Microsoft Windows 10 IOT Enterprise

Syslogic User's Manual

Document Order code: DOC/W10ELTSB16E-8A-32

Revision	Datum	Author	Modification
1.0	16.11.2016	SM	First Release
1.1	25.11.2016	SM	Added Note chapter 3.5.1: UWF and Antivirus software

⬖ **syslog**ic

Content

General Remarks

The content and presentation of this document has been carefully checked. No responsibility is accepted for any errors or omissions in the documentation. Note that the documentation for the products is constantly revised and improved. The right to change this documentation at any time without notice is therefore reserved.

Syslogic is grateful for any help referring to errors or for suggestions for improvements.

The following registered trademarks are used:

Windows 10,	trademark of Microsoft Corporation
Windows Embedded Standard 7	trademark of Microsoft Corporation
Windows 10 IOT Enterprise	trademark of Microsoft Corporation
IPC/COMPACT	trademark of Syslogic Datentechnik AG
WinIO	trademark of Yariv Kaplan

Licensing information

This product is licensed by the Microsoft License Terms that can be found on the following page:
https://www.microsoft.com/en-us/Useterms/OEM/Windows/10/UseTerms_OEM_Windows_10_English.htm
By using the Software, you agree to all the terms of the License Agreement. Especially mentioned that the Software is bound to one device with a valid Entry EPKEA License. The same license counts for delivered recovery medias, which you are only allowed to use with a licensed device.
The Software "PCAN-View" by PEAK-system and the drivers for the PEAK-system Hardware preinstalled on the system are only allowed to be used with PEAK-system Hardware. If the system has no PEAK Hardware, the usage of these software is prohibited.

Safety Recommendations and Warnings

The product is intended for measurement, control and communications applications in industrial environment. The products must be installed by specially trained people. The strict observation of the installation guideline is mandatory.

The use of the product in systems in which life or health of persons is directly dependent (e.g. life support systems, patient monitoring systems, etc.) is not allowed.

1 Introduction

Windows 10 IOT Enterprise LTSB 2016 is based on Windows 10. In fact, both Operating Systems are based on the same binaries.

Windows 10 IOT Enterprise LTSB 2016 is enhanced with special tools to target the needs of embedded systems that run continuously. While a desktop OS like Windows 10 is optimized for maximum user interaction, an embedded OS is the opposite. Embedded systems often run in environments where few user interactions are desired. Embedded systems often supervise safety critical facilities and thus need to be very robust, reliable and autonomous.

This user manual covers some tools and techniques that help to reduce possible software and hardware breakdowns concerning the operation of Windows 10 IOT Enterprise LTSB 2016 on an IPC in an industrial environment. It details some embedded features that can be configured. Basic knowledge of Windows operating systems is required.

For detailed information refer to Microsoft documentation of Windows 10 IOT Enterprise.

https://www.microsoft.com/en-us/WindowsForBusiness/windows-iot

1.1. Supported Hardware

This release of Windows 10 IOT Enterprise LTSB 2016 supports the following systems from Syslogic:

Syslogic products	Product features
COMPACT8	Syslogic Industrial Computer Series 8
PROTOUCH-8	Syslogic Projected Capacitive Display Series 8

Table 1 – Supported Hardware

1.2. Notation within this document

Keys to buttons to be selected are noted with square bracket.

[ctrl]   Press CTRL key

Commands to be entered somewhere are noted as followed:

dir   Enter "dir" to the command shell

Input to be replaced by the user is noted with square brackets:

[name]   Enter your name instead of "[name]"

2 Getting Started

This chapter will give you a "quick start" on how to get Windows 10 IOT Enterprise running on an Intel Atom based system from Syslogic. The same procedure applies for all Systems.

2.1. Booting Windows 10 IOT Enterprise

If you do not have a CompactFlash card with a fully installed Windows 10 IOT Enterprise image, please read chapter 0 on how to install the system files.

Open the service cover of your industrial PC (IPC) and plug the flash card into the corresponding socket. Close the IPC and connect a USB keyboard, mouse and a monitor. Power the device and Windows 10 IOT Enterprise should start loading. If the device doesn't boot from the drive inserted press [DEL] while the BIOS is starting to select the correct drive or change the BIOS setting to boot from the flash.

2.2. User and Password Settings

The Syslogic Windows 10 IOT Enterprise image is configured for auto logon, i.e. if the system starts, the default user "Admin" is automatically logged on.

Default User:

W10IOTE auto logon User:	Admin
W10IOTE auto logon Password:	netipc
W10IOTE auto logon Group:	Administrators

Backup User:

Do not use this user profile for daily use.

W10IOTE backup User:	Administrator
W10IOTE backup Password:	netipc
W10IOTE backup Group:	Administrator

By default, the user Administrator is disabled. To enable this user run the following command with elevated privileges: **net user Administrator /enable:yes**

Refer to 3.8.1 to change the Auto Login User.

2.3. Desktop

On the desktop, the following items can be found:

Disable UWF on and commits changes to drive C:\. A reboot is required

Enables UWF on drive C:\. A reboot is required.

Shows the status of the UWF.

Starts Sysprep. Refer to chapter 4.2.

3 Windows 10 IOT Enterprise Features

The software included in our Windows 10 IOT Enterprise LTSB 2016 image is based on Windows 10 LTSB 2016. This long-term servicing branch (LTSB) of Windows 10 does not include all features included in the current branch (CB). LTSB images will not contain most in-box Universal Windows Apps (for example, Microsoft Edge, Cortana, the Windows Store, the Mail and Calendar apps) because the apps or the services that they use will be frequently updated with new functionality and therefore cannot be supported on PCs running the LTSB OS.

Windows 10 IOT Enterprise LTSB installations fully support the Universal Windows Platform. For apps from other Independent Software Vendors (ISV) contact the ISV to confirm if they will provide long-term support for their specific apps.

For more information about the different servicing models please refer to:

https://technet.microsoft.com/itpro/windows/manage/introduction-to-windows-10-servicing

In compare to Windows Embedded Standard 7, Windows 10 IOT Enterprise is not a component reduced operating system. It contains all the components like the standard Windows 10 LTSB.

Because the current branch includes feature upgrades not available in the LTSB branch, an application might run well in the current branch but run into problems on Windows 10 IOT Enterprise LTSB 2016. In this case looking to the list of installed packages in each of the both branches will help to figure out the rule of the problem. Microsoft provides a tool to manage the package and modules included in a Windows 10 operating system. This tool is called DISM.

For more information about DISM please refer to:

http://msdn.microsoft.com/en-us/library/dd371719%28v=VS.85%29.aspx

Some helpful commands:

Add a package:	**dism /online /add-package /packagepath:[Path and Filename]** [Path and File] has to be replaced by a Path and filename of a cab file or a directory containing a cab file. Make sure all depending packages are already installed.
Remove a package:	**dism /online /remove-package /packagename:[name of the package]** A list of installed Packages is located in the UTILITIES/CURRENT_VERSION/Packages.txt. Replace [Name] by the full name of the package to the console including revision index.
Help adding drives:	**dism /online /add-driver /?**
Help removing drives	**dism /online /remove-driver /?**

3.1. Default Configuration

- Firewall: enabled
- Windows Defender: enabled
- Auto logon: enabled
- UWF: installed, disabled
- Languages: English language support
- DHCP: enabled
- Computer name: random
- Graphics driver: Intel ® HD Graphics

3.2.   Graphics Driver for COMPACT8 and PROTOUCH-8-Systems

Intel is modifying its graphic driver constantly. It's suggested to visit Intel's website from time to time for new driver versions.

Installed driver on the system is Intel HD Graphics Driver. To configure the driver, use the icon in the taskbar notification area.

3.2.1.   Backlight Control for Protouch-8 devices

The brightness of the displays can be controlled by the following options:

- Use slider located in control panel-> Power Options.

- Right Click on Desktop-> Display settings: Use slider Adjust brightness level

- Use standard Windows API for controlling backlight. There are several examples available on the web. A good example can be found here:

  http://www.codeproject.com/Articles/236898/Screen-Brightness-Control-for-Laptops-and-Tablets

3.3.   Ethernet Driver for COMPACT8 and PROTOUCH-8-Systems

Intel is modifying its network drivers regularly, therefore it is suggested to visit Intel's website from time to time for new driver versions.

3.4.   Security

To get a secure system it is required to configure the features provided properly. Main security features are a working firewall and antivirus software.

3.4.1.   Windows Firewall

Windows firewall is installed and activated by default. Two modifications have been made to speed up system development.

- Allow Ping   The system responds to ping commands from outside.
- Enable Remote Desktop   It is possible to connect to the device by remote desktop.

3.4.2.   Antivirus software

Antivirus software is always an important subject of any Windows system. This is valid for Windows 10 IOT Enterprise as well.

Windows 10 IOT Enterprise is protected by Microsoft Windows Defender.

When enabling the Unified Write Filter (UWF) it is recommended to find solutions for the following issues:

- Typically, antivirus software uses a daily growing database of virus definitions. Any change written to the file system may be forwarded to RAM by the write filter. Is there enough RAM available?
- Embedded systems typically get quite old. How long will it be possible to get new virus definitions without any upgrade of the installed antivirus software? Who will upgrade the software if required?
- Rebooting the system with the virus definition stored in RAM only, will end in losing the definition and requires downloading the virus definitions again.

If not using antivirus software, make sure that the system remains safe and free of any unwanted modifications. Some important points are:

- Use a user with no elevated privileges as a default user.
- Prevent user from surfing the Web or receiving emails on the embedded System.
- Do not start not required services.
- Use write-filters as UWF.
- Use keyboard-filter
- Check group policy to further lock down the system
- Do not allow running any code from a device (any USB drives or similar) connected to the system or already installed software on the system using AppLocker.
- Do not allow any unwanted connection by any communication protocol (network vulnerability…) using firewall.
- If possible, reboot the system regularly to reset unwanted changes.
- Allow code running only from known folders or if they are signed.
- Sign update packages, allow only installing signed updates.

3.5. Reliability

Windows 10 IOT Enterprise gives some features to improve the reliability of the system. These features are the Unified Write Filter (UWF), Shell Launcher, Keyboard Filter and Assigned Access. An Overview of the different features can be found at

https://technet.microsoft.com/en-us/itpro/windows/manage/lockdown-features-windows-10

From this webpage, it is possible to find further descriptions for each feature mentioned and examples how to configure them.

Make sure the system is protected adequately. Especially if the system is connected to any network it is important to have a good concept. Use Anti-Virus and Firewall Software if required.

3.5.1. Unified Write Filter

UWF intercepts all write attempts to a protected volume and redirects those write attempts to a virtual overlay. This improves the reliability and stability of your device and reduces the wear on write-sensitive media, such as flash memory media like solid-state drives.

For more information about the Unified Write Filter, refer to:

https://msdn.microsoft.com/en-us/library/windows/hardware/mt572001(v=vs.85).aspx

All configuration settings for UWF are stored in the registry. UWF automatically excludes these registry entries from filtering. To configure Unified Write Filter, use the command line tool uwfmgr.exe. For more information about the command line tool for configuring UWF, see the example or the page

https://msdn.microsoft.com/en-us/library/windows/hardware/mt572002(v=vs.85).aspx

Example:

uwfmgr volume protect C:	to protect volume c:
uwfmgr file add-exclusion C:\Users\Admin\Documents	Add files or directories as exclusions. The file / or files in this directory will not get deleted when the system reboots
uwfmgr get-config	shows the configuration of the UWF
uwfmgr help	shows how to use the command line tool

A description how to apply Windows updates to UWF-protected devices can be found on the following page:

https://msdn.microsoft.com/en-us/library/windows/hardware/mt571988(v=vs.85).aspx

It is important, to regularly update UWF-protected devices if possible, to make sure, that the system has the last critical, security and driver updates installed.

Issues when using Antivirus-Software with enabled UWF

When enabling the UWF on a drive and the Antivirus-Software is installed on this drive and enabled, the RAM can run out of memory as the growing database of the Software fills it. The system would freeze after some time. Therefore, the Antivirus-Software should be disabled (refer to chapter 3.4.2) or the folders and files belonging to the Software should be excluded by the UWF.

3.5.2. Shell Launcher

Shell Launcher may replace the default Windows 10 shell with a custom shell. You can use any application or executable as your custom shell, such as a command window or a custom dedicated application. It is also possible to select a different shell for different users or different user groups.

Note that you cannot use Shell Launcher to launch a Universal Windows app as a custom shell. To run a Universal Windows app please refer to 3.4.4.

For more information about the Shell Launcher please refer to:

https://msdn.microsoft.com/en-us/library/windows/hardware/mt571994(v=vs.85).aspx

To configure the Shell Launcher, useful examples can be found on the same webpage.

3.5.3. Keyboard Filter

You can use Keyboard Filter to suppress undesirable key presses or key combinations. Normally, a customer can use certain Microsoft Windows key combinations like Ctrl+Alt+Delete or Ctrl+Shift+Tab to alter the operation of a device by locking the screen or using Task Manager to close a running application. This may not be desirable if your device is intended for a dedicated purpose.

The Keyboard Filter feature works with physical keyboards, the Windows on-screen keyboard, and the touch keyboard. Keyboard Filter also detects dynamic layout changes, such as switching from one language set to another, and continues to suppress keys correctly, even if the location of suppressed keys has changed on the keyboard layout.

For more information about the Keyboard Filter please refer to:

https://msdn.microsoft.com/en-us/library/windows/hardware/mt587088(v=vs.85).aspx

3.5.4. Assigned Access

You can use assigned access to set up single-function devices, such as restaurant menus or displays at trade shows. If an account is configured for assigned access, a Windows app of your choosing runs above the lockscreen for the selected user account. Users of that account cannot access any other functionality on the device.

For more information about the Assigned Access feature please refer to:

https://msdn.microsoft.com/en-us/library/windows/hardware/mt620040(v=vs.85).aspx

How to configure Assigned Access can be found here:

https://msdn.microsoft.com/en-us/library/windows/hardware/mt620043(v=vs.85).aspx

3.6. Audio Support

3.6.1. Audio Volume Control

Most of Syslogic Hardware does not support any audio outputs. Therefore, audio volume control is disabled in the taskbar notification area. If Audio Output is required connect a USB Audio device to the system and enable the audio volume control in the taskbar by right-click on the taskbar-> Settings-> Turn system icons on or off-> Volume to On.

3.7. Language Packages

By default, only English is installed as a platform and desktop language.

3.7.1. Selecting another Desktop Language

There are 2 ways to change the current language or install a new language.

In the start menu, the Settings application will open the new settings interface. Select "Time & language" and then "Region & language" to open the settings page for the language which allows to download new languages and selecting a new desktop language.

Also, using the control panel allows you to load new languages and selecting a new desktop language.

3.8. Tools

3.8.1. Set Auto Login

The command SetAutoLogin.exe in the System32 Folder allows you to select the user to logon at startup using the command line. The tool changes the settings in the registry and stores the password in a safe place (not visible in the registry).

Set Auto Login User: SetAutoLogin.exe [Username] [Password]

Example: SetAutoLogin.exe Admin netipc

3.9. Wake on LAN

Windows 10 Iot Enterprise and the Hardware support Wake on LAN. This means that it is possible to wake up the system from sleep by sending a Magic Paket to the MAC address of the corresponding ethernet interface. The MAC address can be found by using the command **ipconfig -all** and looking for the physical address of the device. To send magic packets, multiple different tools can be found free for downloading.

4 Installing Windows 10 IOT Enterprise

4.1. Overview

Windows 10 IOT Enterprise is delivered on your IPC or TFT if ordered. Please capture an image if desired using any third-party imaging tool.

4.2. Capturing a System Image

To capture an image of an actual system, insert the flash disk to the computer and use a byte or file image tool. Before capturing an image, it is important to run Sysprep. Using Sysprep before capturing the image will guarantee proper functionality of the UWF and other features. To execute Sysprep use the icon Sysprep available from the desktop.

> **Run Sysprep before capturing an image:**
>
> Disable Write Filter before running Sysprep!
>
> Run Sysprep before capturing an image of a Windows 10 IOT Enterprise image.
> Do not restart the image before capturing the image.

> **Run Sysprep before sending Image for production**
>
> Run Sysprep before sending an Image to Syslogic for production. If not executed, Syslogic will not be able to deploy the image correctly.

4.2.1. Capture Image

After Sysprep has been executed and the system has stopped, remove the flash drive from the target and capture an Image using either a File image or a Byte Image on any other personal computer.

4.2.2. Deploy an Image

The IPC/W10ELTSB16E-8A-xx provides one Byte Image of Windows 10 IOT Enterprise configured for COMPACT8 and PROTOUCH-8 located in the folder /IMAGE. Deploy the image using any byte image tool on a standard computer.

- Remove the flash from the target device and connect it to a personal computer.

- Extract the Image File located on IPC/W10ELTSB16E-8A in the folder IMAGE.

- Write the extracted image using a byte image tool to the drive.

- Now you can configure the partitions. Especially check if the whole size of the flash is used.

- Remount the flash to the target device.

5 Installing new Windows 10 or Windows 10 IOT Enterprise

Most system drivers are provided through Windows or can be downloaded from the manufacturer's web page. For details on Hardware refer to the corresponding manual.

Some drivers that are not provided automatically are located on IPC/W10ELTSB16E-A8-xx Memory drive in the folder DRIVERS. Keep in mind that drivers are updated and improved continuously. Therefore, check for the manufacturers web page for the newest revisions.

6   WinIo Driver Library

6.1.   WinIo Library Overview

WinIo is a driver that grants your application access to Windows XP/2000/NT/7 (only 32Bit) system resources that are normally not accessible. You can use WinIo to simply write a byte to the x86 IO port registers or access physical memory directly. WinIo is written and maintained by Yariv Kaplan (www.internals.com, see 6.5 for license details).

WinIo has the following function interface defined (listing not complete):

bool _stdcall InitializeWinIo()

> This function initializes the WinIo library

void _stdcall ShutdownWinIo()

> This function performs cleanup of the WinIo library.

bool _stdcall InstallWinIoDriver(PSTR pszWinIoDriverPath, bool IsDemandLoaded);

> This function installs the WinIo driver.

bool _stdcall RemoveWinIoDriver()

> This function removes the WinIo driver from the system.

bool _stdcall GetPortVal(WORD wPortAddr, PDWORD pdwPortVal, BYTE bSize);

> This function reads a BYTE/WORD/DWORD value from an I/O port.

bool _stdcall SetPortVal(WORD wPortAddr, DWORD dwPortVal, BYTE bSize);

> This function writes a BYTE/WORD/DWORD value to an I/O port.

6.2. NETIPC extensions to WINIO_V2

Syslogic has extended the original WinIo Library with some hardware-related functions. These extensions can be accessed like any other WinIo function after properly initializing the WinIo driver:

bool _stdcall GetTemp(float& value)

> This function returns the temperature from the on-board LM75 temperature sensor.

bool _stdcall WatchdogGetState(bool& Timeout)

> This function returns the state of the Watchdog. 1=Timeout occurred, 0=No Timeout

bool _stdcall WatchdogEnable()

> This function enables the watchdog. It will reset the board if not triggered by WatchdogTrigger.

bool _stdcall WatchdogTrigger()

> This function triggers the Watchdog.

bool _stdcall WatchdogHardReset()

> This function resets the watchdog by hard resetting the board.

bool _stdcall GetCpuFID(DWORD& FID)

bool _stdcall GetCpuOID(DWORD& OID)

bool _stdcall GetCpuRID(DWORD& RID)

> These functions return the board identifiers.

6.3. Using WinIo in a Visual C++ application

In order to use WinIo in a Visual C++ application, you should take the following steps (please also have a look at the the TestProg Sample Application found in the TestProg directory):

(1) Place winio.dll, winio.vxd and winio.sys in the directory where your application's executable file resides.

(2) Add winio.lib to your project file by right clicking on the project name in the Visual C++ workview pane and selecting "Add Files to Project...".

(3) Add the #include "winio.h" statement to your source file.

(4) Call InitializeWinIo.

(5) Call the library's functions to access I/O ports and physical memory.

(6) Call ShutdownWinIo.

6.4. TestProg Sample Application

The TestProg sample application demonstrates the use of the extended WinIo Library. After reading out the temperature and the board identifiers, it activates the watchdog and triggers it for about 10 seconds before letting the watchdog generate a timeout.

Copy the WINIO/Bin directory to the Windows WIN10ENT device and run TestProg.exe (WinIo.dll and WinIo.sys must be in the same directory as TestProg.exe).

6.5.   WinIO End User License Agreement

Software License Agreement for WinIo

The following terms apply to all files associated with the software unless explicitly disclaimed in individual files.

IMPORTANT- PLEASE READ CAREFULLY: BY INSTALLING THE SOFTWARE (AS DEFINED BELOW), OR COPYING THE SOFTWARE, YOU (EITHER ON BEHALF OF YOURSELF AS AN INDIVIDUAL OR ON BEHALF OF AN ENTITY AS ITS AUTHORIZED REPRESENTATIVE) AGREE TO ALL OF THE TERMS OF THIS END USER LICENSE AGREEMENT ("AGREEMENT") REGARDING YOUR USE OF THE SOFTWARE. IF YOU DO NOT AGREE WITH ALL OF THE TERMS OF THIS AGREEMENT, DO NOT INSTALL, COPY OR OTHERWISE USE THE SOFTWARE.

1. GRANT OF LICENSE: Subject to the terms below, Yariv Kaplan ("AUTHOR") hereby grants you a non-exclusive, non-transferable, non-assignable license to install and to use the downloadable version of WinIo ("SOFTWARE").

a. Redistributable Code. You may reproduce and distribute the object code form of the SOFTWARE solely in conjunction with, and as part of, your application ("Permitted Application"); provided that you comply with the following:

If you redistribute any portion of the Redistributable Code, you agree that: (i) you will only distribute the Redistributable Code in conjunction with, and as part of, your Permitted Application which adds significant functionality to the Redistributable Code and that distribution of the Permitted Application does not compete with the AUTHOR's distribution of the SOFTWARE; (ii) you will include a valid copyright notice on your Permitted Application; (iii) you will not permit further redistribution of the Redistributable Code; and (iv) you will indemnify, hold harmless, and defend the AUTHOR from and against any claims or lawsuits, including attorneys' fees, that arise or result from the use or distribution of your Permitted Application.

b. License to use Source Code. You may not sell, lease, rent, transfer or sublicense the source code of this SOFTWARE.

2. MODIFICATION: SOFTWARE Source Code may be modified without the prior written permission of the AUTHOR. Any modifications made to the SOFTWARE will continue to be subject to the terms and conditions of this AGREEMENT.

3. COPYRIGHT: All rights, title, and copyrights in and to the SOFTWARE and any copies of the SOFTWARE are owned by the AUTHOR. The SOFTWARE is protected by copyright laws and international treaty provisions. Therefore, you must treat the SOFTWARE like any other copyrighted material.

4. TITLE: You acknowledge that no title to the intellectual property in the SOFTWARE is transferred to you. Title, ownership, rights, and intellectual property rights in and to the SOFTWARE shall remain the exclusive property of the AUTHOR. The SOFTWARE is protected by copyright laws of the United States and international treaties.

5. LIMITATION OF LIABILITY: You must assume the entire risk of using the SOFTWARE.

IN NO EVENT SHALL THE AUTHOR BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY DERIVATIVES THEREOF, EVEN IF THE AUTHOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE AUTHOR SPECIFICALLY DISCLAIMS ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHOR HAS NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

References

- Microsoft Developer Network

  http://msdn.microsoft.com/en-us/library/ff795587%28v=WinEmbedded.0%29.aspx

- IPC/COMPACT8-SL user documentation

  (Document Order code: DOC/IPC_SL8-E), available at www.syslogic.com

- Microsoft Windows Sysinternals Tools & Website

  http://technet.microsoft.com/en-US/us-us/sysinternals/bb545021.aspx

7 Contact

Our distributors and system integrators will gladly give you any information about our products and their use. If you want to contact the manufacturer directly, please e-mail a message containing a short description of your application and your request or use one of our request forms on our homepage.

Syslogic Datentechnik AG

Switzerland

E-Mail:	Information	info@syslogic.com
	Technical support	support@syslogic.com
Webpage:		www.syslogic.com