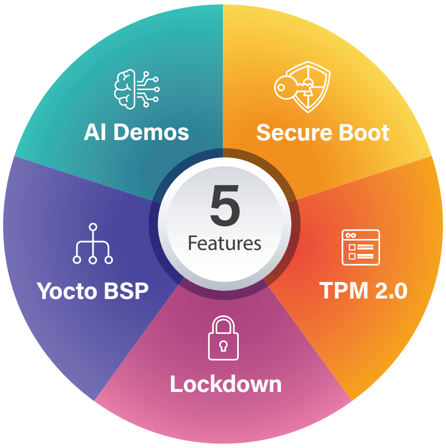
NEXCOM
Committed to Customer Success

White Paper

NEXCOM's Software Solutions Secure and Simplify System Development

NEXCOM prides itself on introducing the most cutting-edge hardware to the transportation industry. But amidst the more recent challenges to technology, where threats to information security and the complexity of tools and resources are all steadily increasing, how can businesses adequately prepare?

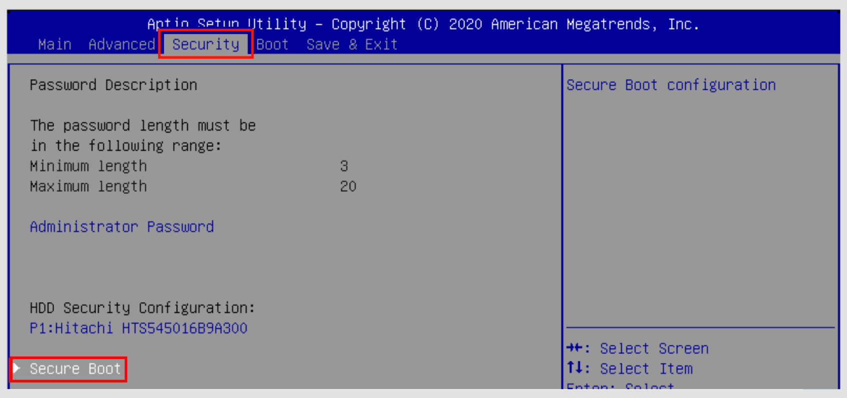
NEXCOM addresses these issues head-on with an extensive package of software features. Ensuring system security and integrity while simplifying the lives of developers, NEXCOM's mobile computing solutions can support five software features: secure boot, TPM 2.0, lockdown, Yocto BSP, and AI demos.



Secure Boot

For any business, computer hardware is irreplaceable and invaluable. The business wants to avoid hardware being used for unauthorized purposes, especially through unintended malware installations, and to protect hardware and software intellectual property rights. NEXCOM industrial computers all provide a standardized secure boot process that begins as soon as BIOS loads the OS. As a Unified Extensible Firmware Interface (UEFI) feature, the BIOS boot encryption function, combined with encrypted boot loader on Linux systems, can protect the machine from use by unauthorized operating systems.

Upon startup, the firmware authenticates credentials via pairs of public and private keys. It won't load any software, drivers, and OS loaders not signed with acceptable digital signatures, thus ensuring the integrity and security of the entire system. Users can learn how to operate the secure boot process via NEXCOM's instructional documents. For customers who have mass production requirements, NEXCOM simplifies the process by placing the encrypted key file in BIOS during production.



```
        Aptio Setup Utility – Copyright (C) 2020 American Megatrends, Inc.
  Main  Advanced  Security  Boot  Save & Exit

  Password Description                              Secure Boot configuration

  The password length must be
  in the following range:
  Minimum length                 3
  Maximum length                 20

  Administrator Password


  HDD Security Configuration:
  P1:Hitachi HTS545016B9A300
                                                    ++: Select Screen
▶ Secure Boot                                       ↑↓: Select Item
                                                    Enter: Select
```

Trusted Platform Module 2.0 (TPM 2.0)

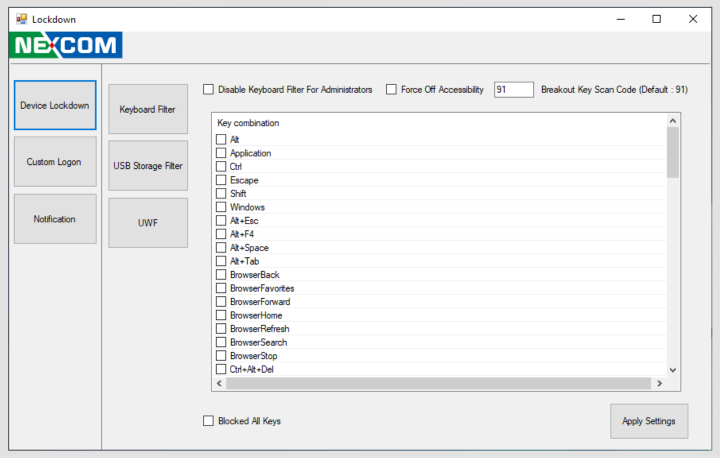
In tandem with secure boot, Trusted Platform Module 2.0 (TPM 2.0) provides complementary security features to prevent hacking and malware attempts when hardware loads the operating system. TPM is a secure cryptoprocessor that can be embedded in PCs and the only chip that they recognize. It's also a hardware encryption lock, generating unique cryptographic keys that are mostly used to authenticate and protect the integrity of files, directories, and sectors. Naturally, other encryption mechanisms can also be applied. TPM will test the system, based on preset measurements, to see if it's safe to boot up. If unsafe, it will lock the system.

As a standard promoted by the Trusted Computing Group (TCG), it was standardized by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) as ISO/IEC 11889, and initiated by well-known PC and software manufacturers such as Intel, IBM, HP, AMD, Sony, Sun Micro, and Microsoft. NEXCOM, in embracing the value of information security standards, simplifies the encryption process. All users can operate TPM with the enclosed instructional documents. For Windows users, BitLocker uses TPM to encrypt entire volumes. Linux users will find it easy to understand TPM with the demo program .

Lockdown

Developers often find user environments too complex. When designing Windows systems, developers only need to perform specific operations and will turn off some of Windows' default functions, including locking special keys, prohibiting access to USB storage, and preventing warning messages from popping up. To protect the integrity of drive volumes, they may also turn off unified write filter features. Yet developers are usually not familiar with some of Windows' special settings and spend unnecessary time locating related instructions with which they are not familiar.

NEXCOM includes a lockdown feature with UI to simplify the process and provide easy customization. Lockdown gives developers an interface from which they can quickly and directly operate to save valuable time, as well as set space parameters and avoid unwanted registry key changes. They can additionally lock down computers to prevent unauthorized usage or unwanted intrusions. For easy configuration, users are also provided with a Windows application.



□ Disable Keyboard Filter For Administrators □ Force Off Accessibility 91 Breakout Key Scan Code (Default : 91)

Key combination
- □ Alt
- □ Application
- □ Ctrl
- □ Escape
- □ Shift
- □ Windows
- □ Alt+Esc
- □ Alt+F4
- □ Alt+Space
- □ Alt+Tab
- □ BrowserBack
- □ BrowserFavorites
- □ BrowserForward
- □ BrowserHome
- □ BrowserRefresh
- □ BrowserSearch
- □ BrowserStop
- □ Ctrl+Alt+Del

□ Blocked All Keys

Yocto BSP

Whenever developers and system administrators want to install new software on their Linux systems, they're often concerned about large file sizes and incompatibility. They also want to simplify the development process as much as possible. NEXCOM resolves all of these issues with the services of Docker, a type of OS-level virtualization that delivers software in packages called containers, which are isolated and independently bundled. These containers can then easily deploy and run applications on new computer environments, including IT and cloud systems. NEXCOM has specifically developed a Docker container with a Yocto BSP.

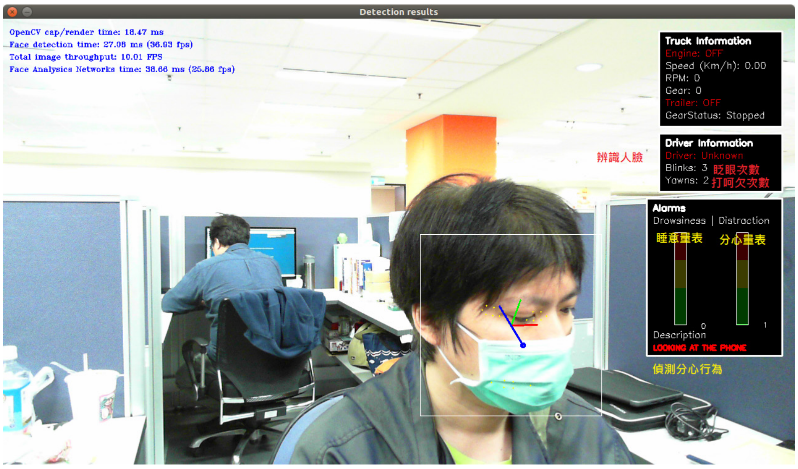
For developers, this simplifies the processes of creating environments and adjusting settings, as well as decreases time needed for development. In addition, it saves CPU resources and runs more efficiently. Instead of dramatically increasing application usage when performing separate tasks, multiple containers can run simultaneously as isolated processes while sharing the same OS kernel. Docker is especially useful for AI applications such as deep learning, as each container can have separate frameworks during testing for ultimate flexibility.

Using Docker images and other files, NEXCOM can include other Yocto-related development environments and source codes, so that developers can build their own Yocto OS without spending extra time downloading and organizing.

AI Demos

Developers often face complications arising from conflicting versions of operating systems and applications, which means they consequently need to build their own development environments. NEXCOM provides Docker images to help developers operate immediately without having to create development environments from scratch, especially through AI demo programs acting as control groups, so that developers can begin their development work more confidently.

NEXCOM simplifies the process with Docker images for various AI-enabled GPU/TPUs: Google Coral, Intel Movidius, and Nvidia. More specifically, NEXCOM provides demos of vehicle and object detection on Google Coral TPUs and Nvidia GPUs, and driving behavior on Intel Movidius GPUs. These images allow users to directly use the Docker image environment for development or reference. Users can simultaneously and quickly use different containers, allowing them to see the infinite possibilities of using graphics cards on NEXCOM's computers.



```
OpenCV cap/render time: 18.47 ms
Face detection time: 27.08 ms (36.93 fps)
Total image throughput: 10.01 FPS
Face Analysics Networks time: 38.66 ms (25.86 fps)
```

```
Truck Information
Engine: OFF
Speed (Km/h): 0.00
RPM: 0
Gear: 0
Trailer: OFF
GearStatus: Stopped

Driver Information
Driver: Unknown
Blinks: 3
Yawns: 2

Alarms
Drowsiness | Distraction
0          1
Description
LOOKING AT THE PHONE
```

NEXCOM Solutions Lead the Way

NEXCOM provides a myriad of comprehensive solutions that include all five of the above software architecture features to enhance security and efficiency in mobile computing applications. Specific hardware solutions include vehicle telematics computers, vehicle mount panel computers, AI telematics computers, vehicle mount displays, and railway computers. In our effort to serve customer needs and be the best in the field, NEXCOM is always developing fresh, innovative solutions for all facets of the mobile computing world.

NEXCOM
Committed to Customer Success

Founded in 1992 and headquartered in Taipei, Taiwan, NEXCOM is committed to being your trustworthy partner in building the intelligent solutions. NEXCOM integrates its capabilities and operates ten global businesses, which are Industrial Mesh, Intelligent Video Surveillance, IIntelligent Platform @ Smart City, Mobile Computing Solutions, Medical and Healthcare Informatics, Network and Communication Solutions, Smart Manufacturing, and Open Robotics and Machinery. This strategic deployment enables NEXCOM to offer time-to-market, time-to-solution products and service without compromising cost.

www.nexcom.com

intel | IOT Solutions Alliance

NEXCOM is an Associate member of the Intel® Internet of Things Solutions Alliance. From modular components to market-ready systems, Intel and the 400+ global member companies of the Intel® Internet of Things Solutions Alliance provide scalable, interoperable solutions that accelerate deployment of intelligent devices and end-to-end analytics. Close collaboration with Intel and each other enables Alliance members to innovate with the latest technologies, helping developers deliver first-in-market solutions.

Learn more at: intel.com/iotsolutionsalliance

Intel and Intel Core are registered trademarks of Intel Corporation in the United States and other countries.

Published in January 2021