

R A D I O N I C S



Radionics[®]

READYKEY[®] K6100 Readykey for Windows[™]

RISSC[™] Application Installation Manual

Notice

The material and instructions in this manual have been carefully checked for accuracy and are presumed to be reliable. However, Radionics, Inc. assumes no responsibility for inaccuracies and reserves the right to modify and revise this manual without notice. It is our goal at Radionics to always supply accurate and reliable documentation. If a discrepancy is found in this documentation, please mail a photocopy of the corrected material to:

Radionics, Inc.
Technical Writing Department
1800 Abbott Street
Salinas, California 93901

UL Listing

UL 294 - Access Control System Units

FCC Notice

This equipment generates and uses radio frequency energy. If not installed and used in accordance with the manufacturer's instructions, it may cause interference to radio and television reception. It has been tested and found to comply with the specifications Subpart F of Part 15 of FCC rules for Field Disturbance Sensors. If this equipment causes interference to radio or television reception - which can be determined by turning the equipment on and off - the installer is encouraged to correct the interference by one or more of the following measures: 1) Reorient the antenna of the radio/television, 2) Connect the AC power cord to a different outlet so the control panel and radio/television are on different branch circuits, 3) Relocate the control panel with respect to the radio/television.

If necessary, the installer should consult an experienced radio/television technician for additional suggestions, or send for the "Interference Handbook" prepared by the Federal Communications Commission. This booklet is available from the U.S. Government Printing Office, Washington D.C. 20402, stock no. 004-000-00450-7.

Readykey is a registered trademark of Radionics, Inc.

RISSC is a trademark of Radionics, Inc.

Window is a trademark of Microsoft Corporation

Table of Contents

| | |
|---|-----------|
| Introduction | 1 |
| Other Documents..... | 1 |
| Compatibility..... | 1 |
| Required Tools | 1 |
| Basic Operation..... | 1 |
| Installation Notes..... | 2 |
| Application Programming | 3 |
| Define PRS and DRS Areas..... | 3 |
| Define PRS and DRS Readers..... | 4 |
| Define Controllers and Select Onboard Relay Outputs | 5 |
| Define Outputs (K2100 / K1100 Onboard Relays) | 6 |
| Define Inputs | 8 |
| Define Outputs (K2015A)..... | 9 |
| PC #2 Outputs..... | 12 |
| Administration - Define Access Groups | 13 |
| DIAGRAM 1 | 14 |
| DIAGRAM 2 | 15 |
| APPENDIX I Power Relay Switch -- Controller Connections | 16 |
| APPENDIX II Data Relay Switch -- Network Connections | 17 |
| APPENDIX III Data Relay Switch -- Faceplate and Controller Connections | 18 |

Introduction

The READYKEY® **INFORMATION SECURITY SYSTEM** for COMPUTERS (RISSC™) application has been developed as an additional means of securing access to information systems. The Administration PC running Readykey software requires a Microsoft Operating System but can control physical access to computers running most common operating systems or networks.

Other Documents

This RISSC™ Application and Installation Manual should be read in conjunction with the following documents:

K2100 / K1100 Operation / Installation Manual
K2015A Alarm Event Manager Installation Manual
Data Relay, Single Protection, and Power Relay Switch Installation Manuals
D8132 Power Supply Manual

Compatibility

Readykey® For Windows™ Ver 3.2 or Later
K2100 / K1100 Controllers Ver 3.0 or Later

Required Tools

When installing a DRS, SPS or PRS control wire as illustrated in the RISSC™ Application and Installation Manual, the technician will need an RJ45 crimp tool. Purchase a CAT5 Modular Plug Kit from Black Box **Part # FTM650** (Includes 1 modular termination tool, 1 4-pair die set, 100 modular RJ-45 plugs in a compact metal case). For troubleshooting, use standard RJ45 terminations jacks to meter wire connections. D166 RJ31X jacks can be used for this purpose.

Basic Operation

A valid read with a Readykey key or card and manually switching from the GREEN position (non-secure network) to the RED position (secured network) at the DATA RELAY SWITCH (DRS)* will complete connection to the secured network and physically isolate the computer from other network drives while logging an "Access Authorized" transaction to the Readykey transaction history. A valid read at the POWER RELAY SWITCH (PRS) will connect power to the computer and log an "Access Authorized" transaction to the Readykey transaction history. A DRS related tamper alarm will be sent to the System Administrator and will interrupt the secured network drive connection from the computer until the System Administrator has accepted the alarm. A PRS related tamper alarm will be sent to the System Administrator and will interrupt power to the computer as well as interrupt the secured network drive until the alarm is accepted by the System Administrator.

A Single Protection Switch (SPS) installation and operation is the same as a Data Relay Switch (DRS) with only a single network connection. All operation is identical, with the exception of the manual switching of the DRS. From this point forward, it is assumed in this document that the DRS and SPS units are considered the same.

* Manually switching the DRS - See **DIAGRAM 2** at the end of this manual.

Installation Notes

- (1) K2100 Controller and (1) K2015A Alarm Event Manager can control access to power and network connection for 2 workstations. All control and reader connections are run from the Readykey controller in a secured area to the protected workstation and are terminated at the DRS and PRS via RJ45. The installer will need to make RJ45 connections or use standard RJ45 cables with a tampered termination. Line supervision resistors for the K2015A tamper inputs are already located inside the PRS and DRS units. The K2003 PRS reader can be concealed in the computer box and be activated with a read from a Readykey Proximity key or card. The internal sounder in the K2003 serves as a local alarm at the workstation in the event of a tamper. The PRS and DRS modules and reader LEDs are controlled by a SET/RESET function from an "Access Authorized" event via K2100/K1100 onboard relays. In Readykey for Windows, programming door alarm and K2015A tamper inputs to "Manual Accept" cause the PRS and DRS modules to latch into Alarm/Interrupt mode until the System Administrator accepts the alarm at the point of administration. A separate power supply will be required. SEE **DIAGRAM 1**, at the end of this RISSC™ Application and Installation Manual for a complete wiring diagram for a 2 PC installation.

Application Programming

(The following programming guide depicts a single workstation installation consuming 2 reader channels. A second workstation would be added to channels 3 and 4 of a K2100 and would utilize Tamper Inputs and Control Outputs of the existing K2015A AEM connected to channel 2.)

Defining PRS and DRS Areas in **Installer: Areas**

Defining PRS and DRS Readers in **Installer: Doors**

Defining the Alarm Event Manager in **Installer: Alarm Modules**

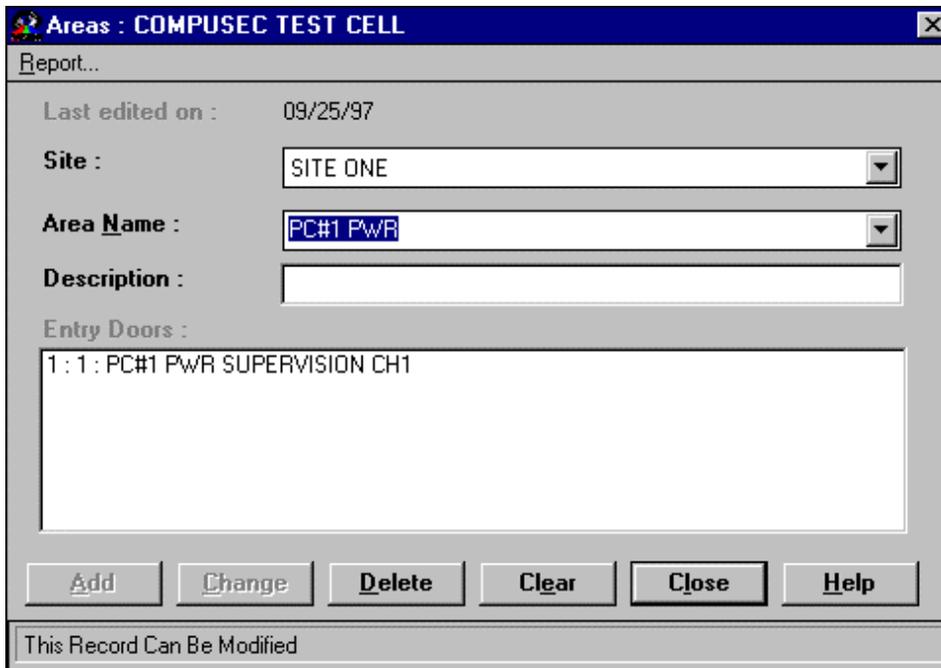
Defining the **Outputs...** of the Onboard Relays

Defining the **Inputs...** of the Alarm Event Manager

Defining the **Outputs...** of the Alarm Event Manager

Creating and modifying authority levels in **Admin: Access Groups**

Define PRS and DRS Areas



1. Start the **Areas** sub-application from within the **Installer** icon group.
2. Make sure the correct **Division** is displayed in the title bar.
3. Select the appropriate **Site** if applicable.
4. Create an **Area Name** that describes the PC or Network to be accessed.
5. Use **Description** to describe location details of access area.

Define PRS and DRS Readers

Doors : COMPUSEC TEST CELL

Report..

Last edited on : 04/22/98

Sites : SITE ONE

Door Controller : MASTER CONTROLLER

Channel Number : 1

Door Name : PC#1 PWR SUPERVISION CH1

Description :

Time Profile : NONE.

Doors on Controller

Controller : Channel : Door Name

1 : 1 : PC#1 PWR SUPERVISION CH1
 1 : 2 : PC#1 DATA SUPERVISION CH2
 1 : 3 : PC#2 PWR SUPERVISION CH3
 1 : 4 : PC#2 DATA SUPERVISION CH4

Door Information

Lock Time : 3 Door Open Time : 2

Reader Type : K2003 MULLION READER

Entry Area : PC#1 PWR

Pin Reader Time Profile : NONE.

Fail Safe Lock : Request For Entry : Elevator Reader :

Exit out of Hours : Emergency Override : Free Exit :

Alarm Graphic : PCPRALM.BMP

Browse...

Add Change Delete Clear Close Help

This Record Can Be Modified

1. Start the **Doors** sub-application from within the **Installer** icon group.
2. Make sure the correct **Division** is displayed in the title bar.
3. Select the appropriate **Site** if applicable.
4. Select the **Door Controller** that the PRS or DRS readers are connected to.
5. Select the **Channel Number** for the PRS or DRS readers are connected to.
6. Create the Door Name that describes the reader name and function.
7. Use the **Description** field to describe location details of the reader.
8. **Time Profile** is not used in this application.
9. **Lock Time** of “3” and **Door Open Time** of “2” are the recommended settings.
10. **Reader Type** of “K2003” for the PRS and **Reader Type** of “K2001” for the DRS are the recommended settings.
11. Select the **Entry Area** that depicts the appropriate PC power that the PRS will control and the **Entry Area** that depicts the appropriate PC / Network that the DRS will control.
12. Pin Reader Time Profile and all remaining check boxes left are not used in this application.

Define Controllers and Select Onboard Relay Outputs

Controllers : COMPUSEC TEST CELL

Report...

Last Edited on : 10/13/97

Site :

Door Controller Name :

Door Controller Type :

Description :

Address :

Enable Controller:

Door Controller Information

Lock Sharing (1-4) Lock Sharing (2-3) : Passback On Exit :

Passback Doors (1-4) Passback Doors (2-3) : Passback Timeout :

Manual alarm accept :

All Controllers

Number : Name

1 : MASTER CONTROLLER

Outputs

This Record Can Be Modified

1. Start the **Controllers** sub-application from within the **Installer** icon group.
2. Make sure the correct **Division** is displayed in the title bar.
3. Select the appropriate **Site** if applicable.
4. Create the **Door Controller Name** of the outputs you will need to program.
5. Select **Controller Type**. A "K1100V3" 2 channel Controller is needed for 1 Workstation.
6. Select the Address 1 for Controller 1.
7. Make sure **Enable Controller** is selected.
8. **Manual alarm accept** must be selected for proper output operation.
9. Click on the **Outputs** button at the bottom of this screen.

Define Outputs (K2100 / K1100 Onboard Relays)

Note: The controller **Onboard Relay Outputs** control power switching to the PRS and DRS modules. When an “**Access Authorized**” event occurs at the PRS or DRS module, the associated relay will set to latch power to the PRS or DRS module.

When the PRS Relay Action is “Set”, the PRS will be energized, connecting the now “Logged In” user to the PC power. When the DRS Relay Action is “Set” the DRS will be energized, connecting the now Logged In user to the secured network. Once an output to the PRS or DRS is “Set”, a subsequent “Access Authorized” event will “Reset”, logging the user off from the respective PRS or DRS connection.

Relay Output : COMPUSEC TEST CELL

Report...

Last edited on : 09/25/97 Controller Number : 1 : MASTER CONTROLLER
 Name :

Relay Number : 1

Relay Name : RLY 1 SET=LOGGED IN / RESET = LOGGED OUT

Description :

Time Profile : NONE

Event code 1 : ACCESS AUTHORIZED

Door Name : PC#1 PWR SUPERVISION CH1

Event code 2 : NOT AFFECTED

No Source :

Event code 3 : NOT AFFECTED

No Source :

Event code 4 : NOT AFFECTED

No Source :

Relay Action Type : SET/RESET

Pulse Period : 0 Secs Wait Time : 0 Secs.

Maximum Activation Time : 0 Mins

Change

Close

Help

This Record Can Be Modified

1. Change **Relay Name** to describe **set** and **reset** functions.
2. Use the **Description** field if needed.
3. **Time Profile** is not used in this application.
4. Select “Access Authorized” for **Event code 1**.
5. Select appropriate **Door Name** that controlled by this output.
6. Select “Set/Reset” for **Relay Action Type**.
7. Repeat the above programming for the DRS switch on the next available output.*

* POINT 7 IS A PRELIMINARY ADDITION

Alarm Modules : COMPUSEC TEST CELL

Report...

Last edited on : 09/26/97

Site : SITE ONE

Door Controller : MASTER CONTROLLER

Channel Number : 2

Alarm Module : ALARM MODULE

Description : TAMPER INPUTS AND OUTPUTS

Type : K2015A ALARM EVENT MANAGER

Alarm Modules on Controller

| Controller | Channel | Name |
|------------|---------|--------------|
| 1 | 2 | ALARM MODULE |

Inputs... Outputs...

Add Change Delete Clear Close Help

This Record Can Be Modified

1. Start the **Alarm Module** * sub-application from within the **Installer** icon group.
2. Select the appropriate **Site** if applicable.
3. Select the **Door Controller** that this module will be run to.
4. Select the **Channel Number** that this module will be connected to.
5. Create **Alarm Module** name.
6. Use **Description** to describe module functions.
7. Select “**K2015A ALARM EVENT MANAGER**” in **Type** field.
8. Click on **Inputs...** button for input options and **Outputs...** button for output options.

*PRELIMINARY EDIT

Define Inputs

Report...

Last edited on : 09/26/97 Controller Number : 1 : MASTER CONTROLLER
 Channel Number : 2

Input Name : PC#1 PRS TAMPER INPUT Alarm Input Number : 1

Description : CHECK PC #1

Time Profile : NONE

Graphic File : Browse...

Re-arm Count : 0

Output 1 Attached : Output 2 Attached : Output 3 Attached : Output 4 Attached :

Alarm Options

Disable Input : Input Normally Open :
 Normal Input : 4 State :
 24 Hour Input : Acknowledge Required :
 Relay Follows Input :

Change Close Help

This Record Can Be Modified

1. From **Alarm Modules** screen, click on **Inputs...**
2. Create **Input Name** for **PRS** and **DRS** tampers.
3. Use **Description** field to display action to be taken on alarm screen.
4. Select Graphic File that illustrates location of the **PRS** or **DRS** tamper.
5. Select "24 Hour Input".
6. **Select "Acknowledge Required"** so relay response will remain active until an operator accepts the alarm.
7. Select "Change" to accept the programming changes and activate the input.

1. Select **Input 2** for the **DRS** Tamper Alarm Input.
2. Create **Input Name** for **DRS** tamper alarm.
3. Use **Description** field to display action to be taken on alarm screen.
4. Select Graphic File that illustrates location of the **DRS** tamper.
5. Select "24 Hour Input".
6. **Select "Acknowledge Required"** so relay response will remain active until an operator accepts the alarm.
7. Select "Change" to accept the programming changes and activate the input.

Define Outputs (K2015A)

Note: *Alarm Outputs* are programmed to activate with a PRS and DRS “**Tampers Alarms**”. The **Relay Action Type** is set to “**latch**” to disable PRS and DRS Readers as well as activate the K2003 Reader’s sounder until the System Administrator acknowledges the tamper alarm. Notice that the PC power is only interrupted by power **PRS** related tamper activations while the Network connection is interrupted by **PRS** and **DRS** related tamper activations.

PC #1 PRS Disable (K2015A Output #1)

Alarm Output : COMPUSEC TEST CELL

Report..

Last edited on : 04/13/98 Controller Number : Name : 1 : MASTER CONTROLLER

Alarm Output Number : 1 Channel Number : 2

Output Name : PC#1 PRS DISABLE

Description : DISCONNECT POWER TO PRS

Time Profile : NONE

Event code 1 : ALARM ZONE ACTIVATE

Alarm Input : PC#1 PRS TAMPER INPUT

Event code 2 : DOOR ALARM/TAMPER

Door Name : PC#1 PWR SUPERVISION CH1

Event code 3 : NOT AFFECTED

No Source

Event code 4 : NOT AFFECTED

No Source

Relay Action Type : LATCHED

Pulse Period : 10 Secs Wait Time : 0 Secs

Maximum Activation Time : 0 Mins

Change

Close

Help

This Record Can Be Modified

1. From **Alarm Modules** screen, click on **Outputs...**
2. Create **Output Name** for **PRS Reader** to be disabled in event of a **PRS** tamper.
3. Use **Description** field to display action to be taken on alarm screen.
4. **Time Profile** is not used in this application.
5. Select “**Alarm Zone Activate**” for **Event code 1**.
6. Select “**PC #1 PRS Tamper Input**” to link this output to K2015A Input #1. (NOTE: This tamper is connected from pins 7 & 8 of the **PC #1 PRS** RJ45 see DIAGRAM 1)
7. Select “**Door Alarm / Tamper**” for **Event code 2**.
8. Select “**PC #1 Power Supervision CH 1**” to link this output to Door Channel #1. (NOTE: DR1 to GND of CH 1 is connected to pins 5 & 6 of the **PC #1 PRS** RJ45.)
9. **Event codes 3 & 4** are unused for the **PRS** output.
10. Set **Relay Action Type** to “**Latched**”.
11. Set **Wait Time** to “**0**” and **Maximum Activation Time** to “**0**”.

PC #1 DRS Disable (K2015A Output #2)

| Alarm Output : COMPUSEC TEST CELL | | |
|-----------------------------------|---------------------------|---------------------|
| Report... | | |
| Last edited on : | 09/25/97 | |
| Alarm Output Number : | 2 | |
| Controller Number : | 1 : MASTER CONTROLLER | |
| Channel Number : | 2 | |
| Output Name : | PC#1 DRS DISABLE | |
| Description : | DISCONNECT DRS ON ALARM | |
| Time Profile : | NONE. | |
| Event code 1 : | ALARM ZONE ACTIVATE | |
| Alarm Input | PC#1 PRS TAMPER INPUT | |
| Event code 2 : | DOOR ALARM/TAMPER | Change |
| Door Name | PC#1 PWR SUPERVISION CH1 | Close |
| Event code 3 : | ALARM ZONE ACTIVATE | Help |
| Alarm Input | PC#1 DRS TAMPER INPUT | |
| Event code 4 : | DOOR ALARM/TAMPER | |
| Door Name | PC#1 DATA SUPERVISION CH2 | |
| Relay Action Type : | LATCHED | |
| Pulse Period : | 10 Secs | Wait Time : 0 Secs. |
| Maximum Activation Time : | 0 Mins | |
| This Record Can Be Modified | | |

1. From **Alarm Modules** screen, click on **Outputs...**
2. Create **Output Name** for **PRS Reader** to be disabled in event of a **PRS** tamper.
3. Use **Description** field to display action to be taken on alarm screen.
4. **Time Profile** is not used in this application.
5. Select “**Alarm Zone Activate**” for **Event code 1**.
6. Select “**PC #1 PRS Tamper Input**” to link this output to K2015A Input #1. (NOTE: This tamper is connected from pins 7 & 8 of the **PC #1 PRS** RJ45 see DIAGRAM 1)
7. Select “**Door Alarm / Tamper**” for **Event code 2**.
8. Select “**PC #1 Power Supervision CH 1**” to link this output to Door Channel #1. (NOTE: DR1 to GND of CH 1 is connected to pins 5 & 6 of the **PC #1 PRS** RJ45.)
9. Select “**Alarm Zone Activate**” for **Event code 3**.
10. Select “**PC #1 DRS Tamper Input**” to link this output to K2015A Input #1. (NOTE: This tamper is connected from pins 7 & 8 of the **PC #1 DRS** RJ45 see DIAGRAM 1.)
11. Select “**Door Alarm / Tamper**” for **Event code 4**.
12. Select “**PC #1 DATA Supervision CH 2**” to link this output to Door Channel #2. [NOTE: DR1 to GND of K2015A, (connected to channel 2 of the controller) is connected to pins 5 & 6 of the **PC #1 PRS** RJ45.]
13. Set **Relay Action Type** to “**Latched**”.
14. Set **Wait Time** to “**0**” and **Maximum Activation Time** to “**0**”.

PC #1 PRS Reader Piezo Alarm (K2015A Output #3)

| Alarm Output : COMPUSEC TEST CELL | |
|-----------------------------------|--|
| Report.. | |
| Last edited on : | 01/14/98 Controller Number : Name : 1 : MASTER CONTROLLER |
| Alarm Output Number : | 3 Channel Number : 2 |
| Output Name : | PC#1 PRS READER PIEZO ALARM |
| Description : | |
| Time Profile : | NONE. |
| Event code 1 : Alarm Input | ALARM ZONE ACTIVATE PC#1 PRS TAMPER INPUT |
| Event code 2 : Door Name | DOOR ALARM/TAMPER PC#1 PWR SUPERVISION CH1 |
| Event code 3 : Alarm Input | ALARM ZONE ACTIVATE PC#1 DRS TAMPER INPUT |
| Event code 4 : Door Name | DOOR ALARM/TAMPER PC#1 DATA SUPERVISION CH2 |
| Relay Action Type : | LATCHED |
| Pulse Period : | 10 Secs Wait Time : 0 Secs. |
| Maximum Activation Time : | 1 Mins |
| This Record Can Be Modified | |

WARNING: Tamper Alarm will result in power loss to the workstation.

1. From **Alarm Modules** screen, click on **Outputs...**
2. Create **Output Name** for **K2003 PRS Reader** to sound in the event of a **PRS or DRS tamper** activation.
3. Use **Description** field to display action to be taken on alarm screen.
4. **Time Profile** is not used in this application.
5. Select "**Alarm Zone Activate**" for **Event code 1**.
6. Select "**PC #1 PRS Tamper Input**" to link this output to K2015A Input #1. (NOTE: This tamper is connected from pins 7 & 8 of the **PC #1 PRS** RJ45 see DIAGRAM 1.)
7. Select "**Door Alarm / Tamper**" for **Event code 2**.
8. Select "**PC #1 Power Supervision CH 1**" to link this output to Door Channel #1. (NOTE: DR1 to GND of CH 1 is connected to pins 5 & 6 of the **PC #1 PRS** RJ45.)
9. Select "**Alarm Zone Activate**" for **Event code 3**.
10. Select "**PC #1 DRS Tamper Input**" to link this output to K2015A Input #1. (NOTE: This tamper is connected from pins 7 & 8 of the **PC #1 DRS** RJ45 see DIAGRAM 1.)
11. Select "**Door Alarm / Tamper**" for **Event code 4**.
12. Select "**PC #1 DATA Supervision CH 2**" to link this output to Door Channel #2. [NOTE: DR1 to GND of K2015A, (connected to channel 2 of the controller) is connected to pins 5 & 6 of the **PC #1 PRS** RJ45.]
13. Set **Relay Action Type** to "**Latched**".
14. Set **Wait Time** to "**0**" and **Max. Activation Time** to "**1**" for 1 minute cutoff time.

PC #2 Outputs

Use the same programming above on Outputs 4 - 6 of the K2015A to control Reader Channels 3 and 4 of a K2100.

Administration - Define Access Groups

Access Groups : COMPUSEC TEST CELL

Report...

Last edited on : 09/25/97

Site : SITE ONE

Name : FULL ACCESS

Description :

Time Profile 1 : NONE.

Time Profile 2 : NONE.

Access List 1 : Areas...

Access List 2 : Areas...

AREA : PC#1 DATA RELAY ACCESS
AREA : PC#1 PWR
AREA : PC#2 DATA RELAY ACCESS
AREA : PC#2 PWR

Add Change Delete Clear Close Help

This Record Can Be Modified

1. Start the **Access Groups** sub-application from within the **Admin** icon group.
2. Make sure the correct **Division** is displayed in the title bar.
3. Select the appropriate **Site** if applicable.
4. Create a **Name** that describes the PC power and Network access that will be assigned to a **Personnel** record.
5. Use **Time Profile 1 and 2** to select time restrictions to various PC power and network access areas. Leave “None” in **Time Profile 1 and 2** to select access areas with no Time Profile restrictions.
6. Click on **Areas...** to select access areas listings for **Access List 1 and 2**.

Access Groups

Available

Select Deselect OK Cancel

Selected

PC#1 DATA RELAY ACCESS
PC#1 PWR
PC#2 DATA RELAY ACCESS
PC#2 PWR

DIAGRAM 1

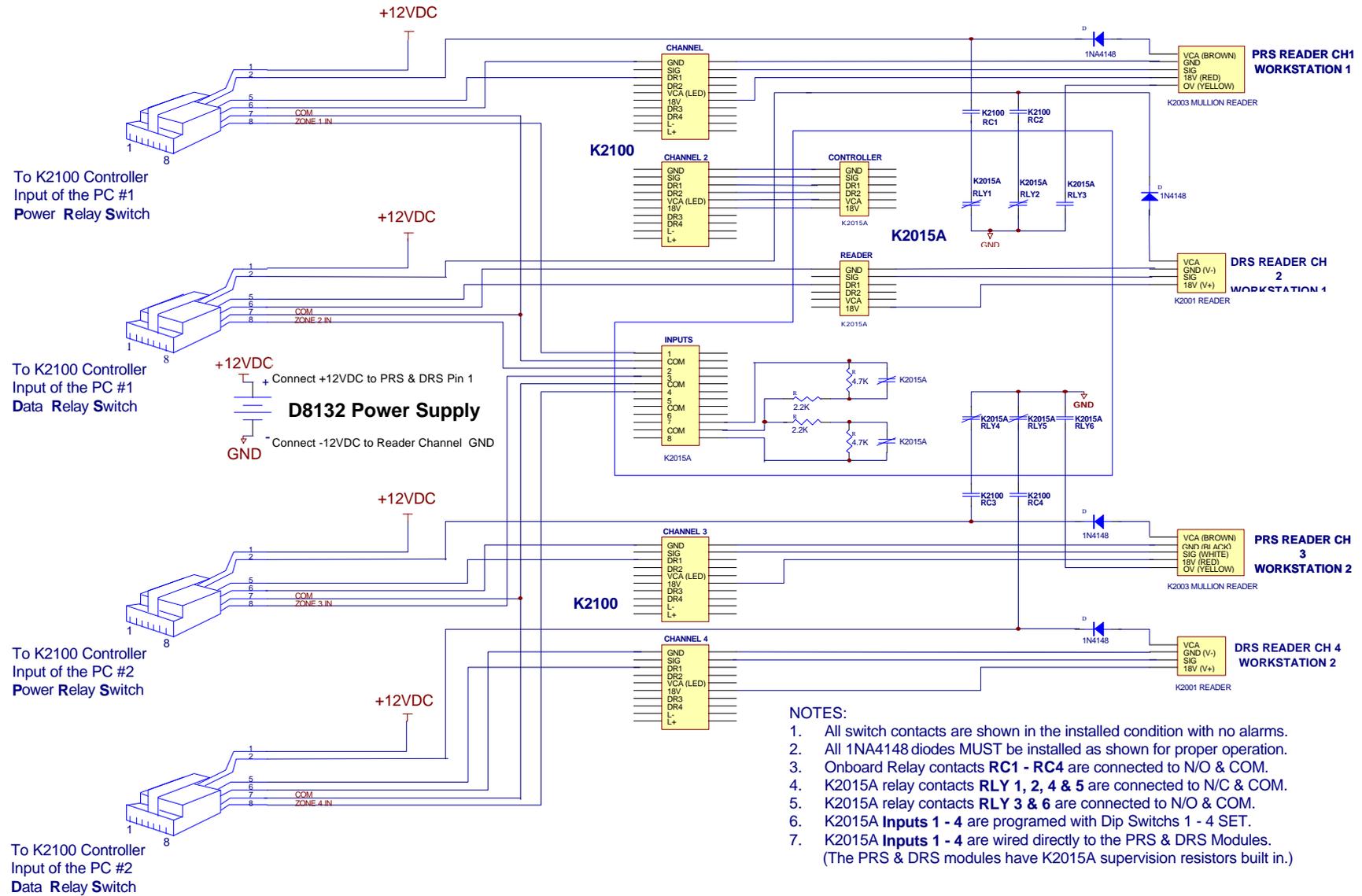


DIAGRAM 2

PRS MODULE



The PRS, DRS, and SPS Modules each have a RJ45 jack visible from the outside of the unit. This is the Readykey Control Input that interfaces the Readykey K2100 / K1100 Controller to the PRS, DRS, and SPS Modules. **DIAGRAM 1** of this Manual illustrates wiring details.

DRS MODULE

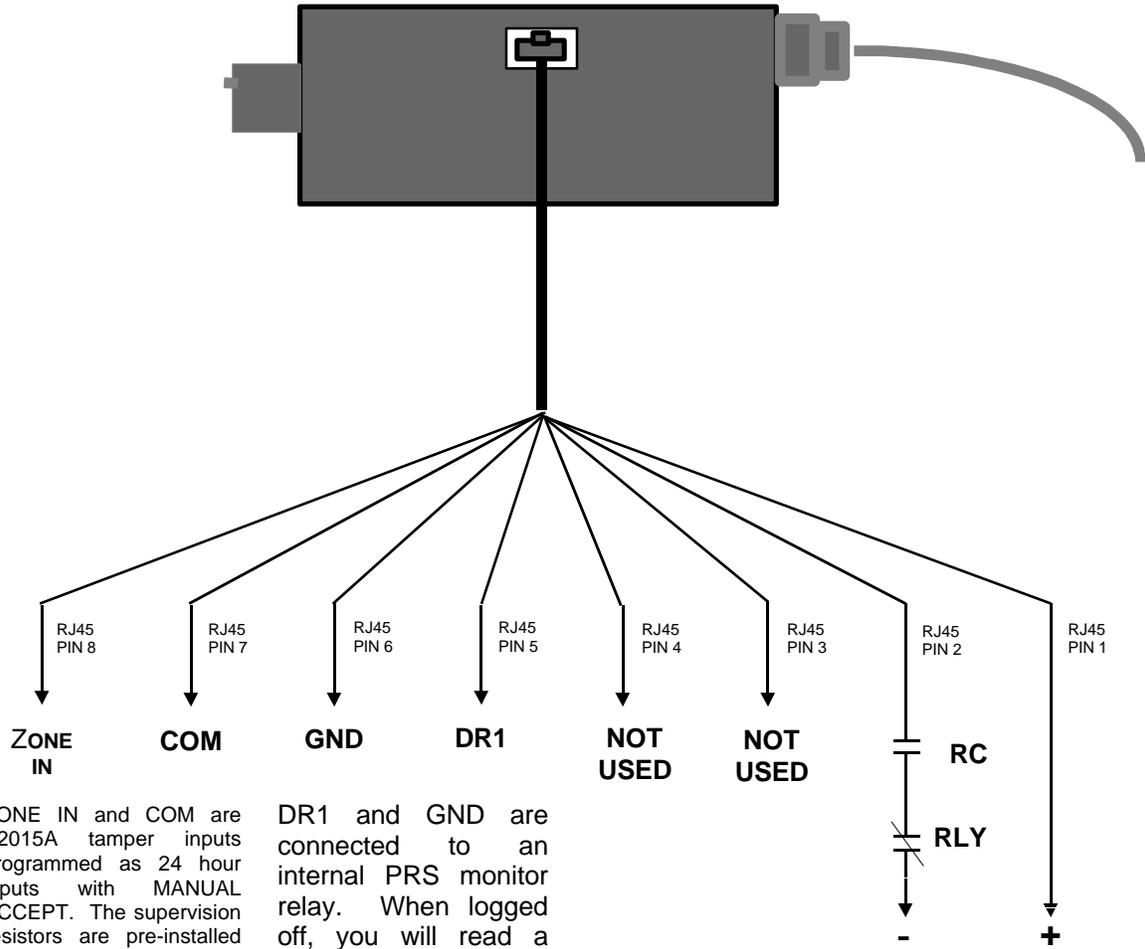


SPS MODULE



APPENDIX I

POWER RELAY SWITCH – CONTROLLER CONNECTIONS



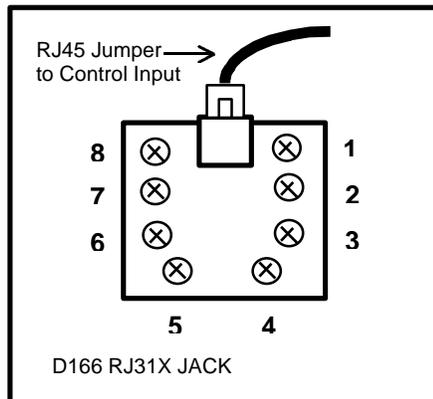
ZONE IN and COM are K2015A tamper inputs programmed as 24 hour inputs with MANUAL ACCEPT. The supervision resistors are pre-installed into the PRS. When all internal tamper contacts are in the installed condition with no alarms, you will read *2.2K ohms. If a tamper condition occurs in the PRS, you will read 6.9K ohms.

*For 2.2K ohms as normal loop condition, you will need to switch the dip switch corresponding to the zone input in the K2015A towards the inside or (OFF) position.

DR1 and GND are connected to an internal PRS monitor relay. When logged off, you will read a short. When logging on with an ACCESS AUTHORIZED event, the monitor relay will open, causing a DOOR LEFT OPEN event.

12VDC POWER SUPPLY

Pins 1 & 2 is the PRS control input. The presence of 12VDC will engage AC power to the PC. The RC contact is typically an onboard relay output programmed for a SET/RESET action from an ACCESS AUTHORIZED event from the PRS reader. The RC contact closes to energize the internal PRS relays. The RLY contact is typically a K2015A relay output that is programmed to open on PRS tamper activation. The tamper inputs are programmed to stay latched, disabling the PRS, until the tamper alarm is manually accepted by the administrator.



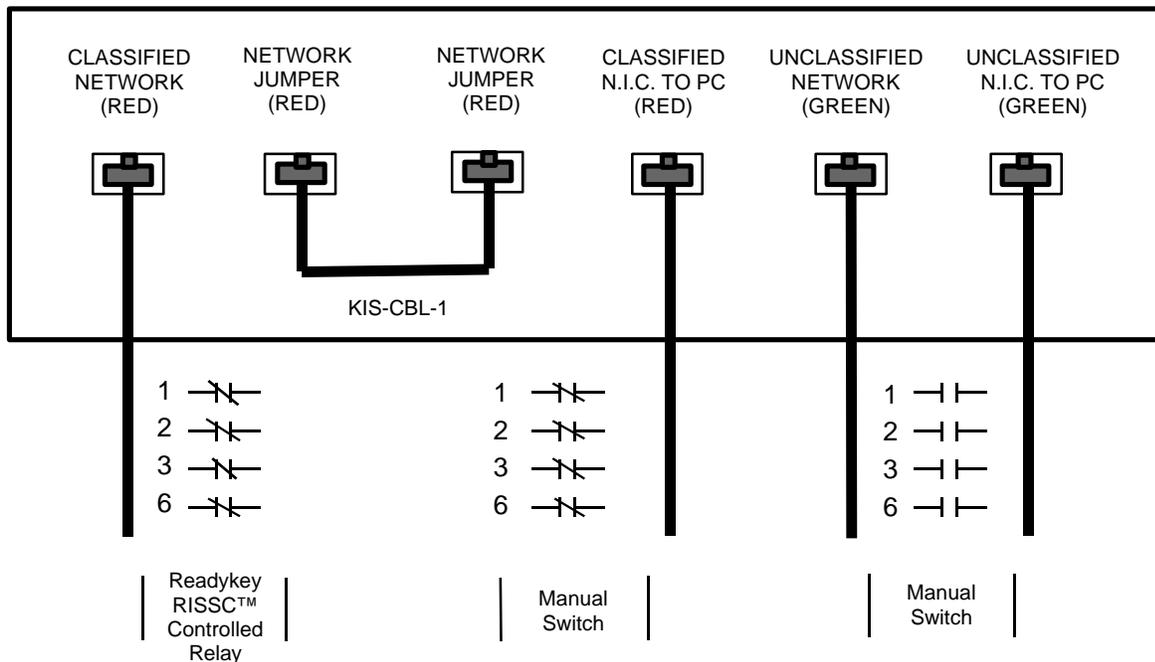
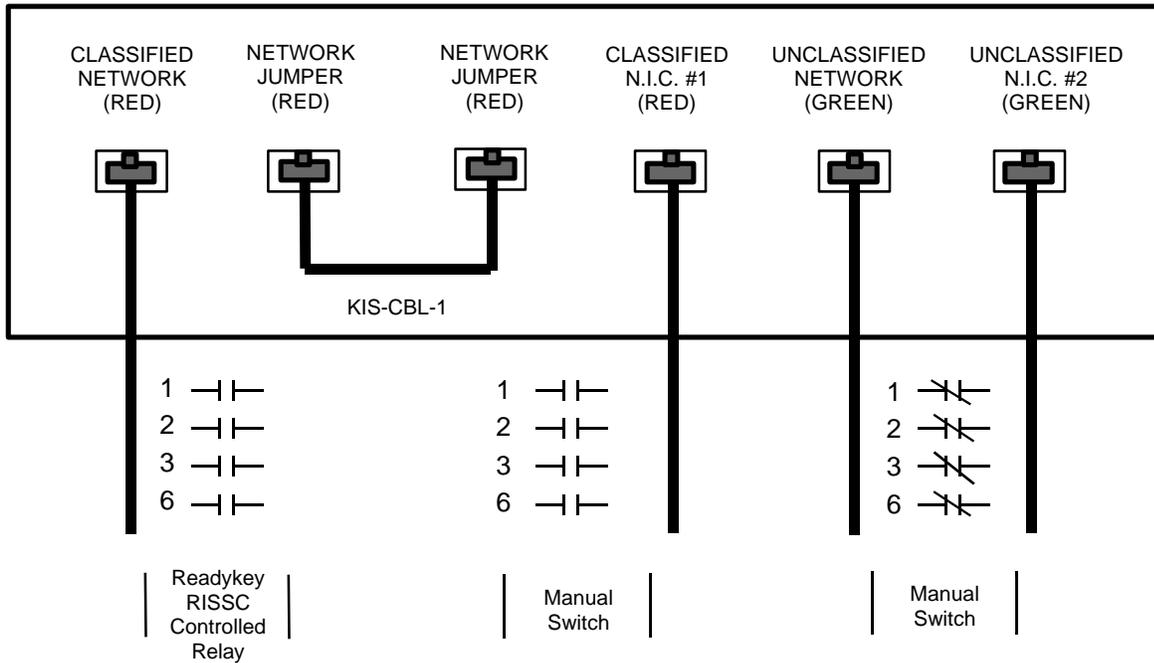
APPENDIX II

DATA RELAY SWITCH - NETWORK CONNECTIONS FOR RISSC™ CONFIGURATION

This configuration will require 2 (N.I.C.) Network Interface Cards in the PC.

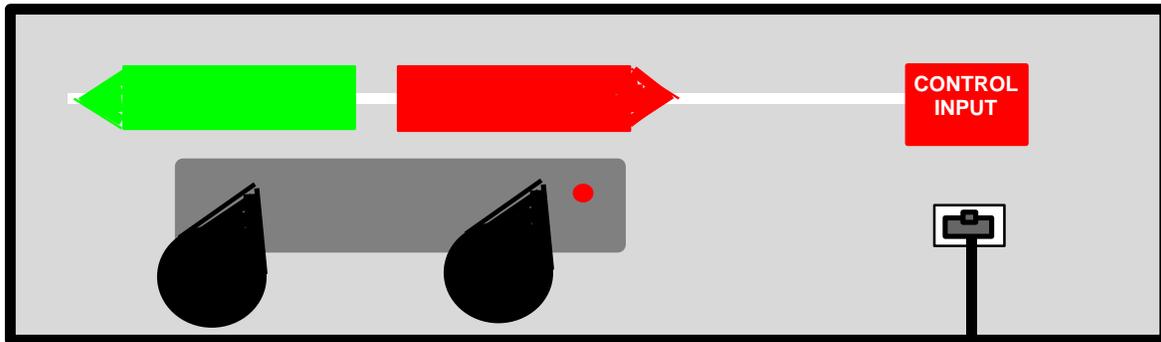
The **top drawing** shows network switch connections when the DRS manual switch is selected to GREEN position and the RISSC™ system is logged out.

The **bottom drawing** shows network switch connections when the DRS manual switch is selected to RED position and the RISSC™ system is logged in.

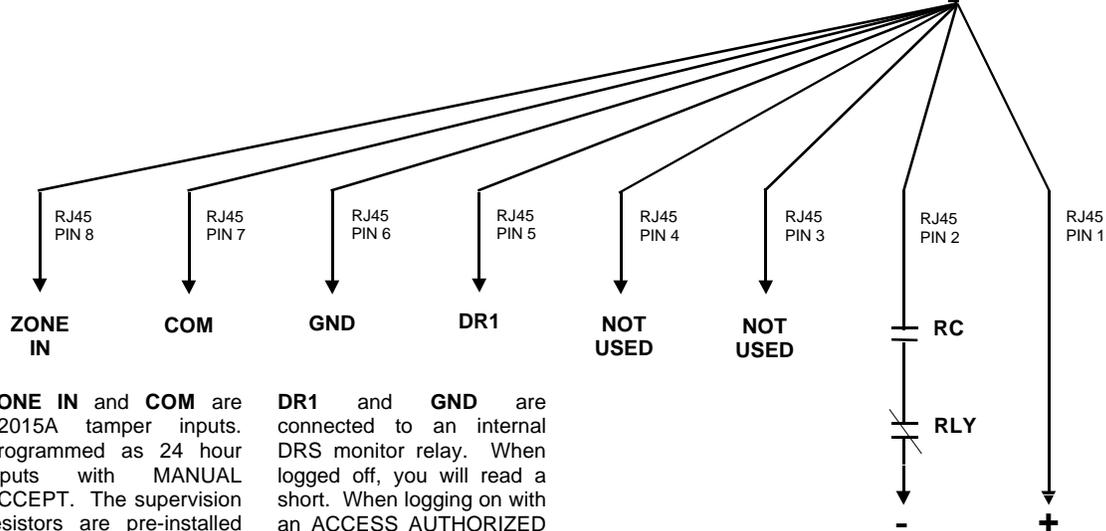


APPENDIX III

DATA RELAY SWITCH - FACEPLATE AND CONTROLLER CONNECTIONS



MANUAL SWITCH SHOWN IN THE CLASSIFIED POSITION

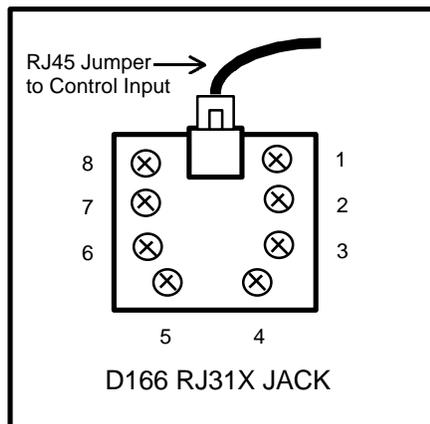


ZONE IN and **COM** are K2015A tamper inputs. Programmed as 24 hour inputs with MANUAL ACCEPT. The supervision resistors are pre-installed into the DRS. When all internal tamper contacts are in the installed condition with no alarms, you will read *2.2K ohms. If a tamper condition occurs in the DRS, you will read 6.9K ohms.
 *For 2.2K ohms as normal loop condition, you will need to switch the dip switch corresponding to the zone input in the K2015A towards the inside or (OFF) position.

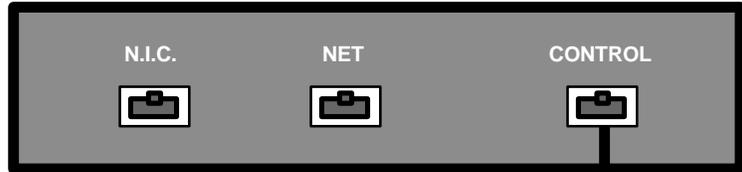
DR1 and **GND** are connected to an internal DRS monitor relay. When logged off, you will read a short. When logging on with an ACCESS AUTHORIZED event, the monitor relay will open, causing a DOOR LEFT OPEN event.

12VDC POWER SUPPLY

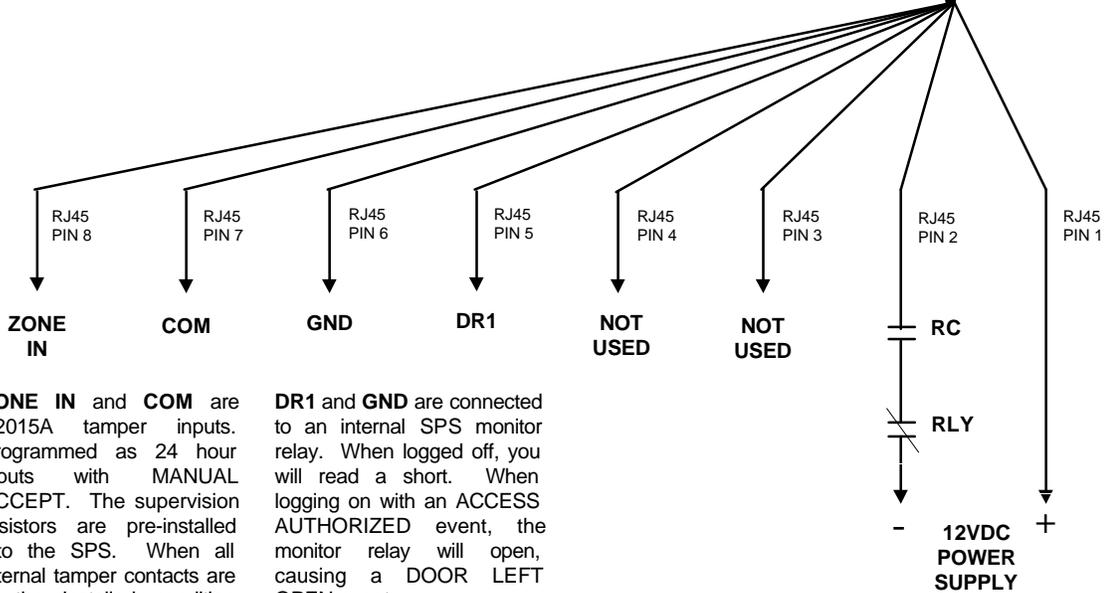
Pins 1 & 2 is the DRS control input. The presence of 12VDC will engage the network connection. The **RC** contact is typically an onboard relay output programmed for a SET/RESET action from an ACCESS AUTHORIZED event from the DRS reader. The **RC** contact closes to energize the internal DRS relays. The **RLY** contact is typically a K2015A relay output that is programmed to open on DRS or PRS tamper activation. The K2015A tamper inputs are programmed to stay latched, disabling the DRS, until the tamper alarm is manually accepted by the administrator.



SINGLE PROTECTION SWITCH - FACEPLATE AND CONTROLLER CONNECTIONS



NOTE: The N.I.C. (Network Interface Card) and NET (Network Source) connections are **not** protected physically like the DRS connections are. It is recommended that the SPS be installed in a protected area.

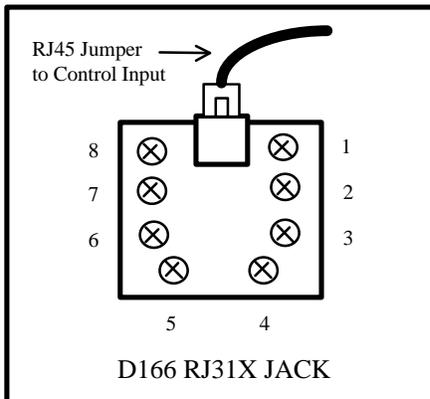


ZONE IN and **COM** are K2015A tamper inputs. Programmed as 24 hour inputs with MANUAL ACCEPT. The supervision resistors are pre-installed into the SPS. When all internal tamper contacts are in the installed condition with no alarms, you will read *2.2K ohms. If a tamper condition occurs in the SPS, you will read 6.9K ohms.

DR1 and **GND** are connected to an internal SPS monitor relay. When logged off, you will read a short. When logging on with an ACCESS AUTHORIZED event, the monitor relay will open, causing a DOOR LEFT OPEN event.

Pins 1 & 2 is the SPS control input. The presence of 12VDC will engage the network connection. The **RC** contact is typically an onboard relay output programmed for a SET/RESET action from an ACCESS AUTHORIZED event from the SPS reader. The **RC** contact closes to energize the internal SPS relays. The **RLY** contact is typically a K2015A relay output that is programmed to open on DRS, SPS or PRS tamper activations. The K2015A tamper inputs are programmed to stay latched, disabling the SPS, until the tamper alarm is manually accepted by the administrator.

*For 2.2K ohms as normal loop condition, you will need to switch the dip switch corresponding to the zone input in the K2015A towards the inside or (OFF) position.



D166 RJ31X JACK