PAC8000
8851-LC-MT
SafetyNet Logic Controller

GFK-2569B
December 2010

The 8851-LC-MT PAC8000 SafetyNet Logic Controller is used for logic control applications in an SIL2 environment. It provides:

- Subset of IEC 61131-3 languages
- Redundancy with bumpless transfer for higher availability
- Dual-redundant high-speed Ethernet connections
- Peer to peer communications between controllers
- On-line configuration

Product Documentation

PAC8000 Safety Manual 3.3

8000 System Specification Data Sheet

PAC8000 SafetyNet Data Sheet

8000 I/O – 2/2 I/O Modules, General Purpose and 2/2 Applications Including SafetyNet, Instruction Manual - INM8100

8000 I/O – 2x I/O Modules (2/1 applications) Instruction Manual – INM8200

System Specifier's Guide – SSG8002

Product documentation can be downloaded from www.ge-ip.com/support

Release Information

PAC8000 8851 firmware release 1.26 for PAC8000 8851-LC-MT SafetyNet Controller adds the following features:

- Update for Modbus read load balancing
- Update for the Register Protection Table

For details, see "Problems Resolved by Release 1.26" on page 2.

Updates

Existing versions of the 8851-LC-MT Controller can be upgraded to version 1.26 using upgrade kit 82A1744-MS10-000-A0.

Upgrade kits can be downloaded from the Support website, www.ge-ip.com/support.

The upgrade kit is published as a SIM for the PAC8000 Workbench programming package. After installing the SIM, firmware upgrades can be done through the Firmware Downloader utility launched from PAC8000 Workbench from PAC8000 SafetyNet controllers.

Compatibility

This release replaces all previous versions of the 8851-LC-MT Controller firmware.

Subject	Description
PAC8000 Workbench Version Requirements	To support all features of 01.26, Workbench 8.3.0 SP1 or later is required.
Upgrading From Previous Firmware Versions	Version 1.x PAC8000 SafetyNet controllers can be upgraded to release 1.26.
Downgrade To Previous Firmware Versions	Downgrading from release 1.26 to previous releases of 1.x is supported for PAC8000 SafetyNet controllers.

Problems Resolved by Release 1.26

Subject	Configuration	Description
A Clean Flash command cleared only the Master	Duplex	A Clean Flash command was processed only by the master controller. This had no impact on operation.
Modbus read load balancing on Duplex SafetyNet	Duplex	In previous releases, large numbers of Modbus reads could cause the master to abort or the standby to refresh in duplex systems. This could exhibit in multiple ways: ▪ The master would abort and record an “Abort by other processor” log event. The standby would record an “Abort master, rendezvous timeout xx ms at <xxxxxx>” event. ▪ The master would record multiple Inter AXE Link Events such as “IAL incomplete Rx standby diag [3] size 2 bytes” and “Inter AXE Link failed: retries Tx 0, Rx 1”. Finally a “Force standby, Inter AXE Link failed” event would be recorded and the standby would refresh. ▪ The master would record a “Forced other, railbus mismatch” event and the standby would refresh. This issue is corrected in this release.
Handling of differences between RTC and CPU date/time	Simplex, Duplex	In previous releases under heavy communication load or, rarely under normal load, a controller could abort with a log event indicating “TmrPIT FIT Interrupt rate.” This was due to an incorrect diagnostic check in the controller and has now been corrected.
RTOS did not manage the rollover of time-slice up-counter correctly	Simplex, Duplex	In previous releases a rollover of an internal clock could result in a controller aborting. The event log would indicate, “Abort due to SpvTaskTimeout” for either a UDP or TCP task. The clock rollover occurs at approximately 13 months from the last reset or power cycle.
Strategy download caused Task Timeout		Projects containing Safe ISaGRAF strategies and with several thousand tags mapped into the Discrete Control Interface were failing during the Strategy download due to task timeouts. The building of the Register Protection Table (RPT) was changed to better handle these projects. The following error message appeared in the controller event log: “Abort due to SpvTaskTimeout”
ISaGRAF debugger sometimes failed to start correctly	Simplex, Duplex	The ISaGRAF debugger did not reliably connect to the controller. In these cases, no log message was generated in the controller log, and the ISaGRAF debugger indicated a failure or a connection was not obtained.

Restrictions and Open Issues

Subject	*Configuration*	*Description*
8811 Module driver	Simplex, Duplex	For channels configured to output single pulses, multiple output pulses can be seen if the pulse length is set below the time of the execution cycle of the controller. RECOVERY: None. The pulse duration should normally be substantially longer than the execution cycle. A technical note that recommends appropriate values is available on the Support website, www.ge-ip.com/support.
SpvTaskTimeout during sporadic Peer to Peer communications	Duplex	The SpvTask Timeout may occur on a duplex controller with peer-to-peer communications starting and stopping, and while creating ISaGRAF TCP socket after firmware download and clean flash. The controller event log may contain errors such as the following: 00349 0000464.329 00 B ! !Abort due to SpvTaskTimeout task !EXEC 0x27 RECOVERY: Controller returns to healthy master after the reset due to the abort.
Debugger locking up	Simplex, Duplex	The ISaGRAF debugger locks up under certain conditions. To avoid this problem, only use the ISaGRAF debugger in Config mode. Stop the ISaGRAF debugger when going to Safe mode and do not attempt a connection while the controller is in safe mode. RECOVERY: Power cycle the controller(s).
Controller aborts during Register Mapping Table download	Simplex, Duplex	While downloading the Register Mapping Table or the Reg Init Values, the controller aborts with message: "Abort due to RtosAlloc NU_Allocate_Memory NU_INVALID_MEMORY" RECOVERY: Controller successfully resets after the abort and returns to healthy master or request standby depending on its partner controller's state.
Downloaded rejected with a CSC_CORRUPT error on peer to peer table	Simplex, Duplex	Strategy download may be abandoned while downloading the Peer-to-Peer Table with both master and standby offline. PAC8000 Workbench logs the following error in the Microsoft Event Log: "Download Failure: Request to AXE timed out - Download failed for the following reason: Load RIT: CRC does not match". The controller log also contains the message "Download Peer to Peer Table CSC_CORRUPT." RECOVERY: Re-download the strategy

Subject	Configuration	Description
Invalid data when using packed discrete points in Modbus master	Simplex, Duplex	When the PAC8000 controller is used as a Modbus Master and an option other than “No Packing” is selected from the WorkBench, the controller could return erroneous Modbus values to the slave. The issue occurs only for discrete Modbus registers. This issue occurs on the standard controller with firmware v2.x, RTU with firmware v2.11, and safety controller with firmware 1.1x and above. RECOVERY: To avoid this issue select the “No Packing” option on the “Map Remote Device Points” dialog in the WorkBench. This would ensure that the issue is not encountered. For complete information on this issue refer to Field Service Bulletin 100929.
Insertion of standby controller causes master abort	Duplex	On rare occasions, inserting an unpowered standby controller into a carrier with an operating master may cause the master to abort and go into failsafe. If this occurs, the master will record an "Abort due to SpvTaskTimeout task" in the event log. RECOVERY: If this occurs, power cycle the controller to cause the master to exit failsafe and resume normal operation. The master can also be commanded to exit failsafe via software tools such as the IO or Network Configurator. After the master is healthy, power can be applied to the standby controller.
Removing power to one controller may cause the second controller to abort	Duplex	On rare occasions, in duplex systems removing power to either the master or standby controller may cause the master to abort and go into failsafe. If this occurs, the controller in failsafe will record an “Abort due to PiReadStateFlags Unstable” in the event log. This issue occurs on units with a date code of 11/3/10 or later. RECOVERY: If this occurs, power cycle the controller to cause the master to exit failsafe and resume normal operation. The master can also be commanded to exit failsafe via software tools such as the IO or Network Configurator. .

Operational Notes

Subject	*Configuration*	*Description*
Abort after strategy download	Simplex, Duplex	Abort due to SpvTaskTimeout task may occur after strategy download of a project with a long execution cycle time. The controller event log may contain errors such as the following: 01835 0000507.070 00 B !08:14:53 ~~~~~~ 01836 0000507.070 00 B ! !Abort due to SpvTaskTimeout task !EXEC 0x27 01837 0000507.070 00 B !08:14:53 ~~~~~~ 01838 0000507.070 00 B ! Exec: 1st control package HISR SYSTEM H 01839 0000507.070 00 B ! Active Task !EXEC RECOVERY: Download a new strategy with shorter execution cycle time.

Compliance Information

For detailed installation and operating procedures, refer to the user manual for the module.

Hazardous Locations

- Factory Mutual, Class 1, Div 2, Groups A, B, C, D hazardous locations with Temperature Code T4
  Refer to Control Drawings SCI-701 and SCI-1004 for the PAC8000 8811-IO-DC module.
  Refer to Control Drawings SCI-701 and SCI-956 for the PAC8000 8851 Controller
- ATEX II 3 G, Ex nA nL IIC T4 for the PAC8000 8811-IO-DC module
  ATEX II 3 G, Ex nL IIC T4 for the PAC8000 8851 Controller
- CSA, Class 1, Div 2, Groups A, B, C, D hazardous locations with Temperature Code T4
  Refer to Control Drawings SCI-702 and SCI-1005 for the PAC8000 8811-IO-DC module.
  Refer to Control Drawings SCI-702 and SCI-957 for the PAC8000 8851 Controller

Functional Safety

- TUV Rheinland Safety Related Programmable Electronic System – suitable for safety related applications up to SIL 2.

Applicable Standards

- FM Approvals: *FM 3600, FM 3611, FM 3810*
- ATEX Approvals: *EN 60079-15:2005*
- CSA Approvals: *C22.2 No. 0-M91, C22.2 No. 142-M1987, C22.2 No. 213-M1987*
- TUV Rheinland: *IEC 61508, IEC 61511, EN 50156-1, NFPA 85, EN 61131-2, EN 61010-1, IEC 61326-1, EN 54-2, NFPA 72*