INTEGRATED PHYSICAL PROTECTION SYSTEM

Ranajit Kumar
Control Instrumentation Division,
Bhabha Atomic Research Center,
Trombay, Mumbai – 400085,
India

Abstract

An Integrated Physical Protection System (IPPS) was developed for the consolidation of all sub systems, sensors and elements related to physical protection for an efficient and effective security environment of a facility. An effective physical protection system discharges the functions of detection, delay, communication, response, access control etc. IPPS performs, controls and monitors all the above functionality and helps in taking quick action on occurrence of unusual incidents by instantly reporting the incident in easily understandable audio, video, graphical and textual format and also by initiating automatic interactions among sub-systems.

Major security sub-systems integrated in the IPPS are, access control, intrusion detection, CCTV surveillance, emergency door monitoring system etc. The access control sub-system utilizes intelligent card readers and interfaces with the PC based central controller through RS-485 communication network. Similarly, intrusion detection system utilizes intelligent distributed I/O controllers for alarm acquisition from field sensors / detectors etc. and communicate to the IPPS through RS485 bus network. CCTV system is controlled by using a dedicated controller which performs the functionality of matrix switcher and camera control. The distributed CCTV controller interfaces with the IPPS by RS232 serial interface. All the sub-systems are modular in nature and can work stand alone without the IPPS. IPPS also monitors individual sub-systems and indicate their health status on-line. Fig.1 gives the overall schematic of the IPPS.

One of the major functions of IPPS is to facilitate automatic interaction among sub-systems so that occurrence of an event in one component can initiate a series of actions in one or many sub-systems. For example, an intruder alarm can cause homing of video camera of the specified zone and start recording the scene in the VCR. It is possible to define any input event as logical ‘AND’ or ‘OR’ of two or more independent input events.

Data originating from all sub-systems are integrated and presented to user in easily comprehensible format (tabular, graphical, audio, textual) on demand. However, appropriate level of protection is applied to prevent unauthorized access and use of data.

The IPPS was developed on IBM-PC platform under QNX real time operating system (RTOS) and uses QNX-Windows GUI.

1. INTRODUCTION

Integrated physical protection system (IPPS) is the consolidation of all sub systems, sensors and elements related to security of an organization in one platform or control center for carrying out functions necessary for an efficient and effective security environment. The main objective of an

IPPS is to ensure the protection of assets of an organization against all types of risks like theft, pilferage, sabotage etc and aid the organization for smooth functioning and seamless integration with other facility operational systems. An effective security system discharges the functions of detection, delay, communication and access control. IPPS perform, control and monitor all the above functionality and helps in taking quick action on occurrence of unusual incidents by initiating automatic interactions among sub-systems. It also aids security personnel by presenting data originating from various sensors and sub-systems in easily understandable audio, video, graphical and textual format.

Individual security sub-systems viz. access control, intrusion detection, CCTV surveillance, emergency door monitoring were developed using personal computers and intelligent front end controllers. An IPPS - Manager was developed which controls and monitors all the above security sub-systems and facilitates interaction among these sub-systems. Both the individual sub-systems and the IPPS Manager runs on IBM-PC under QNX real time operating system (RTOS) [1] and uses QNX-Windows GUI [2]. Watcom 'C' [3] has been used for program development and Watcom SQL [4] for database purpose.

2. SYSTEM REQUIREMENT

2.1. Functions

IPPS is consolidation of major security related functions in one control center. These functions are intrusion detection, access control, surveillance and alarm monitoring. The IPPS should provide all the above functions in modular form and allow for expansion and modifications. The system should provide full integration in one control center and should be amenable to on-line and dynamic reconfiguration.

2.2. Interaction among sub-systems

One of the most important aspects of IPPS is the automatic interaction between different sub-systems. System should provide facility for configuring interaction between various component sub-systems. It should be possible to define a sequence of output activities in response to an input event. Similarly, it should be possible to define any input event as logical 'AND' or 'OR' of two independent input events.

2.3. Data presentation

Data originating from all sub-systems should be integrated and presented to user in easily comprehensible format (tabular, graphical, audio, textual). These data may be transaction data from access control system or alarm data from perimeter protection system or video clips from CCTV surveillance system. IPPS should ensure that adequate protection mechanism have been incorporated to prevent unauthorized access and use of various data.

2.4. Monitoring

IPPS should monitor and indicate the status of all sub-systems on-line. Whenever any sub-system is reconfigured for modified system capabilities, the configuration should be validated with respect to individual sub-systems.

3. OVERALL SCHEMATIC AND FUNCTIONALITY

IPPS consists of different physical protection sub-systems viz. access control system (ACS), intrusion detection system (IDS), CCTV surveillance system and emergency door monitoring system (EDMS) under the control of IPPS-Manager. The overall schematic of the IPPS is shown in fig.1.

Individual sub-systems like ACS or PIDS can work standalone without the presence of IPPS-Manager. The IPPS-Manager provides control for launching or termination of individual sub-systems. IPPS-Manager also provides interaction among all sub-systems by defining input – output interaction relationship. User can select input from the available sub-systems and define the output(s) to be activated in different sub-systems, as input–output interaction relationship. For example, it can be configured to select a particular camera (in CCTV system) for homing on a video monitor and start recording the video (output event) in case of occurrence of an alarm in IDS (input event). It provides the facility to configure such input-output interaction matrix. Fig.2 shows a schematic of functional interactions among different sub-systems of the IPPS.

4. INDIVIDUAL SUB SYSTEMS

The major sub-systems of the IPPS are ACS, IDS, CCTV and EDMS. All these sub-systems work stand-alone without using the IPPS-manager. Salient features of individual sub-systems are given in the following section –

4.1. Access Control System (ACS)

ACS controls the movement of authorized personnel and detects and denies the unauthorized movement of personnel. ACS consists of maximum 64 intelligent card readers controlling turnstiles or electrically operated locks and connected to the IPPS-computer by RS485 network. In addition to card number, the system facilitates verification of global and local multi level anti pass back (APB), multiple time frame and access level, recording of all transaction with real time and date, database facility and on-line configuration capability. Main features of the ACS are -

(a) Maximum 64 card readers can be connected on two 4-wire RS 485 bus.
(b) Standard access control functionality supported along with online display of all transactions, system and reader status.
(c) Provides emergency aids like head count, tracing of a person etc.
(d) Provides database of all events with real time of occurrence.
(e) Support on-line configuration of system and interaction with other systems through IPPS-Manager.

4.2 Emergency Door Monitoring System (EDMS)

EDMS readers are used in access control system for monitoring of emergency exits from vital areas or other exits. Doors requiring monitoring are equipped with door sensors and are interfaced to the EDMS readers. EDMS reader indicates the status of all doors locally and also communicates the status to the IPPS computer. Salient features of the EDMS are –

(a) Maximum 32 readers can be connected in one loop.
(b) EDMS readers share RS-485 network along with access control readers.
(c) Maximum 16 door sensors can be connected to one EDMS reader.
(d) Real time textual and graphical annunciation of door alarms at IPPS-computer.
(e) Database of all events with real time of occurrence.

4.3 Intrusion detection System (IDS)

IDS consists of up to 32 detector control units (DCU) interfacing different intrusion detectors. DCUs are connected to the IPPS by a 2 wire RS-485 network. Maximum 8 detectors can be interfaced to each DCU. Features of the IDS are as follow –

(a) 32 DCUs can be connected in one loop. Can be extended to maximum 256 DCUs.
(b) Real time audio-visual and textual annunciation of alarms on graphical map plan of facility with actual location of the alarm.
(c) Event database with real time of occurrence of events.
(d) On-line remote monitoring and testing of the detectors and DCU.
(e) Interfaces various types of intrusion detectors.

4.4 CCTV Control System

CCTV surveillance sub-system of the IPPS utilizes the Distributed CCTV controller which connects up to 64 cameras to 8 buses of twin co-axial cable and provide video output on 8 CCTV monitors. Cameras are connected to intelligent slave controllers which also carries out camera control functions. Main features of the DCCTV System are –

(a) Transmission of video signal and digital control data on a single twin coaxial cable.
(b) Provides remote camera controls like pan, tilt, focus and environmental controls like heater, fan, wiper etc.
(c) Standard video sequencing functions like auto-home-bypass with user programmable sequence time.
(d) Large number of remote and local alarms monitoring and remote camera homing.
(e) Event driven recording for future investigations

.

5. RESULTS & CONCLUSIONS

An integrated system having following sub-systems configuration was deployed in one installation –

(a) Access Control – 40 card readers controlling 4 dual bi-directional turnstiles and 24 doors by using electromagnetic locks.

(b) EDMS – 40 door sensors connected to 4 EDMS readers.

(c) IDS – 20 pairs of microwave intrusion detectors connected to 12 DCUs.

(d) CCTV Surveillance – 40 cameras, 16 with PTZ and environment control, 5 with PTZ capability, 5 with PT capability and 14 fixed cameras.

This system is working satisfactorily for more than one and half year. Security personnel could change sub-system interaction configuration to suit security environment. The system is being expanded to integrate with facility operating LAN and various safety and emergency control functions.

REFERENCE

[1] QNX SOFTWARE SYSTEM LIMITED, Kanata, Ontario, Canada, QNX System Architecture.

[2] QNX SOFTWARE SYSTEM LIMITED, Kanata, Ontario, Canada, QNX Windows Programmers Reference, Users' Guide.

[3] WATCOM INTERNATIONAL CORPORATION, Waterloo, Ontario, Canada, Watcom 'C' Library Reference, Compiler and Tools Manual.

[4] WATCOM INTERNATIONAL CORPORATION, Waterloo, Ontario, Canada, Watcom SQL Users' Guide.

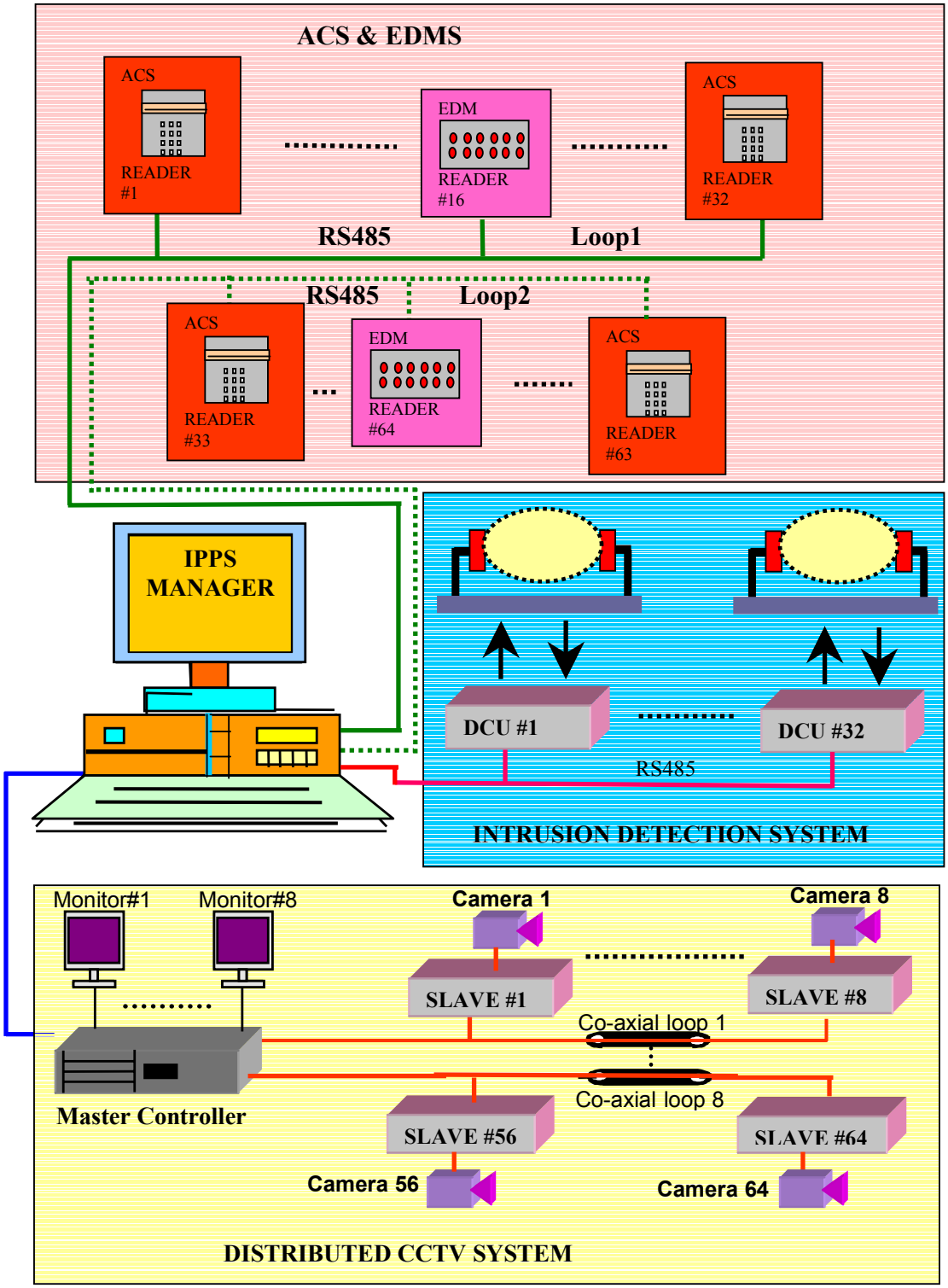

FIG 1. Schematic of Integrated physical protection system.

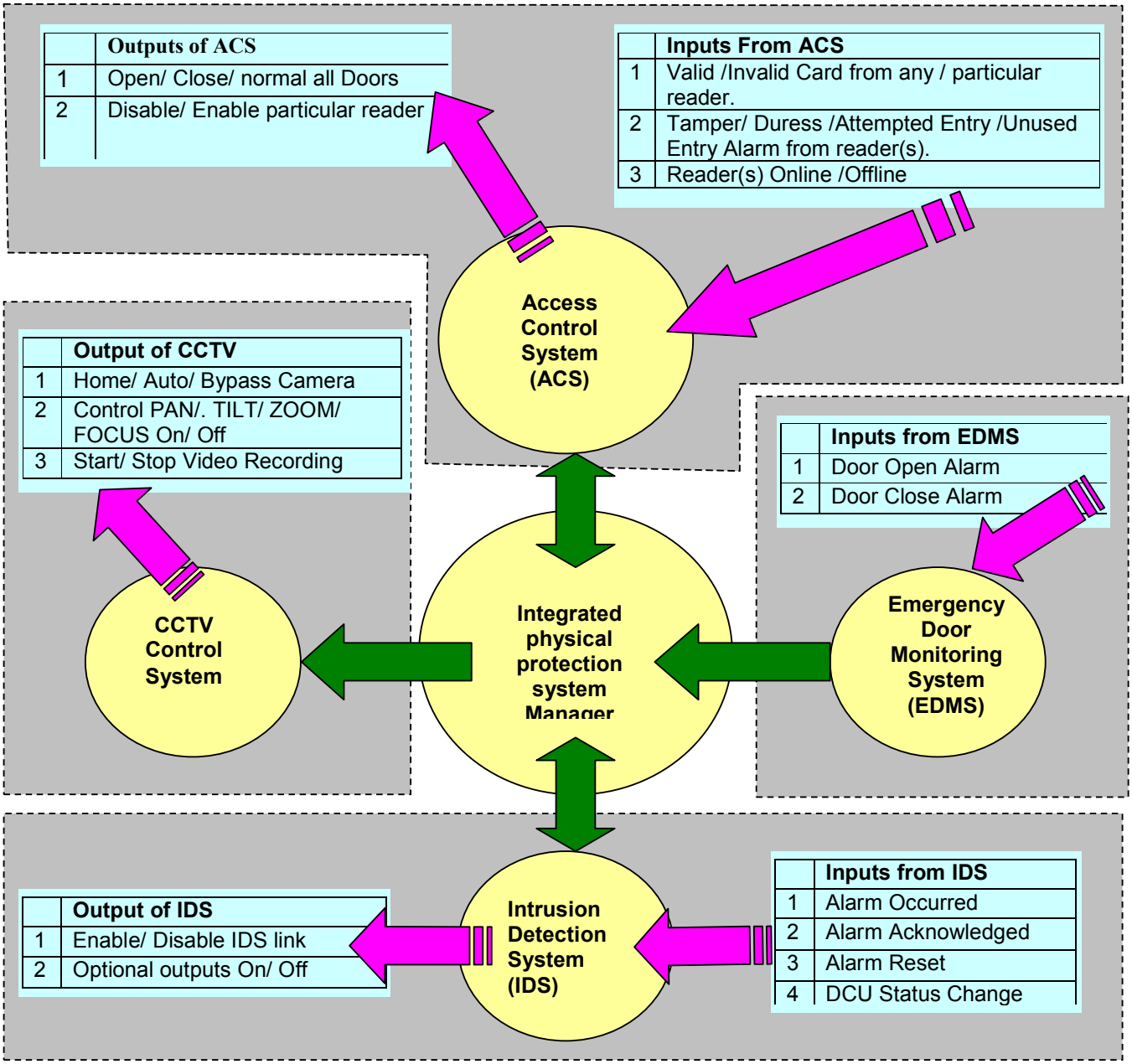

FIG 2. IPPS Functional Interaction Block Diagram