A4F Safe II+

...I have to stay outside...

Not only the case is solid. The system is protected against viruses by hardware.

The carefree computer, resistant for sure.

Schneider Elektronik GmbH & Co. KG

Dresdener Straße 29
D-01909 Großharthau
Germany

www.schneiderelektronik.com

Info:

Buy at:

Info & Webshop (Exclusive **U**ni**X**/**L**inu**X** Solutions): www.uxlx.com/a4f www.uxlx.eu

A4F Safe II+  Table of content

Table of Content

Filename a4f_safe2p_en_09.doc

A4F Safe II+  Pictures & views

Front views

To clarify the size ratios two coins (1 Euro & 1 Dollar) have been placed on top of the system.

The switch combi on the right side is visible as well. This can be interrogated by software and may be used to trigger any event. In the reference implementation a complete Windows is started additionally as a virtual machine (the completion of the installation, the acquisition of the license and the activation is the responsibility of the end user).

Perspective view

A complete computer that does not only look beautiful, but also lets you forget many of the current worries when dealing with computers. The unique feature of this computer is a *hardware-write-protected medium* for the operating system and the installed applications. This means that the system can be "locked" after the installation with a safe-security-key (the hardware write protection is activated) to assure a permanent reliable protection.

Even for the most experienced hackers or other criminal users (even with full administrative privileges) the operating system or the installed software can not be modified if the write protection is activated (in simple words, the device has been "locked" with the safe-security-key). At the latest after a reboot the original state is back again.

The safety lock keys are visible on the left side. If the device has been "locked" with the safe-security-key, the entire operating system and the software installed on the medium with hardware write protection is 100% protected against any modification (accidental erasure, malicious software, any type of virus, ...).

Rear views

As to see in both pictures above the safe-security-cover can be removed after unlocking it with the safe-security-key. Afterwards the medium with the complete operating system and the applications can simply be exchanged with just a few hand movements. Furthermore you may easily exchange the internal harddisk/SSD (Solid State Disk, used to store user data) within a few seconds.

A4F Safe II+  Options

Introduction

During an online order the current model with an optional queryable switch on the right sight would be supplied. Starting in 2020 a small modification with a second optional switch could be delivered. Usually those switches will not be needed but may be used for special applications as an additional input option.

Furthermore, there are currently a variety of specially adapted systems. The replacement of the removable O/S medium by an internal M.2 SATA SSD with hardware write protection may be an interesting option. But also a removable SSD with more capacity or an internal NVMe SSD could satisfy even higher demands.

For questions or in case of uncertainties please contact the manufacturer before ordering.

If after months of use it should turn out that this aforementioned second optional switch would be desired, that would be no problem at all. Since the owner of the safe security key may swap the system medium and the data SSD in a few simple steps. The new system would be identical in a few minutes without much effort.

Current implementations

This document contains all the required details of the current implementation. In some pictures there is already a small additional modification to see. There will be a second switch on the right side optionally available starting in 2020.

The front LED assignments and the marginal technical detail differences are at the end of the section Technical Details (1804 + 2001). If a custom adjustment of the functionality of the right switch is desired, those could be helpful. For any further questions please contact the manufacturer.

Historical implementations

There were several variants, e.g. with other motherboards, enlarged housing, other O/S Medium, ..., other CPUs. The corresponding documentation is currently only available to the existing customers. If you have specific requirements or questions, so please contact the manufacturer directly.

A4F Safe II+  History & future

The beginning and interesting details

Based on the proven basic model "A4F Slim" and the predecessor model "A4F Safe I" and the more than 20 years of experience in fan-less computer engineering, this new system was developed together with external partners. It provides a currently unique implementation of a noncompromisable protection of the operating system and the installed software (after appropriate activation). In order to prevent any change to any components of the operating system and the software, a hardware write-protection for the system medium can be activated by means of a safe-security-key. If this protection is enabled, it is not possible to modify even a single bit from the operating system or the installed software because the medium itself is no longer writable. At the latest after a reboot of the system it is exactly as before. There will be definitely no changes since those were made impossible by the hardware itself.

Since some kind of data may be created in a system with which to work or play, the A4F Safe II+ also contains a writable SSD (Solid State Disk). If configured accordingly, this created data can also be accessed after a restart. In the current reference implementation, it is recommended to use this SSD simply to store the "user home directories (HOME of user XYZ = /homeSSD/XYZ)".

Through the combination of the carefully chosen hardware and the powerful operating system and the huge choice of freely available software “nearly everything for normal life” may be covered. Most times it is a good choice to just start with the reference implementation and to adopt it over the time to your needs.

If the requirements are far above the average, it should be relatively easy to find a solution in the big Linux community. Alternatively, full support is also available via the manufacturer or some partner. The suggestions generated by this path are again beneficial to all subsequent reference implementations and thus to all customers.

The "A4F Safe II+" was developed in Germany and is also manufactured in Germany. The design is solid and proven and can not be compared with cheap plastic or sheet metal housings. The components used were carefully chosen. The operating system and the pre-installed software are used millions of times. The number of commercially available software is growing steadily. There is an almost incredible amount and variety of freely available software.

Since the system was originally designed for use as a "Web PC" in a highly frequented environment, it is particularly suitable for this application. It may make sense to use the special guest mode in such a constellation. A system with a similar configuration is running without problems since April 2016.

Limitations

The system is currently not suitable for "high-end gamers" with extremely high hardware requirements. Furthermore some really high-intensity tasks such as may be the extensive editing of high resolution 4K-HD videos on this device is no fun. But for normal everyday use the system is more than adequate and the reliability is far above the average. The operating system and the installed programs are reliably protected from unintentional changes in the safe mode by the hardware itself. A kind of golden compromise between high performance and power consumption was realized. Because the system was designed without fans and therefore without disturbing noise and dust circulation, only performance-optimized components could be used. In addition to the unusually comfortable noise-free operation and the elimination of regular maintenance work (such as CPU and graphic card fans dust removal / replacement, internal casing dust removal, contacts maintenance, etc.), this is also noticeable on the electricity bill at each years end.

Operating system

If you have read up to here and think this "A4F Safe II+" seems to be nearly perfect, you have already recognized it. However, there is still a small challenge. The native operating system on this device is not Windows but Linux. For the reference implementation, Ubuntu was chosen in the current LTS version (long term support, 18.04.3). There were several reasons for this choice. A reference implementation of any distribution in all conceivable combinations and the coverage of various requirements can be made available if really required in a short period of time.

Currently, there are native Linux alternatives for most Windows applications. Unfortunately, there are currently still isolated manufacturers, which do not yet offer their software as a Linux version. The good is, these are becoming less and less. Furthermore, the number and quality of the Linux alternatives is constantly increasing. However if you are forced to use a Windows program which has currently no native Linux version available there is also a solution. The switch combi is located on the right side. In the end, this is only a switch that can be evaluated via software. If the first switch is set to I during system startup, a full Windows 7 virtual machine (KVM) is started in the current reference implementation. In simple terms, you now have a fully-fledged Windows 7 in a window for this one program. You can also use this in full screen mode. Then there is actually no difference in look, feel and functionality to a native Windows 7 system. The Windows 7 virtual system is prepared and has already installed the majority of the updates. To use it fully you must have a valid license and complete the installation yourself and then activate it.

It was intentionally chosen Windows 7 as this version is still very often in use and would also be used by different people for a variety of reasons for a while. However, this is sometimes not possible or is very difficult at all on current hardware. In the present constellation with the prepared virtual Windows 7 system, this is almost a children's game.

If you want to use Windows 10, you could create another VM (virtual machine) which may be based on the Windows 7 system VM example. If you definitely do not need Windows 7, simply

install Windows 10 over the existing installation. Otherwise, it may make more sense to simply create a second virtual machine according to your requirements.

Theoretically there is also the possibility to install Windows 7 (or 10, ...) natively as dual boot. However, since this does not fit completely to the intended security concept, details are not discussed. However, in the case of actual demand, corresponding details can be made available.

Applications and system updates

This system is perfect for kiosk systems with constantly changing users. And it is perfect for a lot of other scenarios as well. For instance if a system is simply implemented and shall stay unchanged and remain reliable for long periods of time.

Thus the apparatus is very well suited for small enterprises, where there is no own IT department for regular system maintenance. The system is set up and performs its work in unchanged form over a very long period of time.

But even in very large companies there are often systems that are to be operated over several months or even years with a static configuration and equipment that must not be changed. This can be ensured permanently by means of a simple "closing" it with the safe-security-key.

Another example is an advanced computer cabinet in a school. There is no need for regular, unplanned effort to recover software and settings, or to remove viruses and so on. Every lesson (today, in a week, in a year, ...) always begins with the same defined initial state. There are a very large number of programs for daily use in education. But there are also powerful development environments for a computer science cabinet, many programming languages and almost all "state of the art" software.

Currently the implementation of Linux school computers is not very common. This system would be a very good investment. It is able to cover all current and future requirements in this direction with a single device.

This system is perfect if you have an existing constellation running, and an uncontrolled change in the system or software, e.g. through viruses or malicious software, or unwanted manual intervention must be prevented. In simple terms, this means that you do not have any maintenance requirements for the device over a longer period of time, which is defined exclusively by yourself. If that systems starts today in a predictable time X this time will never change as long it is in the "locked" mode. This time will not be any longer either tomorrow, or in a month or in 2 years. Also any annoying forced updating at undesired times during shutdown or startup is not necessary. As long as the system is in "locked" mode it will be exactly as before after each restart.

At the latest after several years or after becoming aware of a real problem or a non-tolerable feature, an update or other changes can be performed in a scheduled time window. Various approaches are practicable:

1. The owner of the safe-security-key can "unlock" the system (remove the hardware write protection). After that, the software can be easily updated or extended or changed. After the action

has been performed, the system is "closed" again (hardware write protection is activated with the safe-security-key). From now on, the entire operating system is in an invariable mode and will continue to function well for months.

2. An update of individual software components or the installation of programs could possibly also take place in safe mode. However, the changes are not permanently stored, since the hardware write protection is activated. After a restart, the action shall be repeated. If necessary, the change could be repeated later in the "temporarily unlocked mode" at a scheduled time in order to be active even after a restart.

3. An updated reference implementation of the system can be obtained at regular intervals from the manufacturer on the easily interchangeable medium. The owner of the safe-security-key can "unlock" the system and replace the write protected system medium easily. After locking it again the system is back in a safe and up-to-date state. If, contrary to expectations, it should appear in days or weeks that the previous state is desired for some reason, this is very easy. There is no need to think about complicated re-installation / restore scenarios, recovery points, or manipulation of software packages. Simply switch off, unlock, reinsert the old medium, close it and everything is well as before. If necessary, the presumed irregularity could then be investigated by simply sending the suspect medium for analysis to the manufacturer without affecting any local work.

Since the operating system is normally on the read-only ("locked") medium, a modification by viruses or other malicious software is also excluded. The system can provide all its resources for normal work. A deceleration of the performance through constant virus scanning of the operating system is a thing of the past on this device.

A4F Safe II+  Technical details

Basic configuration

- Intel® Celeron® J4105 (Quad Core) 1.5 GHz / 2.5 GHz

- 8 GB main memory (up to 16 GB)

- Integrated Intel® UHD Graphics 600/605

- 32 GB medium (up to 128 GB) with hardware write protection for system and software

- 512 GB SSD (2,5 inch SATA, customer replaceable) for user data

- Noiseless, since neither fan nor rotating hard disks are installed

- Typical power consumption (depending on usage profile) approx. 12 Watt

- Optional deviations can be agreed at time of order (for instance more RAM, SSD with more capacity, additional internal M.2 NVMe SSD, 32GB SATA-DOM with hardware write protection, 32GB M.2 SATA SSD with hardware write protection, …), on any question please contact the manufacturer

Measures and weight

Width:	290 mm
Height:	47 mm (including 4 mm rubber feet)
Depth:	187 mm
Weight:	approx. 2.6 kg

Front

1. *2x control LEDs, very left, red (top, #1) + green (bottom, #2)*

These two LEDs reflect the state of the safe-security-lock. In normal circumstances the green LED (#2) should be on and the red LED (#1) should be off. This means that the medium for the operating system and software is changed to read-only by hardware. In this state, it is not possible to change the operating system or the software. For a planned update of the operating system or for the installation of additional software, the write-protection must be temporarily deactivated with the safe-security-key. In this case, the green LED turns off and the red LED turns on.

2. 2x control LEDs, left beside on- off-switch, red (top, #3) + green (bottom, #4)

The green LED shows activities on the SSD. The red LED is freely programmable. In the reference implementation, it is turned on as soon the internal SSD is occupied with more than 90% of data.

3. On / off button with indicator light

4. 4x control LEDs, right beside on- off-switch, red (top, #5) + green (bottom, #6) & red (top, #7) + green (bottom, #8)

These four LEDs reflect the state of the switch combo that can be interrogated by software on the right side (I = red, II = green). In the reference implementation the left switch is checked during start-up. If it is in position I (the corresponding red LED #5 is on), a prepared virtual Windows machine is automatically started. If you want to use this, you must have a corresponding Windows license and you must complete the Windows installation yourself and activate it accordingly. It is recommended to do the "normal things" with the native applications and to use the virtual Windows system only if there are missing alternatives.

5. 2x USB 3

6. Analog Audio (Headphone Out/left & Microphone In/right)

ATTENTION, remark: The aforementioned LED-description is already adjusted to the 2020 optional deliverable two switch version (2001). The current version (1804) has just a few small derivations (#4 = HDD; #3,#5, #6 = programmable; #7 red on, if switch I / WindowsVM; #8 green on, if switch=0 / no action).

Sides / right & left

A switch combo on the right side; two software-freely configurable mechanical switches; the state is also displayed on the front via the four LEDs to the right of the on/off switch.

On the left side there is the safe security lock. The current state may be recognized by the most left control LED's on the front (red/#1 = hardware write protect = off = system may be intentionally modified or updated OR green/#2 = hardware write protect = on = SAFE).

Back

1. Optional one or two WLAN-antennas

2. Power supply connection (8-24 Volt, wide range)

For several reasons a mainboard with an external power supply has been chosen. Service is more easy and through the wide range input there is no dependency on expensive special supplies.

3. 2x Monitor / Displayport #1 left, #2 right, V1.2a, max. 4096 X 2160 @ 60 Hz

→ is compatible with following adapters: (Dual Mode / DisplayPort++)

o DP to HDMI (passive + active)

o DP to DVI (passive + active)

o DP to VGA (active)

4. 2x 1000MBit Ethernet (Intel i210 / Realtek RTL8111G)

5. 4x USB 2.0

6. Safe-security cover; behind the cover is the read-only removable media for the operating system and the software and furthermore the easily exchangeable SSD for user data.

Metal case

- the casing is made of strong aluminum with precise machined details

- the internal precision-made heat conduction systems are developed in-house

- the system is prepared for anti-theft protection with a "Kensington-Lock” security slot (right side)

- optional, suitable for wall mounting

- optional, vertical case support is available

- optional, the available space at the front may be used for an own logo

- optional, mounting of a separately available VESA holder can be prepared

- optional, the system is available in various well chosen surface and color combinations; optionally, the color can be chosen freely by means of RAL code and thus adapted to your own needs

Mainboard

The mainboard has been designed and made in Germany. Following a few interesting remarks:
- 1x M.2 Key M socket (max. 2230), used for Wifi/BT
- 1x M.2 Key B socket (max. 2280 bzw. 2260, oder 2242), Key B; SATA and PCIe x1, Key B and Key B+M modules useable (like Intel OptaneTM SSD 800P-Serie, bootable, …)

Restrictions (directly from the manufacturer):
- Due to Intel restrictions, D3544-S (GeminiLake) is the first platform that necessarily requires an UEFI/GPT-based OS installation. Legacy Boot support (e.g. USB Stick- DOS Boot, MBR-based OS installation) as used on previous mainboard models is no longer supported.
- The M.2 socket (SATA interface only) is shared with SATA Port 1. They can not be used simultaneously. In order to use up to three memory devices, following configuration is possible:
* SATA port 0: 2.5” HDD / SSD
* SATA port 0: 2.5” HDD / SSD
* M.2 socket: PCIe-based M.2 module (2242 or 2260 or 2280)
- Mainboards D354x-S are designed according to the Microsoft Guidelines for MS Windows 10 RS2 / RS3
- The typical battery lifetime is designed for 5 years. If the mainboard is just stored (no operating voltage attached), the typical battery lifetime is also 5 years. Due to tolerances of the installed battery, the effective battery lifetime may be in the range of 4.5 years – 6 years

Additional software information

The operating system and installed software is a customized standard installation of the current Ubuntu LTS version (long term support, 18.04.3). The changes made are traceable on the system.

The purchase price completely covers the complete hardware and a small part of the development costs. Furthermore a part of it will be used for the further development of the specialized hardware and a future provision of a continuously developed and updated reference implementation. This benefits all existing customers.

The operating system and the installed software are available without additional costs as a reference implementation. If other reference implementations are developed in the future, those may be obtained by existing customers from the manufacturer.

For this system, at least once a year, there will be a reference implementation based on the current Ubuntu LTS version. This is guaranteed for a period of at least 5 years from the date of purchase. It can be obtained by existing customers from the manufacturer.

The operating system and the installed software can be updated manually or automatically after temporary "unlocking with the safe-security-key" (removal of the write-protection). The most common mechanisms of the O/S distributor can be used for this purpose. Furthermore it is also possible to make any desired adjustments and to install additional software without problems. In the case of specific, clearly defined requirements, the manufacturer or some corresponding partner may provide each kind of support.

Technical internal details / 1804, one switch on the right side

GPIO-Assignments:

289 direction in only / security key lock switch:

security key makes led #1 / red / upper left on when open / key vertical position / 1

security key makes led #2 / green / lower left on when closed / key horizontal position / 0

292 = led #3 / red

293 = led #4 / green

294 = led #5 / red

HDD led #6 / green

295 direction in only / switch on the right side:

295 = led #7 / red / upper most right / right side right switch to rear I / 1 / Win-VM if configured

295 = led #8 / green / lower most right / right side right switch to front 0 / 0 / no action

there may have been a few systems having an inverse setting of gpio 295 compared to above:

201901xx, (switch 0, gpio = 1 = led #7/red on; switch I, gpio = 0 = led #8/green on)

Technical internal details / 2001, two switches on the right side

GPIO-Assignments:

289 direction in only / security key lock switch

security key makes led #1 / red / upper left on when open / key vertical position / 1

security key makes led #2 / green / lower left on when closed / key horizontal position / 0

292 = led #3 / red /freely programmable

HDD led #4 / gn

294 = led #5 / red / upper / right side left switch up / I on

293 = led #6 / gn / lower / right side left switch down / II on

if right side left switch is in middle position, 2x gpios above may be used as in our out

#

296 = led #7 / red / upper most right / right side right switch up / I on / Win-VM if configured

295 = led #8 / gn / lower most right / right side right switch down / II on

if right side right switch is in middle position, 2x gpios above may be used as in our out

A4F Safe II+  Food for thought

There is no need to continue reading if you have already chosen to buy this system. If you are not quite sure yet, there are a few additional thoughts which may lead to more understanding and may deliver a few more arguments.

If I have a working system and it meets all my requirements, why should I update it daily and add, remove or change sporadically and uncontrollably any kind of software? Or is it better to keep the system easy in this state and to exclude changes ("lock" the device)? Does it make sense to know the exact times when changes have been made to the system? Isn't it nice if I have a completely up-to-date system with a few hand movements (exchange of the system medium against a current reference implementation or against a self-generated backup medium) or can always go back to some known good reference level?

Let us assume I think already for a while to use a virtual machine. I understood some of the unbeatable arguments, but I could not yet decide for a solution. If money does not matter, VMware is certainly a very good choice. If I get the complete VM (virtual machine) already completely prepared (for use or as an example for the creation of additional VMs) with the "A4F Safe II+" in the reference implementation, then KVM is surely a very good choice. In the given constellation, the Windows VM is essentially just a configuration file and a disk file. If the VM is switched off, you can create a full copy of the complete Windows system within a few minutes and you would have a way to completely restore this Windows system within minutes.

Join the people who want to use a computer system just as a tool (or toy or working equipment etc.) and just use it reliably. Do not worry about unwanted changes to the operating system and its components. Gone are the fears that something is "twisted" on the system in the background or during rebooting or switching off. There will be no bad times when one tries to understand who has changed what from whom and why and why the difference between theory and practice is usually much greater in practice.

Thanks also to Oerties GmbH (www.oerties.com)