TOTAL CONTROL
ACCESS CONTROL SOLUTIONS INTEGRATED BY PANASONIC
Access control and alarm systems are essential for the implementation of security in commerce and industry as well as in public spaces. Getting the best possible security at the best price is just as important as getting a fully functioning system with the best possible functionality.

Bravida is an integrated security system for access control, card production, burglar alarms, fire alarms, and CCTV surveillance that provides excellent security at a reasonable price.

Bravida is simple to manage, and it is fully possible to expand the system with additional customised functions.

Bravida is simple to integrate and external systems are easily managed through additional modules, such as OPC, Data Service and Alarm Service through our open interface Bravida EasyConnect.

Bravida has been developed to satisfy the market’s stringent demands for functionality and ease of use.

This system description is intended to provide an overview of the system’s components, as well as to demonstrate the options and solutions that Bravida has to offer. For more detailed information, please refer to the user manual, consultant manual and the individual product sheets.
SYSTEM COMPONENTS
SOFTWARE

Bravida (Integrated by Panasonic) – A scalable system

The software for Bravida is scalable, can be modified and is capable of handling both large and small systems. The largest installations comprise thousands of door environments and alarm points, while the smallest systems may have only a few. The system sizes below can be supplemented with a number of additional modules, such as CCTV, Data Service, Guard Report, Alarm Distribution, Alarm Monitoring, etc. More information about these modules can be found in separate product sheets.

BRAVIDA (INTEGRATED BY PANASONIC) COMPRISSES THE FOLLOWING PROGRAMS:

Bravida Server
Bravida Server is the main program that handles communication between substations in the system. It works in the background on a separate or the same PC where the SQL Server is installed and running. Bravida Server is receiving, evaluating and handling all events and alarms from devices. It’s also responsible for keeping the whole configuration database and distributing changes to all devices.

Bravida Client
Bravida Client can be run on the same computer as the Bravida Server software. The license for Client can be used by several computers, but only one user can use the program per license. Both the Premium and Base versions can be expanded with several licenses.

Bravida Card Production
Bravida Card Production Client is an additional module that enables card production. Card production is fully integrated and the program includes capabilities for taking photos, printing and designing access cards.

Bravida EasyConnect IEC
Bravida EasyConnect is a program that serves as a link between external systems, such as HR systems, and Bravida Server. IEC communicates with 3rd party systems using the SOAP protocol and WEB Service interface. IEC has the following features:

Cardholder: Create, Update, Read and Delete
Card: Create, Update, Read, Delete, Attach to Cardholder, Detach from Cardholder.
Access level: Get List of Access Levels in Bravida, Attach to Cardholders, Detach from Cardholders.

Bravida OPC Server
Bravida OPC Server is a program that serves as a link between Bravida Server and external systems. Bravida OPC Server enables interaction with external systems such as opening doors, controlling areas, controlling alarm relays and presenting alarm point statuses. OPC is an open standard for integration of systems. OPC (OLE for process control) is a standard specified by the OPC Foundation for communications between control devices from different manufacturers. This solution can be used together with a SCADA or HVAC system.

Bravida OPC Client
Bravida OPC Client is a program that serves as a link between external systems and Bravida Server. OPC Client converts OPC Tags into points that can be shown in Bravida Client as standard objects. There are two kinds of objects that can be created in Bravida Client – Inputs (External Digital Input) and outputs (External Digital Output). This solution can be used together with a Bravida and Panasonic CCTV system.

Bravida Alarm Service
Bravida Alarm Service is a program that serves as a link between external systems, such as a paging system from 3rd party suppliers and Bravida Server. This solution can be used between Bravida and a Panasonic Fire Alarm system.

BASE
For smaller systems that require a high level of security and user-friendliness, but have fewer door environments and alarm points.

PREMIUM
For medium-sized to large systems or when you want to integrate other products via one of the many interfaces supported by Bravida. Well-structured and easy-to-use alarm graphics can be used to visualise and manage alarm points.

ENTERPRISE
For large systems that demand high performance and functionality. Well-structured and easy-to-use alarm graphics can be used to visualise and manage alarm points.
CARD READERS

Bravida includes a number of different card reader models (BCR) that support proximity keycards, such as EM-Marine, Mifare and DESFire. All other card models that support Wiegand or ‘data-clock’ interfaces can be used, including various types of biometric systems. All SmartCard readers are ready for NFC-reading.

BCR-SD 1.5 AND BCR-S MINI PROXIMITY SMARTCARD READERS

**BCR-SD 1.5**

A BCR-SD 1.5 card reader is included in the Bravida access system for contactless card reading. The BCR-SD 1.5 has a keypad for use in door environments that require an access code.

The card reader is equipped with a built-in antenna for card reading, a clearly visible keypad, LED indication, internal buzzer and convenient display for graphical symbols. The card reader is protected against substations and intruders in a sturdy ABS case with an RS485 interface. The reader has certification class S-EN 50131-3:2009, grade 4.

**BCR-S Mini**

A BCR-S Mini card reader is included in the Bravida access system for contactless card reading. This card reader has a sturdy design. The card reader features a built-in antenna for card reading, LED indication, internal buzzer and an RS485 interface with molded plastic encapsulation.

DOOR NODES AND ALARM NODES

Various nodes for door controls and alarms are connected to substations.

**S-Node**

The S-Node is a door control and alarm unit for high-security doors. It can also be used purely as an I/O unit that supervises up to 16 alarm inputs and performs any actions required. S-Node provides in basic configuration eight double balanced inputs and four digital outputs. The number of inputs and outputs can be extended with different expansion cards. S-Node communicates with superior C-Node G2 via LonWorks FTT110. The unit supports fast and easy remote firmware upgrade.

**ComHub**

The ComHub is a door box for 1:8 BCR-SW wireless readers. The ComHub communicates with a host C-Node on RS485. The ComHub is powered by 24 VDC.

ACCESS CONTROL UNIT

Substation C-Node G2

C-Node G2 is a powerful central unit with a full configuration database. The purpose of unit is to maintain alarm and access control functions, all in one device. It integrates all required functionality including standalone operations. C-Node G2 handles all cards, time programs, alarm handling, security levels and other integral functions of the system. Based on the configuration it makes all decisions and sends alarm data to the supervising Bravida system. The unit supports fast and easy remote firmware upgrade so new functions are delivered just by click of your mouse. Optimized memory management offers possibility to store up to 250 000 cards. C-Node G2 communicates with Bravida Server via TCP/IP.

POWER SUPPLY WITH BATTERY (UPS)

The C-Node G2 and underlying units are supplied with DC power from a separate battery pack with two 40 Ah batteries, larger if so required. This provides sufficient power for several hours of operation in the event of a power outage.

THE BCR-SD 1.5 AND BCR-S MINI CAN READ MIFARE CLASSIC, MIFARE PLUS AND DESFIRE EV1 CARDS:

MifareClassic - UID 4 or 7 bytes, sector reading and MAD 1 and 2, Mifare Plus - UID 4 or 7 bytes, sector reading and MAD 1 and 2, Security Level 0-3, including switching to higher Security Level, DESFire EV1 - UID 7 bytes and random UID, AES 128.

The card readers are generally mounted on non-secure side of door environment with the S-Node door control unit in a sub-assembly. The elegant and robust design allows both inside and outdoor installations. The card reader is subjected to robust ABS case with an EIA485 interface. The reader has certification class S-EN 50131-3:2009, grade 4.

NXP Semiconductor has developed the Mifare smart card technology. Mifare is based on the HID technology that is currently used in fields such as transport, payment services and security, for example. The technology is especially useful due to its capability to save data in several sectors on a card. Smart cards can provide data in several different ways, simply in UID, than sector data, MAD1 and MAD2 and on the end the file system on DESFire cards.

Card readers with Mifare technology read cards at a distance of up to 6cm from the reader (CR80 Cards). The reading distance varies depending on the surroundings and any radio or metallic interference.

The cards for Mifare and Prox readers can be supplied as traditional cards or keyrings. Credit card-size proximity cards (CR80) can be combined with a magnetic strip and printed using a standard card printer.

THE BCR-SD 1.5 AND BCR-S MINI CAN READ MIFARE CLASSIC, MIFARE PLUS AND DESFIRE EV1 CARDS:
BCR-PD 1.5 AND BCR-P MINI PROXIMITY READERS FOR PROX EM MARIN

BCR-PD 1.5

A BCR-PD 1.5 card reader is included in the Bravida access system for contactless card reading. The BCR-PD 1.5 has a keypad for use in door environments that require an access code. The card reader is equipped with a built-in antenna for card reading, a clearly visible keypad, LED indication, internal buzzer and convenient display for graphical symbols. The card reader is protected against sabotage in a sturdy ABS case with an EIA485 interface. The reader has Certification class SS-EN 50131-3:2009, grade 4.

BCR-P Mini

A BCR-P Mini card reader is included in the Bravida access system for contactless card reading. This card reader has a sturdy design. The card reader features a built-in antenna for card reading, LED indication, internal buzzer and an EIA485 interface with moulded plastic encapsulation.

BCR-PD 1.5 and BCR-P Mini

These are visually same readers as BCR-SD and BCR-S Mini but compatible with 125kHz proximity cards from EM MARIN. Readers are supporting 4300 RO and 4550 RW at the same time. Card readers with EM-Marin technology read the card at a distance of up to 12 cm from the reader. The reading distance varies depending on the surroundings and any radio interference.

The card readers are generally mounted in a door environment with the S-Node door control unit in a sub-assembly. The lightweight format is easy to position for ultimate user convenience. The EM-Marine cards can be supplied as traditional cards or keyrings. Credit card size proximity cards can be combined with a magnetic strip and printed using a standard card printer.

BCR-SW WIRELESS PROXIMITY READERS FOR SMARTCARDS

BCR-SW

BCR-SW is the smart technology that enables mechanical locks to be wirelessly linked to Bravida access control systems. The heart of BCR-SW is a short-range, wireless communications protocol, designed to link with an online electronic access system with a BCR-SW-enabled mechanical lock. A straightforward, easy and convenient way to add more monitored doors to a security system, BCR-SW allows for online access control and management, increasing both security and controllability.

BCR-SW is compatible with MIFARE & DESFIRE EV1 cards – UID and sector data reading.
BRAVIDA V6 SUPPORTS:

- **EM-Marine:** 4200 RO and 4550 RW
- **Mifare Classic:** UID, sector reading and MAD with 4 or 7 bytes
- **Mifare Plus:** UID, sector reading and MAD SL 0-3 with 4 or 7 bytes
- **Mifare DESFire EV1:** UID and AES encrypted Application reading.

**KEYCARDS**

**PROXIMITY CARDS, TAGS AND SMART CARDS (RFID)**

This technology is based on radio signals. The card contains an integrated circuit that draws current from a coil in the card when the card is moved close to the reader. The card therefore has no battery and will continue to work provided there is no physical damage to the card or tag. Credit card-size cards are available. These can also be combined with a magnetic strip or smart card chip. Keying tags of various designs are also available. However, tags do have a slightly shorter read distance.

**BRAVIDA (INTEGRATED BY PANASONIC)**

**NO. 1 ON SMART CARDS**

With Bravida V6 a lot of effort has gone into developing a simple administrative solution for smart cards. Reading keys for Mifare sector reading and MAD can be downloaded from a central location using encrypted communications and without any separate programming of card readers.

Bravida V6 supports several reading keys in the same card reader for Mifare sectors and MAD reading, which means that in addition to the customer’s unique keys, the same system can also read cards from several suppliers, e.g. SITHS (county councils), ID06, etc.

**MIFARE CLASSIC**

Mifare Classic can be used with ISO/IEC 14443-A unique serial numbers, 4 or 7 bytes and random IDs. The security level uses CRYPTO1 encryption based on a 48-bit key length.

**MIFARE PLUS**

Mifare Plus can be used with ISO/IEC 14443-A unique serial numbers, 4 or 7 bytes and random IDs. Mifare Plus cards can be used on multiple security levels. The highest security level uses AES (Advanced Encryption Standard) encryption based on a 128-bit key length. The lowest security level uses CRYPTO1. To facilitate the migration process for existing infrastructures based on MIFARE Classic, the MIFARE Plus chip on its lowest security level is backwards compatible with MIFARE Classic. Cards using chips on this lowest security level can be switched to a higher security level. Once a card is switched, it can only operate at that higher security level and cannot be switched back to a lower security level.

- **Security Level 0** – MIFARE Plus cards are pre-personalised with configuration keys, level-switching keys, MIFARE Classic CRYPTO1 and AES keys for the memory.
- **Security Level 1** – On this level, the cards are 100% functionally backwards compatible with MIFARE Classic 1K/4K cards. Cards work seamlessly in existing MIFARE Classic infrastructures.
- **Security Level 2** – Mandatory AES authentication. MIFARE Classic CRYPTO1 for data confidentiality.
- **Security Level 3** – Mandatory AES for authentication, communications confidentiality and integrity. Optional proximity detection (MIFARE Plus X only).

**MIFARE DESFIRE**

Mifare DesFire can be used with ISO/IEC 14443-A unique serial numbers, 7 bytes and random IDs. Mifare DESFire cards can be used on multiple file system and fully compliant with ISO/IEC 14443A (part 1-4) using optional ISO/IEC 7816-4 commands security levels. The highest security level uses AES (Advanced Encryption Standard) encryption based on a 128-bit key length. This enables MIFARE DESFire EV1 to hold up to 28 different applications and 32 files per application in its flexible file system.
COMMUNICATIONS BETWEEN SERVERS AND C-NODES

COMMUNICATION VIA ETHERNET/IP VPN
TCP/IP communications over a network is the best option when communications involve units at multiple geographic locations. The C-Node G2 contains a built-in network card for communications over Ethernet via TCP/IP protocols. The substation can then be connected to the PC network while it is online. A fixed IP address is defined for the C-Node G2.

SYSTEM DESIGN

Communication via LON (Echelon FTT-10)
LON bus communications are used for communications between the C-Node G2 and sub-node (S-Node). This method is intended for situations when there are multiple substations within a relatively small area. The cable distances without using repeaters are comparatively long and cabling is easy. Network cards are not necessary. The C-Node G2 has a built-in communication port for LON communications with sub-nodes.

Communication via Wi-Fi
RS485 bus communications are used for communications between the C-Node G2 and radio hub for Wi-Fi readers. The cable distances without using repeaters are comparatively long and the cabling is easy.

The C-Node G2 has two built-in communications ports for RS485 communications. Wi-Fi communications between a radio hub and BCR-SW readers comply with IEEE 802.15.4 and define the medium access control and the physical layer for WSN. It operates primarily in the 2.4-GHz band, using 16 channels. The bandwidth of each channel is 5 MHz. The MAC employs the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) mechanism. CCA (Clear Channel Assessment) is used in the physical layer to determine the channel occupancy. Distance between HUB and Wi-Fi readers can be up to 25 meters.

MANAGEMENT SYSTEM | WORKFLOW SYSTEM | HR SYSTEM

CCTV | FIRE | ALARM | VISITOR | BMS | X

C-NODE | C-NODE | HUB

S-NODE | S-NODE | S-NODE

ELEVATOR NODE

VISITOR BMS X
FIRE
ALARM

12 13
SOFTWARE, PLATFORMS AND FUNCTIONS

OPERATING SYSTEMS AND PROGRAMMING LANGUAGE

The system employs a standard PC platform and is compatible with Windows Vista, Windows 7, Windows 8, and Microsoft Server 2008 and Microsoft Server 2012, 32- or 64-bit R2.

DATABASE

The system uses SQL Server as a database. The actual database is normally MS SQL 2012 Express. The full version of SQL Server can also be used. The database is run as a background program for Bravida Server PC. Bravida is compatible with MS SQL 2008 and 2012 64-bit R2.

SCREEN MANAGEMENT

Administrative tasks are performed in an environment similar to Windows Explorer. The structure comprises folders and objects in the same way as Windows Explorer. Objects represent all users, components and parameters present in the system. Folders with subfolders are created individually as required. The system uses the ‘drag and drop’ principle to move objects between folders and to link objects. One example would be access permission for users.

ACCESS LEVELS

The access permissions in the system are based on a combination of card readers. Each card reader can be linked to a time zone to define when a card with specific rights can be used. Access permission can also be linked to access the setting for ‘ bistable opening’, when a card reader is used to set a door to permanent open mode.

TIME ZONES

Day schedule for time zones
The day schedule defines periods within each 24 hours when a time zone will be on and off. One-minute intervals are used. The period is defined using the left and right mouse buttons for on and off respectively, and can be highlighted using the mouse cursor to change periods within the 24-hour period. The day schedule follows the predefined time period.

Time zone (comprising day schedule)
Time zones are used for normal time-controlled functions, such as restricted access to doors. A time zone is made up of several day time zones. A day time zone can last for several days for a single activity. This is determined in the field used to select the ‘Day’ period. The periods that can be selected are:

- Date
- Special days
- Monday–Friday
- Holidays

A time zone is normally made up of Monday–Friday, Saturday–Sunday and a holiday.

Calendar
The calendar function is used to specify the function of a time zone on an unspecified holiday.

Analogue time zone
An analogue time zone is used to limit functions by time, for instance, open doors with a time limit (e.g. 30 min) or ‘buy time’ when bypassing burglar alarms.

SECURITY LEVELS

The security level determines how the various card readers will function during the day.

Security level
A security level is created in the same way as a time zone, but uses a day schedule for the security level. A security level can be used by one or more card readers.

Day schedule for Security Level
A day schedule for a security level determines how a card reader will function during the day. The options include:

- Unlocked: Usually a main entrance during normal working hours
- Card: Usually a department door during normal working hours
- Locked: Usually a back door during evenings
- Card+PIN: Normally all doors with a keypad during evenings/night
- Card Toggle: Usually an office door that is opened/closed regularly
- Card+PIN Toggle: As above but with PIN code
- GIN: General code
- PGIN: Personal code
SYSTEM SECURITY

COMMUNICATIONS

Communications between Bravida Server and substations is possible over different communications interfaces. Regardless of the type of communications, data can be encrypted, which increases security.

Between substations and door environments
Communications between substations and door environments/nodes are via LON FTT-10. This communication type can also be encrypted. All sensitive data between the Bravida Server and card reader are encrypted with AES128 to protect sensitive content.

DATABASE

Microsoft SQL Server is used as the system database. The necessary security systems are built-in with MS SQL. For more detailed information, please refer to the document: C2 Administrator’s and User’s Security Guide.

PASSWORD PROCEDURES

Bravida requires users to have their own passwords, which are chosen by each user.

Operator
User access will be defined for each user:
• How long the user will remain logged in
• The time or date for which permission applies
• Rules on how long a password remains valid

There is no limit to the number of users that can be defined.

All passwords are encrypted and stored in the database.

User groups
Each user is assigned to a user group. The various user groups receive different access rights to folders in the system. Access to folders is configured for functions such as display, change and delete.

ALARM COLLECTION, PRESENTATION AND MANAGEMENT

COLLECTING ALARMS

Alarm inputs on S-Node
An S-Node can be used as a combined door and IO node or solely as an IO node. When used solely as an IO node, it has 8 double-balanced alarm inputs and 4 relay outputs.

ACKNOWLEDGE ALARMS ON AN ALARM LIST

An alarm list of unacknowledged alarms can be shown on the screen. Various colours are used to indicate status. Active alarms appear in red. Active acknowledged alarms appear in green, etc. For more information, please refer to the user manual. Alarms are assigned to the presentation group. The operator is assigned access to one or more presentation groups. This can be used for example, to alert maintenance personnel of technical alarms, and security guards of burglar alarms.

GRAPHICAL AND DYNAMIC ALARM PRESENTATION

The system features an integrated graphical presentation of alarms. Alarms can be immediately displayed on a zone map, and doors can be opened remotely from the map.

MANAGEMENT OF ALARMS IN CARD READERS

An alarm zone that may comprise one or more alarm points can be defined for the system. Various actions can be implemented for card readers with keypads and displays.

• Alarm zones can be switched off and on
• ‘Buy alarm bypass time’
• Transmission of status of current areas/zones
• Triggered alarms can be shown on the card reader display
• Inhibit points
• Etc.

Authorization to handle alarms can be assigned to any card user and by any reader in the system.
SPECIAL FUNCTIONS

LIFT CONTROL

The standard C-Node G2 is used for access control in lifts. The solution makes it possible to define a virtual card reader for each floor. A physical card reader is installed in the lift. Virtual card readers are added at access levels, making it possible to assign different access levels to each floor. When the card is read by the card reader in the lift, a relay is activated for each floor to which access is granted. The relays are connected to the lift control unit. The buttons for the floors to which the cardholder has access are now activated. The lift control solution can be used for several functions like one reader for several doors or cabinets.

SMS TO MOBILE PHONES

System messages can be sent to a mobile phone as SMS messages. Messages are sent to third-party software using the SMTP protocol. The Omnigate software forwards alarms via a telephone with a SIM card.

INTERFACES WITH OTHER SYSTEMS

Bravida can interact with other systems. We have chosen to integrate card production and alarm collection/management in Bravida. In addition, Bravida can be integrated with other systems using a variety of interfaces.

CCTV SYSTEMS

Bravida is integrated with the CCTV platform from Panasonic. It also has the ability to integrate with other available systems. This integration is implemented over OPC communications between Bravida and the Panasonic CCTV platform.

One example of using OPC interface is starting the camera recording in a specific area triggered by alarm from movement detector.

OPC INTERFACE

Bravida includes an OPC Server and OPC Client. This makes a number of solutions possible for interaction with other systems. One example is displaying messages from components and controlling components in the Bravida system from a host presentation system.

OPC CLIENT & SERVER

With an OPC Client, Bravida can among other things, receive and display alarms, and handle instructions from other systems. With an OPC Server, the Bravida system can control functions in other systems. The OPC Client is also used in integration with other systems like CCTV platforms.

FIRE ALARMS

There is an interface in Bravida to integrate fire alarm panels from Panasonic. The idea behind this integration is that fire alarms can be presented and displayed as a part of Bravida’s alarm graphics. The alarms can also be displayed using Bravida’s presentation system.

DATABASE INTERFACES FOR HR DATABASES

There is a program module that has been developed for exchanging data with other databases. For example, student registries or other personnel databases. This function can automate and simplify card administration for large access systems with many users.

TERMINAL SERVER CLIENTS

Bravida Client can be run on thin clients (Citrix Client) connected to a terminal server. The Bravida Server software is installed on an external server/PC and connected to Citrix Terminal Server via a network. Please contact us for more information about this solution.