White Paper

Customized Tools for Embedded Linux Applications

Executive Summary

This white paper will expound on customizable tools that can be added to create an optimized Linux solution for embedded platforms.

The use of App Launcher, Write Shield, Secure Boot, and Linux Backup and Recovery can be added to any system running Linux operating systems to enhance user convenience and address concerns regarding data backup, security and data protection.

Introduction

Linux operating systems (OS) are open source and free of use. This had led to an increase in use in the industrial embedded sector. The driving factor behind this is that proprietary operating systems, such as Windows, come with a significant added cost. However, although expensive, the proprietary operating systems mostly offer the needed applications and software to fit the system integrator's requirements. This is not necessarily true for Linux.

The availability of Linux applications is dependent on what the community has created and available solutions are often insufficient for embedded industrial use. This leaves it to the system integrator to create or modify software which can be both costly and time-consuming.

This paper will look at 4 key tools that can strengthen and enhance the use of Linux in the industrial embedded field:

1. App Launcher: a tool that covers all background windows and desktops, which is essential for digital signage, point-of-sale (PoS) and kiosk applications
2. Write Shield: a tool that provides partition protection through a RAM drive function, allowing the user to protect parts or all of the non-volatile storage
3. Secure Boot: this feature only allows OS startup after checking that the relevant hardware is present through a serial number check. If any of the hardware has been swapped, system startup will fail
4. Linux Backup and Recovery with iCover™: system backup and recovery in case of system crash or instability

Where relevant, the tools will be compared to similar Linux apps that are available.

Background

The first Linux OS kernel was launched in 1991 and since then, Linux has grown to be the dominant open-source operating system. More surprisingly, it is also the most commonly used operating system worldwide due to its kernel being used in Android operating system.

Linux is also found in industrial embedded systems where devices are simpler and the operating system usually performs fewer but more specialized tasks. These systems include everything from network routers, digital signage to factory automation and in-vehicle computers.

Challenges

Every industrial embedded application is faced with unique requirements and challenges. When opting for a Linux solution, finding the correct tools for your application can be difficult, often necessitating new software.

Thus the cost saved by using Linux will be offset by having to create or modify software. This again requires specific know-how and the operator might have to look outside the company for help, further increasing the associated cost.

Other than the cost side of implementing Linux systems, this paper will also address the following challenges:

- User convenience: Simplifying the user experience
- Data protection: Sectioning off and protecting essential data
- Data tampering: Ensuring that the storage device is in its assigned system before allowing access to data
- Data recovery: System recovery in case of a crash or other critical errors

Solutions

App Launcher

The App Launcher allows an image or app to run on top of the desktop as well as adjusting image size to the screen. It will cover the desktop and any messages that might pop up.

This is necessary for applications displaying ads, information kiosks, and PoS systems. Without App Launcher other apps or messages suddenly popping up can disrupt business and the problem can be hard to fix, especially for untrained personnel.

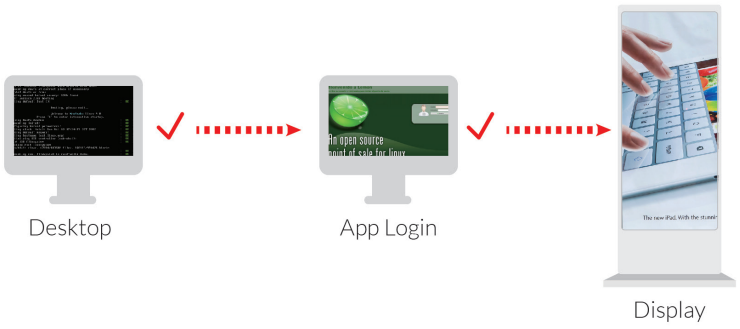


Figure 1: The desktop image on the right is covered with an app displaying ads

This function ensures that the system automatically opens the chosen app, simplifying the process and also allowing inexperienced users to run system startup.

Write Shield

Write Shield provides data protection through two processes:

1. RAM-level writing: Data that appears to be written to the disk is actually only written to RAM. This means that as soon as the computer shuts down, all data and changes disappears as RAM is volatile storage.
2. Partition and file protection: The data can be split into partitions (files) and protected. Any data deemed essential can thus be sectioned off and protected from any changes.

This form of data protection brings with it several benefits. Firstly, using RAM to store data means less wear on the SSD, which in turn increases device longevity. Secondly, viruses and other malicious code will be unable to access essential files. Thirdly, the human error factor is mitigated through all changes to the protected files being reversed after system restart. Furthermore, sudden power outages can cause critical errors and data loss. These errors can be rectified with a system restart.

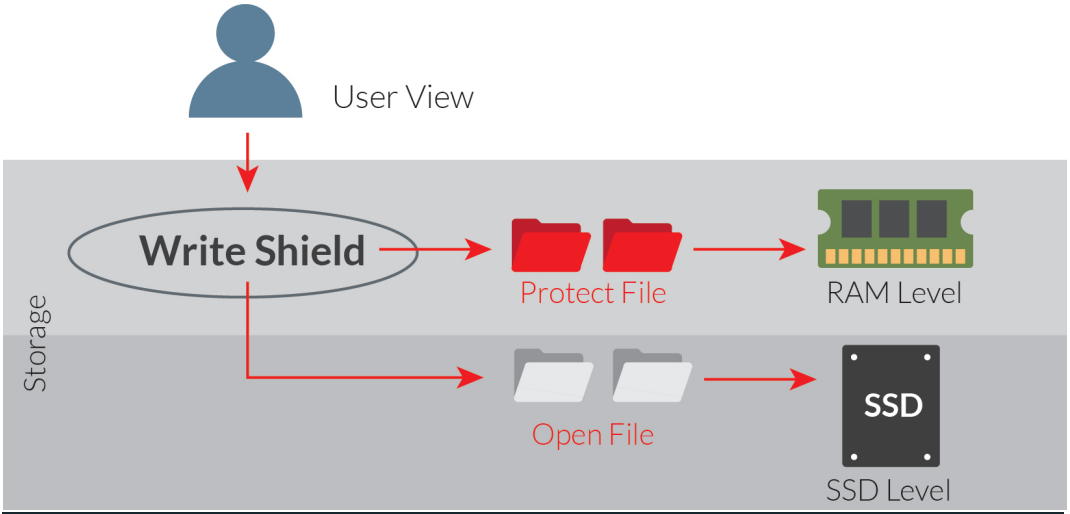


Figure 2: Write Shield uses RAM-level writing and partition (file) protection to safeguard essential data

Secure Boot

Secure boot is a safety measure that can check serial and model numbers of components, as well as checksums before allowing access to the SSD and starting up the Linux operating system.

For example (see figure 3), this is how secure boot could be run after turning on your device:

1. Power is turned on and the bootloader is initiated
2. The system will check any preset number to determine if it is the system and components in place as configured
3. Only when these numbers pass the check will the OS finally be initialized

If at any time any number or parameter is not met, the process is canceled and system initiation will fail. The parameters can be determined beforehand and more can be added to ensure sufficient security.

This measure is to prevent data from being compromised. If the SSD is removed from the original setup, the parameters will change and it will be impossible to access the data.

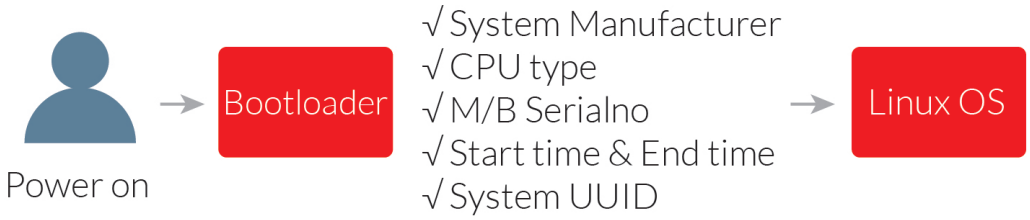


Figure 3: Flowchart showing an example of a secure boot process

This feature is aimed at industries such as casino gaming, PoS and networking where data falling into the wrong hands can have a particularly negative effect on business.

Linux Backup and Recovery

Backup and recovery are at its simplest a backup of essential files, such as an OS, on a separate storage medium that can be used in case the original data is corrupted to a degree where the system cannot run anymore. This feature is not only limited to critical systems but should be in place for every industrial embedded application. Creating and storing a backup is a nearly cost-free measure that can quickly resuscitate any system and drastically reduce downtime.

There is already free-to-use software for Linux backup and recovery available online. Below are a short introduction and a comparison with the Innodisk software.

dd

dd is a commonly used backup and recovery tool for Linux. The software works by creating a full image of the disk in question. However, the software is unable to do partial backups, and the speed is comparatively low.

When using dd, the user has to access the terminal to initiate the backup of the disk. As this process is not very intuitive, it can create issues for even experienced personnel.

Clonezilla

Compared to dd, Clonezilla offers more functionalities and higher data transfer speeds. Clonezilla has different user interfaces, a backup can be run on the whole or partitions of the disk, and recovery can be done remotely.

However, the user interface is relatively complex with several layers of options, and can often leave less experienced personnel at a loss on how to initialize backup and recovery. Due to this lack of an intuitive user experience, it should only be used by users already familiar with Linux systems.

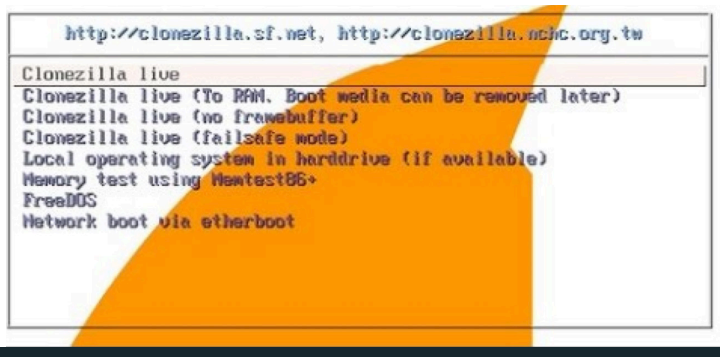


Figure 4: Screenshot of Clonezilla backup and recovery software

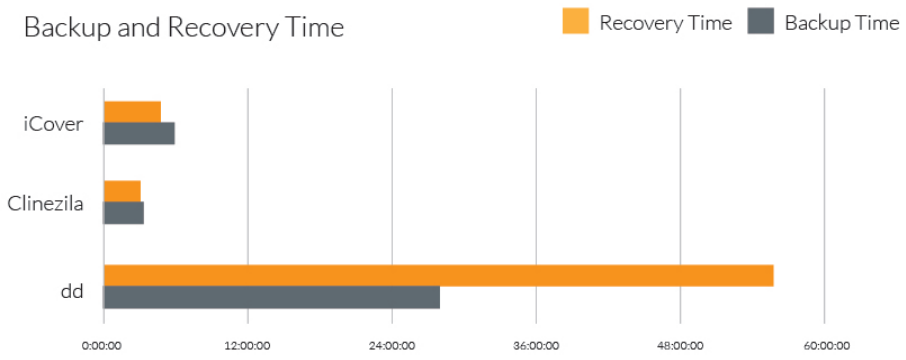
Innodisk's iCover and Comparison

The iCover software is compatible with all Linux operating systems. As with Clonezilla, it can handle backup of both full-disk and partitions with the option of remote execution, and speeds are approximately the same.

iCover's strengths, however, lie in its flexibility and intuitive use. As seen from the screenshot below (figure 5), the iCover API is a single page with the option of running recovery or backup. Furthermore, iCover has the most versatile set of execution and can be run through FnKey, DVD ROM, and USB.

Figure 5: Screenshot of iCover user interface

A test was run for both backup and recovery for all three pieces of software. The test was run on a rig with ATOM CPU, 8GB RAM, and a 64GB SSD. The test showed iCover at slightly lower speeds compared to Clonezilla, taking 1-2 minutes longer. However compared to dd with recovery and backup time of 56 and 27 minutes respectively, both iCover and Clonezilla performed the tasks relatively fast.



Graph 1: Backup and recovery time for iCover, Clonezilla and dd

Linux Customization – An Example

We can use a Point-of-Sales (PoS) system to illustrate a scenario that incorporates all four tools (see figure 6):

1. The computer is first booted up
2. Secure Boot is initialized
   A. If passed, the OS boots
   B. If failed, the OS will fail to load, i.e. startup is denied
3. After boot up, data can be written and deleted, but any alterations in protected files or drives will be disregarded and reset to original settings after system reboot
4. After a successful boot up, the App Launcher will immediately pop up allowing the user to log into the PoS software
5. If a crash were to occur, the recovered image can easily be run from the backup medium

This example shows how security and data safety can be easily interwoven in an easy-to-use manner. Even with an inexperienced user, the system is intuitive with little risk of mishandling.

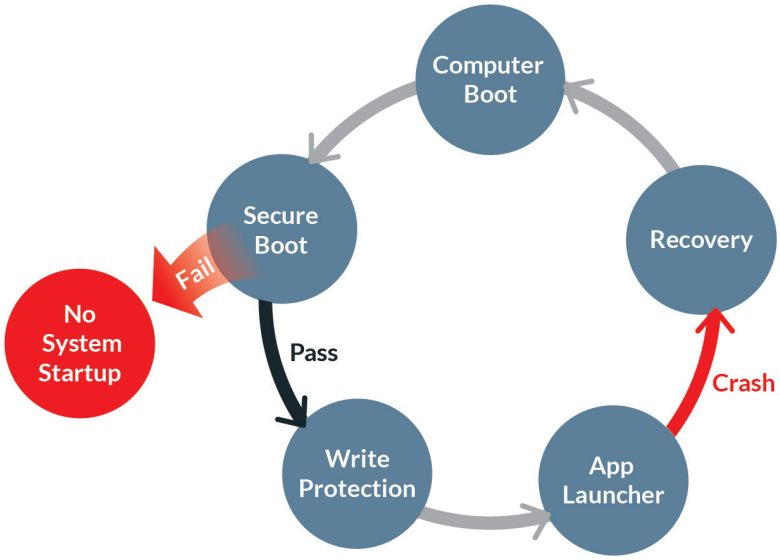


Figure 6: Flowchart showing how the four tools can be implemented together

Conclusion

Opting for Linux for your embedded application can be a good choice in terms of business. However, it is important to first be aware of the potential pitfalls in deploying this open source alternative.

As Linux is reliant on the community to output new apps and software, the right tools for your business might simply not be available. In this case, the cost of R&D can be significant, and further costs will occur if the user lacks the needed know-how.

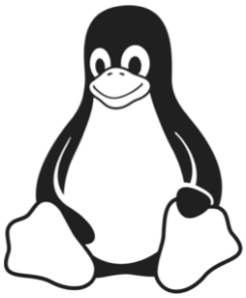
The use of App Launcher, Write Shield, Secure Boot, and Linux Backup and Recovery will address most concerns of user convenience, security, and backup for industries including retail, casino gaming, automation, and transportation.

The Innodisk Solution

Linux OS Customization

Comprehensive service that ensures an operating system optimized for your application

Innodisk customizes an operating system designed for your hardware platform. Through our Operating System Building Service, we are able to provide suggestions and plans suitable for an embedded system that optimizes the performance of your platform.



Innodisk Corporation

5F., NO. 237, Sec. 1, Datong Rd., Xizhi Dist., New Tapei City, 221, Taiwan
Tel : +886-2-7703-3000
Fax : +886-2-7703-3555
E-Mail : sales@innodisk.com
Website : www.innodisk.com