incident Detection Management Module

Information from detectors and alarms can be captured, categorised and displayed graphically within the incident zone allowing for visual confirmation via video or by inspection. Automated responses can be generated automatically or manually.

Surveillance Video Monitoring Management Module

Interfacing with all types of CCTV and digital video monitoring systems, thus allowing for pan-and-zoom operations (if required) and digital video recording.

Response Management Module

This module has two distinct operational phases:

1. Pre-defined security management control response plans for the particular scenario's, are presented to the operational team as key actions and options. The status is updated in real time as each element is completed by each individual member of the operational team.
2. If an "out-of tolerance" incident occurs and is not resolved by an automated response in a pre-determined time interval the response module demands manual resolution; records the actions; allocate team responsibilities for each; and records progress in completing these actions.

Analytics Management Module

All performance information which is captured, from either polling or from receipt of alarm/incidents, is able to be passed in real time to the Analytics Service, which carries out computational / analytical tasks on the data. The outputs from the Analytics can take the following form

1. Used as an action trigger for the Response and the Rules Based Logic Modules
2. Form the basis of Reports, Graphical display, Dashboards and more..
3. Passed to Third Party ERP and other software applications

Rules Based Logic Management Module

This module provides the means in which captured data, either before and /or after being processed by the Analytics Service; can be used to trigger automated multi dimensional cause and effect control scenarios for any and all connected points on systems / sub systems.

Group Collaboration Management Module

This module provides a secure "groupware" area for the operational team members and managers to view up-to-date information with regards to "out-of-tolerance" incidents.

Communications Management Module

The ability to manage and record communications across a wide range of transmission media .

The CDC **Security Manager** is optimised to establish intelligent inter-operability between connected systems and manage any Standard Operating Instructions (SOI) that are already in place. Operators can be guided by drop down menus to respond to all types of incidents in the most appropriate manner. All alarms, system and operator actions are held in an audit log and regular operational statistics are available in report format for Management enquiry.

All communications (including voice recording) are recorded and grouped together into a comprehensive audit log which can be used post-incident for debriefing, process improvement and/or audit exercises.

Key Features

The key features of the CDC **Security Manager** are:

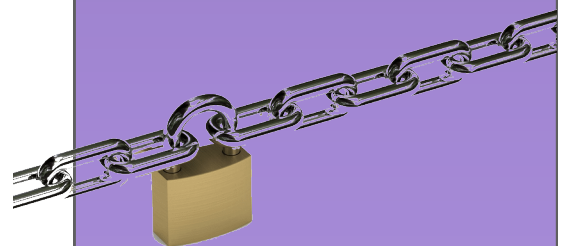
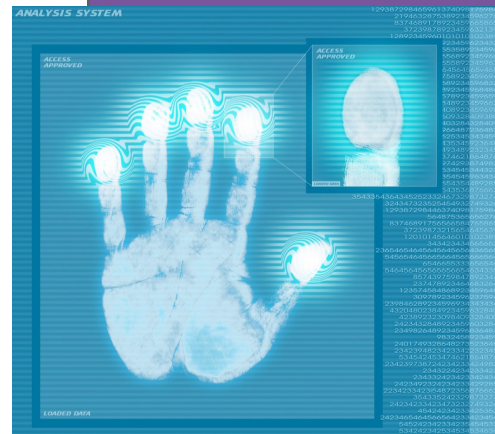
- A wide range of features and functionalities , all contributing to operating cost reduction and improved systems operational performance.
- Automated monitoring of all the security & environmental monitoring and control systems, conditional sensors and external contributory factors:
 - Consistent "out-of-tolerance" alarm trapping, and handling functionality across a wide range of connected systems and monitored domains.
 - Automated alerts and alarm handling set against pre-defined thresholds
- Automated control responses to alerts and alarms
- Powerful analytics tools which can be applied to the real time data so as to have actual operating data and performance for comparison with plans and targets
- Intelligent automated responses to event driven alerts and alarms, providing the ensuing cause and effect control strategies, which can be applied to any and many points on an connected system
- Graphical and geographical representation of a managed controllable zones of operation, the entire site, or sites.
- Operational teams can operate from dispersed different locations yet still remain in constant communication.
- Connectivity to a wide range of different systems, involving different vendors, and both legacy and new systems. Integration of existing sub-system with the capability to seamlessly and inexpensively add new sub-systems when required.
- Incorporates integrated digital images, voice and data including video surveillance and digital video recording solutions.
- Scenarios can be simulated and the resultant audit trails examined for continuous improvement and training purposes.
- The audit trail allows for powerful unbiased "forensic" analysis after real incidents have taken place to contribute to future security policy design and to support corporate governance and best practice methods.
- Accessibility from LAN, WAN and Intranet or Internet networks.
- Consistent "out-of-tolerance" alarm functionality across a wide range of monitored domains.
- Eliminates the multiplicity of paper based plans to ensure that all plans are current and readily available online.
- Scenarios can be simulated and the resultant audit trails examined for continuous improvement and training purposes.
- The audit trail allows for powerful unbiased "forensic" analysis after real "out-of-tolerance" incidents have taken place to contribute to future planning design and to support corporate governance and best practice methods.
- Normalisation of interval data from multiple sources to provide a comprehensive database that can be interrogated to provide:
 - Dashboard provision of key security and sustainability operational performance indicators.
 - Profile generation – analysis and comparison of performance over selected time intervals.
 - Year on year statistics and trend analysis for improved budgeting, planning, forecasting and capital allocation.
- Refer to the CDC **Security Manager** Fact Sheet

Benefits

The CDC **Security Manager** represents a consistent approach to security management, allowing for centralised operational control and easier implementation of security policies which provides the following demonstrable benefits:-

- Flexible, system condition **VIEW** display capabilities. Allowing information to be seen by those that need to have it, where they need to have it.
- Operates over local and wide area networks as well as over the internet.
- Feature rich and powerful data **ANALYTICS** capability applied to all data that is able to be captured automatically or manually.
- Powerful and fully configurable automated cause and effect **CONTROL** strategies
- Ability to send data to and receive from other third party applications such as financial management systems, ERP, and more
- Pro-active management improvements - a transition from "Assess and Report" to "Monitor, Control & Predict".
- A portfolio-wide operational solution that contributes to occupational efficiencies, organisational awareness, and tenant attraction / retention programmes.
- Accurate and granular information for the provision of key performance indicators, benchmarking and year-on-year comparisons for budgeting, forecasting and reporting.
- Centralised command & control operations reduces operational space requirements and the need for remote / satellite control stations.
- Integration of security sub-systems into one simpler graphical interface reduces resource and training requirements.
- Sub-systems can be replaced or upgraded in an incremental manner, without loss of functionality within the controlled environment.
- As a software solution, there is no requirement for specialist or proprietary equipment, hence significant capital outlay can be avoided.
- Integration occurs at the CDC Integra™ server / workstation level, therefore individual sub-system maintenance and operating agreements are unaffected.
- The solution contributes to "good practice" management such as BS and ISO standards for security management.

The CDC Security Manager provides consistent real-time monitoring, a wide range of communication options, scenario planning, controlled responses and an auditable record of events.



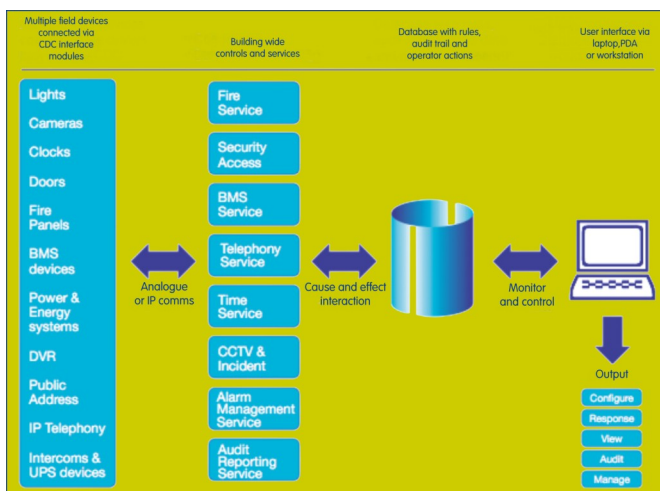
Powered by Integra™

The CDC IntegraT software solution is a uniquely flexible interface and control system, designed to allow for integrated communication and operational control between the different sub-systems that support the operation of any type of facility.

All types of facility sub-systems are presented in an easily comprehensible graphical format to integrate all operational management services into a single control environment. The solution operates across, and groups together, management solutions for:

- Heating, Ventilation and Air Conditioning (HVAC).
- Environmental Monitoring and climate control.
- Energy management and carbon reduction.
- Physical and site access security.
- CCTV and Digital CCTV recording.
- Fire, Life and Safety systems.
- Lighting and shade.

Versatility is the key to the CDC IntegraT concept. Instead of attempting to force adoption to a particular standard, its success as an approach to system integration lies in being sufficiently flexible to adopt whatever communications media and protocols are already employed by the



proprietary sub-systems.

CDC's approach is to integrate the site sub-systems so that the functional autonomy of the individual systems is unaffected. This approach also preserves confidence and integrity in the independent operation of all the sub-systems.

CDC Integra™ hosts a suite of applications called CDC Server Services that each have a clearly defined role in terms of the discipline or function to which they relate

(such as Fire, Security, BMS etc). Each Server Service applies discipline-specific rules to maintain the integrity of the systems they control.

CDC Integra™ Server Services have the following characteristics:

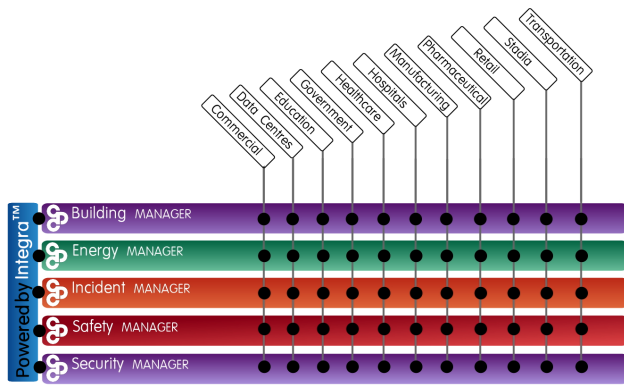
- A **Grouping Service** used to combine management tasks from the different Server Services on a location basis. This allows, for example, Fire Objects (detectors and text messages) to be grouped into a Room, and Rooms to be grouped into an Area, and Areas to be grouped into a Section, and Sections into a Floor, and so on. Graphical representation of the state of any Group is displayed, which in turn represents the state of its constituent components.
- The **Logging and Report Generating Service** provides audit trail information, and also acts as a central report storage facility.
- The **Alarm Management Service** receives alarms and allocates them into a prioritised Alarm List. It also builds a Response Plan for each received alarm to provide clear operator instructions.
- The **Response Plan** method of integration is designed to analyse a large number of different alarm conditions. Each plan creates "easy to interpret and follow" instructions in response to particular alarm stimuli. The response plan can automate some response actions, and assist operators or operational managers in completing others.
- The **Analytics Service** receives All performance information which is captured, from either polling or from receipt of alarm/incidents, is able to be passed in real time to the Analytics Service, which carries out computational / analytical tasks on the date. The outputs from the Analytics can take the following form
 - Used as an action trigger for the Response and the Rules Based Logic Modules
 - Form the basis of Reports, Graphical display, Dashboards and more..
 - Passed to Third Party ERP and other software applications

Response Plans are designed to provide operations and management teams with a tried and tested operational procedure when an alarm situation occurs, and to record their actions and feedback to an audit trail.

Integra™ Applications

The CDC Integra™ Manager applications build upon the Integra™ software platform to provide an interconnected suite of feature rich applications designed to monitor, control and group together disparate building sub-systems. The main CDC Integra™ applications are:

- Building Manager
- Energy Manager
- Incident Manager
- Safety Manager
- **Security Manager**



Additional CDC Integra™ Manager applications are also available for specific operational solutions such as Vehicle inspection & parking management and Production control & automation.

About CDC

CDC is one of the pioneers of the intelligent buildings concept and has been a market leader since its inception in 1988. An international network of offices in London, Dubai, Istanbul and Beijing supports our activities as a leading authority in existing and new build projects.



CDC solutions are used in over a 1,000 global locations and we are solution partners with many of the world-renowned organisations in the provision of intelligent building solutions.

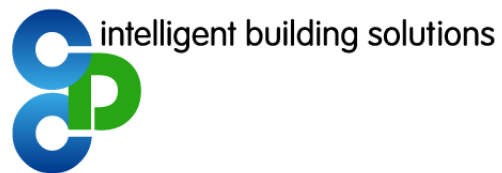
A founder member of the Intelligent Buildings Group, CDC also continues to invest in R&D at leading universities to help drive the market and develop new technologies.

CDC provides many intelligent building management solutions covering sectors such as Healthcare & Hospitals, Retail Malls, Commercial, Industrial, Pharmaceuticals, Transportation, National & Local Government and Education.

IBG is an international not for profit organisation dedicated to the improvement of the built environment, through research into building intelligently an intelligent building. IBG is supported by government and affiliated with sister organisations in China Asia, Europe, US and more







CDC intelligent building solutions

Riverside Building,
County Hall,
Westminster Bridge Road,
London, SE1 7PB.
United Kingdom

Telephone +44 (0)20 7928 9150

Fax +44 (0)845 330 7267

Email: sales@cdc.uk.com

Web: www.cdc.uk.com

CDC is a Cisco and Microsoft Development Partner