A4F Safe II+

...ich muss draußen bleiben...

Nicht nur das Gehäuse ist solide. Das System ist durch die Hardware vor Virenbefall geschützt.

Der Sorglos-Computer, mit Sicherheit beständig.

Schneider Elektronik GmbH & Co. KG

Dresdener Straße 29
D-01909 Großharthau

www.schneiderelektronik.com

informieren: kaufen:

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

A4F Safe II+ Inhaltsverzeichnis

Inhaltsverzeichnis

A4F Safe II+....1
A4F Safe II+ Inhaltsverzeichnis....2
A4F Safe II+ Bilder & Ansichten....3
Vorderansichten....3
Perspektivische Ansicht....4
Rückansichten....5
A4F Safe II+ Optionen....6
Einführung....6
Aktuelle Implementierungen....6
Historische Implementierungen....6
A4F Safe II+ Historie & Zukunft....7
Der Anfang, interessante Details....7
Einschränkungen....8
Betriebssystem....8
Anwendungen und Systemaktualisierungen....9
A4F Safe II+ Technische Details....12
Basiskonfiguration....12
Abmessungen und Gewicht....12
Vorderseite....13
Seiten / rechts & links....14
Rückseite....15
Gehäuse....16
Mainboard....16
Zusatzinformationen Software....17
Technical internal details / 1804, one switch on the right side....18
Technical internal details / 2001, two switches on the right side....19
A4F Safe II+ Denkanstöße....20

Dateiname: a4f_safe2p_de_09.doc

A4F Safe II+ Bilder & Ansichten

Vorderansichten

Zur Verdeutlichung der Größenverhältnisse wurden auf dem System zwei Münzen (1 Euro & 1 Dollar) positioniert.

Auf der rechten Seite ist eine frei programmierbare Schalterkombination zu erkennen. Diese kann per Software abgefragt und zum Auslösen von beliebigen Ereignissen verwendet werden. In der Referenzimplementierung wird damit zusätzlich ein vollständiges Windows gestartet (die Fertigstellung der Installation, der Erwerb der Lizenz und die Aktivierung obliegen dem Endanwender).

Perspektivische Ansicht

Ein vollständiger Computer, der nicht nur schön aussieht, sondern auch viele der gegenwärtigen Sorgen beim Umgang mit Computern, wie z.B. das unliebsame Einnisten von Viren oder das versehentliche verstellen wichtiger Parameter, vergessen lässt. Das Alleinstellungsmerkmal dieses Computers ist ein per Hardware schreibgeschütztes Medium für das Betriebssystem und die installierten Applikationen. Somit kann das System nach der Einrichtung mit einem Safe-Sicherheits-Schlüssel „zugeschlossen“ (der Hardware-Schreibschutz wird aktiviert) und dauerhaft zuverlässig geschützt werden.

Selbst für die erfahrensten Hacker oder auch andere kriminell veranlagte Benutzer (sogar mit vollen administrativen Privilegien) ist bei aktiviertem Schreibschutz (in einfachen Worten, das Gerät wurde mit dem Safe-Sicherheits-Schlüssel/hinten links „zugeschlossen“) keinerlei Änderung des Betriebssystems oder der installierten Software möglich. Spätestens nach einem Neustart ist der Originalzustand wieder vorhanden.

An der linken Gehäuseseite sind die Sicherheitsschüssel deutlich zu erkennen. Wenn das Gerät mit dem Safe-Sicherheits-Schlüssel „zugeschlossen“ wurde und bleibt, ist das komplette Betriebssystem und die auf dem Medium mit Hardware-Schreibschutz installierte Software zu 100% vor jeglicher Manipulation (versehentliches Löschen, bösartige Software, jegliche Art von Viren, …) zuverlässig geschützt.

Rückansichten

Wie in den vorstehenden Abbildungen zu sehen, kann nach dem Aufschließen mit dem Safe-Sicherheits-Schlüssel die Safe-Sicherheits-Verdeckung abgenommen werden und das Medium mit dem vollständigen Betriebssystem und den Applikationen kinderleicht mit wenigen Handgriffen komplett ausgetauscht werden. Des Weiteren ist es Dank des gut bedienbaren Wechselrahmens möglich, die interne Festplatte/SSD (Solid-State-Disk, Speicherort für die Benutzerdaten) kinderleicht auszutauschen.

A4F Safe II+ Optionen

Einführung

Bei einer Online-Bestellung wird gegenwärtig das aktuelle Modell mit einem optional abfragbaren Schalter an der rechten Seite geliefert. Ab 2020 wird zusätzlich eine Modifikation mit zwei abfragbaren Schaltern an der rechten Seite erhältlich sein. Im Normalfall werden diese nicht benötigt, sie könnten jedoch für Spezialanwendungen als zusätzliche Eingabe-Option Verwendung finden.

Weiterhin gibt es gegenwärtig eine Vielzahl von speziell angepassten Systemen. So könnte z.B. der Ersatz des herausnehmbaren O/S-Mediums durch eine interne M.2 SATA SSD mit Hardware-Schreibschutz unter Umständen sinnvoll sein. Aber auch eine herausnehmbare SSD mit mehr Kapazität oder eine interne NVMe-SSD könnten für spezielle Anwendungen mit noch höheren Anforderungen Sinn machen. Bei Fragen oder Unsicherheiten kontaktieren Sie bitte den Hersteller vor der Bestellung.

Sollte sich einmal nach monatelanger Benutzung herausstellen, dass z.B. doch dieser zweite optionale Schalter gewünscht würde, so wäre das auch kein Problem. Da der Besitzer des Safe-Sicherheits-Schlüssels das System-Medium und die Daten-SSD mit nur wenigen Handgriffen übernehmen kann, wäre das neue System ohne viel Aufwand in wenigen Minuten identisch im Betrieb.

Aktuelle Implementierungen

Dieses Dokument enthält alle benötigten Details der aktuellen Implementierung. Auf den Bildern ist bereits eine kleine zusätzliche Modifikation (ein zweiter Schalter an der rechten Seite, optional erhältlich ab 2020) zu erkennen.

Die Front-LED-Zuordnungen und die marginalen technischen Detail-Unterschiede sind am Ende des Abschnittes Technische Details (1804 + 2001) aufgeführt. Wenn eine kundenspezifische Anpassung der Funktionalität des rechten Schalters gewünscht ist, könnten diese hilfreich sein. Bei weitergehenden Fragen kontaktieren Sie bitte den Hersteller.

Historische Implementierungen

Es gab verschiedene Varianten, z.B. mit anderen Mainboards, vergrößertem Gehäuse, anderem O/S-Medium, …, andere CPUs. Die entsprechende Dokumentation steht gegenwärtig nur den Bestandskunden zur Verfügung. Wenn Sie spezifische Anforderungen oder Fragen haben, so wenden Sie sich bitte direkt an den Hersteller.

A4F Safe II+ Historie & Zukunft

Der Anfang, interessante Details

Basierend auf dem bewährten Grundmodell „A4F Slim“ und den Vorgängermodellen „A4F Safe I“ und „A4F Safe II“ und weiterhin der über 20 jährigen Erfahrung im lüfterlosen Computerbau wurde zusammen mit externen Partnern dieses neuartige System entwickelt. Es bietet so in der Form eine gegenwärtig einzigartige Implementierung eines bei entsprechender Aktivierung nicht kompromittierbaren Schutzes des Betriebssystems und der installierten Software. Um jegliche Änderung aller Komponenten des Betriebssystems und der Software zu verhindern, wurde ein mit Hilfe eines Safe-Sicherheits-Schlüssels aktivierbarer Hardware-Schreibschutz für das Medium mit dem Betriebssystem und der installierten Software implementiert. Wenn dieser Schutz aktiviert ist, kann nachweisbar nicht einmal ein einziges Bit vom Betriebssystem oder der installierten Software geändert werden, da das Medium selbst nicht mehr beschreibbar ist. Spätestens nach einem Neustart des Systems ist es exakt so wie vorher, definitiv ohne jegliche Änderungen, da diese in Hardware unmöglich gemacht wurden.

Da in einem System, mit welchem gearbeitet oder gespielt werden soll, auch Daten anfallen, befindet sich in dem „A4F Safe II+“ zusätzlich eine beschreibbare SSD (Solid State Disk / Festplatte). Bei entsprechender Konfiguration kann dann auf diese Daten, wie zu erwarten, auch nach einem Neustart zugegriffen werden. In der gegenwärtigen Referenzimplementierung wird empfohlen, diese SSD einfach für die Speicherung der „Benutzer-Heimatverzeichnisse (user HOME = /homeSSD/user)“ zu verwenden.

Da die verwendete Kombination aus sorgfältig ausgewählter Hardware und dem mächtigen Betriebssystem und der riesigen Auswahl an frei erhältlicher Software nahezu „alle Anforderungen im normalen Alltag“ abdecken kann, wird für einen „sauberen Einstieg“ auf die vorstehende Empfehlung verwiesen. Sollten die Anforderungen überdurchschnittlich anspruchsvoll werden, so sollte es relativ leicht sein, in der großen Linux-Gemeinde zeitnah eine Lösung zu finden. Alternativ ist auch über den Hersteller ein vollständiger Support möglich. Die über diesen Weg entstehenden Anregungen kommen wiederum allen nachfolgenden Referenzimplementierungen und somit allen Kunden zu Gute.
Der „A4F Safe II+“ wurde in Deutschland entwickelt und er wird auch in Deutschland gefertigt. Die Konstruktion ist solide und bewährt und mit billigen Plastik- oder Blechgehäusen nicht zu vergleichen. Bei den verwendeten Komponenten wurde nicht an der falschen Stelle gespart. Es wurde weiterhin Wert darauf gelegt, ein ebenfalls in Deutschland entwickeltes und hergestelltes Mainboard zu verwenden. Das verwendete Betriebssystem und die vorinstallierte Software sind millionenfach im Einsatz. Die Anzahl kommerziell verfügbarer Software steigt stetig. Es gibt eine unglaubliche Menge und Vielfalt an frei verfügbarer Software.

Da das System ursprünglich für den Einsatz als „Web-PC“ in einer von verschiedensten Kunden stark frequentierten Umgebung konzipiert wurde, ist es für diesen Einsatzfall besonders gut geeignet. Es macht Sinn, in solch einer Konstellation einen speziellen Gast-Modus zu verwenden. Es gibt mehrere Referenzimplementierungen, wobei ein System mit einer vergleichbaren Konfiguration seit April 2016 ohne Probleme im Einsatz ist.

Einschränkungen

Das System ist gegenwärtig für „High-End-Gamer“ mit extrem hohen Anforderungen an die Hardware nicht geeignet. Des Weiteren machen einige wirklich rechenintensive Aufgaben, wie z.B. das umfangreiche Bearbeiten von hoch aufgelösten 4K-HD-Videos, auf diesem Gerät keinen Spaß. Aber für den täglichen normalen Einsatz ist das System mehr als ausreichend dimensioniert und vor allem ist die Zuverlässigkeit sehr weit über dem Durchschnitt, da ja das Betriebssystem und die installierten Programme zuverlässig vor ungewollten Änderungen im Safe Modus durch die Hardware selbst geschützt sind. Es wurde ein alltagstauglicher Kompromiss zwischen Hochleistung und Stromverbrauch realisiert. Da das System ohne Lüfter und somit ohne störende Geräuschentwicklung und Staubzirkulation konzipiert wurde, konnten nur leistungsoptimierte Komponenten verwendet werden. Neben dem ungewohnt komfortablen, geräuschfreien Arbeiten und dem Wegfall regelmäßiger Wartungsarbeiten (wie CPU- und Grafik-Lüfter entstauben / tauschen, eingesaugten Staub entfernen, …) macht sich dieses am Jahresende auch auf der Stromrechnung bemerkbar.

Betriebssystem

Wenn Sie jetzt bis hier gelesen haben und denken, dieser „A4F Safe II+“ scheint ja perfekt, so haben sie es bereits erkannt. Es gibt jedoch noch eine kleine Herausforderung. Das native Betriebssystem auf diesem Gerät ist nicht Windows, sondern Linux. Für die Referenzimplementierung wurde Ubuntu in der aktuellen LTS-Version (long term support, 18.04.3) gewählt. Es gab verschiedene Gründe für diese Wahl. Eine Referenzimplementierung jeglicher Distribution in allen erdenklichen Kombinationen und die Abdeckung verschiedenster Anforderungen kann bei Bedarf zeitnah zur Verfügung gestellt werden.

Mittlerweile gibt es für die meisten Anwendungen native Linux-Alternativen. Leider gibt es jedoch gegenwärtig noch vereinzelt Hersteller, die noch keine auf Linux lauffähigen Versionen anbieten. Das Gute ist, diese werden immer weniger. Weiterhin steigen die Anzahl und die Qualität der Linux-Alternativen permanent. Sollte jedoch in den nächsten Monaten sich für irgendein Programm keine native Linux-Version besorgen lassen, und es gibt keine geeignete Linux-Alternative und Sie sind gezwungen dieses entsprechende Programm zu verwenden, so gibt es auch eine Lösung.

An der Seite befindet sich eine Schalterkombination. Letztendlich sind dieses über Software auswertbare Bedienelemente. Wird der vordere Schalter beim Systemstart auf I (oben) gestellt (rote Kontroll-LED #5 geht an), so wird in der gegenwärtigen Referenzimplementierung ein vollwertiges

MS-Windows-System in einem Fenster (virtueller Rechner / KVM) gestartet. In einfachen Worten haben Sie jetzt so für dieses eine Programm ein vollwertiges Windows 7 in einem Fenster. Gern können Sie das auch im Vollbildmodus betreiben. Dann ist augenscheinlich kein Unterschied zu einem nativen Windows 7-System zu erkennen. Das virtuelle Windows 7-System ist vorbereitet und hat auch bereits den überwiegenden Teil der Aktualisierungen installiert. Um es zu verwenden, müssen Sie eine gültige Lizenz besitzen und die Installation selbst abschließen und es dann aktivieren.

Es wurde mit Absicht Windows 7 gewählt, da diese Version noch sehr oft im Einsatz ist und auch von verschiedenen Menschen aus verschiedenen Gründen sehr gern noch eine Weile verwendet werden will. Das ist aber auf aktueller Hardware manchmal gar nicht oder nur sehr schwer möglich. In der vorliegenden Konstellation mit dem vorbereiteten virtuellen Windows 7-System ist dieses nahezu ein Kinderspiel.

Wenn Sie Windows 10 verwenden möchten, könnten Sie sich an der Windows 7-System VM (virtuelle Maschine) orientieren. Wenn Sie Windows 7 definitiv nicht benötigen, installieren Sie Windows 10 einfach über die bestehende Installation. Ansonsten macht es eventuell mehr Sinn, sich einfach eine zweite virtuelle Maschine nach entsprechenden Anforderungen zu erstellen.

Theoretisch gibt es auch die Möglichkeit, Windows 7 (oder 10, …) nativ als „dual boot“ zu installieren. Da dieses jedoch nicht komplett zum angestrebten Sicherheitskonzept passt, wird auf Details hier nicht eingegangen. Bei realem Bedarf können jedoch entsprechende Details zur Verfügung gestellt werden.

Anwendungen und Systemaktualisierungen

Dieses System ist perfekt geeignet für Kiosk-Systeme mit ständig wechselnden Benutzern. Aber auch für viele andere Einsatzfälle, z.B. wenn ein Gerät einfach implementiert und dann so in der Form unverändert zuverlässig für lange Zeiträume einfach nur gut funktionieren soll.

So ist das Gerät z.B. sehr gut in kleinen Unternehmen, in denen es keine eigene IT-Abteilung für die regelmäßige Systempflege gibt, einsetzbar. Das System wird aufgesetzt und verrichtet seine Arbeit in unveränderter Form über einen sehr langen Zeitraum.

Aber auch in sehr großen Unternehmen gibt es oft Systeme, die über mehrere Monate oder Jahre mit einer statischen, nicht zu verändernden Konfiguration und Ausstattung betrieben werden sollen. Durch ein einfaches „Zuschließen“ kann dieses dauerhaft gewährleistet werden.

Ein weiteres Einsatzbeispiel ist ein fortschrittliches Computerkabinett in einer Schule. Es ist kein regelmäßiger, unplanbarer Aufwand mehr für die Wiederherstellung von Software und Einstellungen oder das Beseitigen von Viren und so weiter nötig. Jeder Unterricht (heute, in einer Woche, in einem Jahr, …) fängt immer mit dem gleichen definierten Ausgangszustand an. Es gibt eine sehr große Anzahl von Programmen für den täglichen Einsatz in der Bildung. Aber auch für eine Informatik-AG gibt es mächtige Entwicklungsumgebungen, sehr viele Programmiersprachen und nahezu sämtliche „state of the art“ - Software.

Gegenwärtig ist der Einsatz von Linux auf Schulcomputern in Deutschland noch nicht Standard. Dieses System ist eine lohnende Investition und kann die bestehenden und zukünftigen Anforderungen in dieser Richtung mit einem Gerät abdecken.

Dieses System ist perfekt, wenn sie eine bestehende Konstellation einmal am Laufen haben und dann eine unkontrollierte Veränderung des Systems oder der Software, z.B. durch Viren oder Schadsoftware oder ungewollte manuelle Eingriffe über große Zeiträume definitiv ausschließen möchten. Das bedeutet in einfachen Worten, dass sie über einen längeren, von ihnen selbst festgelegten Zeitraum keinerlei Pflege- oder Wartungsaufwand für das Gerät haben. Weiterhin heißt das z.B. auch, dass das Gerät heute in einer vorhersehbaren Zeit X startet. Solange es sich im „abgeschlossenen“ Modus befindet, wird diese Zeit auch morgen, oder in einem Monat oder in 2 Jahren nicht länger. Auch ein lästiges nicht zu verhinderndes Aktualisieren zu unerwünschten Zeiten beim Runter- oder Hochfahren ist nicht notwendig. Solange sich das System im „abgeschlossenen“ Modus befindet, wird es nach jedem Neustart exakt wie vorher sein.

Eventuell nach mehreren Jahren oder nach dem bekannt werden eines realen Problems oder eines nicht zu tolerierenden Features, könnten in einem geplanten Zeitfenster eine Aktualisierung oder andere Änderungen wünschenswert werden. Es sind verschiedene Vorgehensweisen praktikabel:

1. Der Besitzer des Safe-Sicherheits-Schlüssels kann das System „aufschließen“ (den Hardware-Schreibschutz aufheben). Danach kann die Software einfach aktualisiert oder erweitert oder verändert werden. Nach erfolgter Aktion wird das System wieder „verschlossen“ (Hardware-Schreibschutz wird mit dem Safe-Sicherheits-Schlüssel aktiviert). Ab jetzt befindet sich wieder das komplette Betriebssystem in einem unveränderbaren Modus und wird wieder über Monate unverändert gut funktionieren.

2. Eine Aktualisierung einzelner Software-Komponenten oder die Installation von Programmen könnte unter Umständen auch im Safe-Modus erfolgen. Die Änderungen werden jedoch nicht permanent abgespeichert, da ja der Hardware-Schreibschutz eingeschaltet ist. Nach einem Neustart müsste die Aktion wiederholt werden. Bei Bedarf könnte die Änderung auch später zu einem geplanten Zeitpunkt im „temporär aufgeschlossenen Modus“ wiederholt werden um dann auch nach einem Neustart noch aktiv zu sein.

3. Vom Hersteller kann in regelmäßigen Abständen eine aktualisierte Referenz-Implementierung des Systems auf dem leicht auswechselbaren System-Medium bezogen werden. Der Besitzer des Safe-Sicherheits-Schlüssels kann das System „aufschließen“ und NUR im „aufgeschlossenen“ Zustand ohne Werkzeug mit wenigen einfachen Handgriffen das Medium tauschen. Nach dem Verschließen ist das System dann wieder sicher und aktuell. Sollte sich wider Erwarten nach Tagen oder Wochen herausstellen, dass aus irgendeinem Grund noch einmal der vorherige Zustand gewünscht wird, so ist das sehr einfach möglich. Es muss weder über komplizierte Neuinstallation / Restore-Szenarien noch über Wiederherstellungspunkte oder Manipulation von Softwarepaketen nachgedacht werden. Einfach ausschalten, aufschließen, altes Medium wieder rein, zuschließen und es kann weitergearbeitet werden. Bei Bedarf könnte dann die vermutete Unregelmäßigkeit z.B. durch einfaches Einschicken des verdächtigen Mediums zum Hersteller ohne Beeinflussung der lokalen Arbeit analysiert werden.

Da das Betriebssystem sich im Normalfall auf dem schreibgeschützten („abgeschlossenen“) Medium befindet ist auch eine Veränderung durch Viren oder andere Schadsoftware ausgeschlossen. Das System kann all seine Ressourcen zum normalen Arbeiten zur Verfügung stellen. Ein Ausbremsen der Leistung durch ständiges Virenscannen des Betriebssystems gehört auf diesem Gerät der Vergangenheit an.

A4F Safe II+ Technische Details

Basiskonfiguration

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

- 8 GB Hauptspeicher (bis zu 16 GB)

- Integrated Intel® UHD Graphics 600/605

- 32 GB Medium (bis zu 128 GB) mit Hardware-Schreibschutz für System und Software

- 512 GB SSD (2,5 Zoll SATA, leicht austauschbar) für veränderbare Daten

- geräuschlos, da weder Lüfter noch drehende Festplatten installiert sind

- typische Leistungsaufnahme (abhängig vom Nutzungsprofil) ca. 12 Watt

- optional können Abweichungen bei der Bestellung vereinbart werden (z.B. mehr Hauptspeicher, größere SSD, zusätzliche interne M.2 NVMe SSD, 32GB SATA-DOM mit Hardware-Schreibschutz, 32GB M.2 SATA SSD mit Hardware-Schreibschutz, …), bei Fragen kontaktieren Sie bitte den Hersteller

Abmessungen und Gewicht

Breite:	290 mm
Höhe:	47 mm (inkl. 4 mm Gummifüße)
Tiefe:	187 mm
Gewicht:	ca. 2,6 kg

Vorderseite

1. 2x Kontroll-LEDs, ganz links außen, rot oben (#1) + grün unten (#2)

Diese zwei LEDs spiegeln den Zustand des Safe-Sicherheits-Schlosses wider. Im Normalfall sollte die grüne LED an und die rote LED aus sein. Dieses bedeutet, dass das Medium für Betriebssystem und Software durch die Hardware schreibgeschützt ist. In diesem Zustand ist es nicht möglich, das Betriebssystem oder die Software zu verändern. Eventuelle Änderungen können nicht auf das System-Medium geschrieben werden und werden somit beim Ausschalten des Computers verworfen. Für eine geplante Aktualisierung des Betriebssystems oder für die Installation zusätzlicher Software muss der Schreibschutz mit dem Safe-Sicherheits-Schlüssel temporär deaktiviert werden. In diesem Falle erlischt die grüne LED und die rote LED erleuchtet.

2. 2x Kontroll-LEDs, links neben dem Ein- / Aus-Schalter, rot oben (#3) + grün unten (#4)

Die grüne LED zeigt Aktivitäten auf der SSD an. Die Funktion der roten LED ist frei programmierbar. In der Referenzimplementierung (vgl. Absatz Zusatzinformationen Software) wird diese rote LED eingeschaltet, sobald die interne SSD mit mehr als 90 % Daten belegt ist.

3. Ein- / Aus-Taster mit Kontrollleuchte

4. 4x Kontroll-LEDs, rechts neben dem Ein- / Aus-Schalter, rot oben (#5) + grün unten (#6) & rot oben (#7) + grün unten (#8)

Diese vier LEDs spiegeln den Zustand der per Software abfragbaren Schalter an der rechten Seite (I = rot, II = grün) wider. In der Referenzimplementierung wird nur beim Starten des Computers überprüft, ob der vordere Schalter sich in Position I befindet (nur die entsprechende rote LED #5 ist an). Ist dieses der Fall, wird automatisch eine vorbereitete virtuelle Windows-Maschine gestartet. Wenn diese verwendet werden soll, müssen sie eine entsprechende Windows-Lizenz besitzen und die Windows-Installation selbst fertigstellen und dementsprechend aktivieren. Es wird empfohlen, die „normalen Sachen“ mit den nativen Anwendungen zu erledigen und das virtuelle Windows-System nur bei fehlenden Alternativen zu verwenden.

5. 2x USB 3

6. Analog Audio (Headphone Out/links & Microphone In/rechts)

Zur Beachtung. Die vorstehende LED-Beschreibung ist bereits auf die ab 2020 optional erhältliche Zweischalter-Version angepasst. Die aktuelle Version hat nur kleine Abweichungen (#4 = HDD; #3, #5, #6 = frei programmierbar; #7 rot an, wenn Schalter hinten/I, WindowsVM; #8 grün an, wenn Schalter vorn/0, keine Aktion)

Seiten / rechts & links

An der rechten Seite befinden sich mittels Software abfragbare mechanische Schalter. Der Zustand wird zusätzlich an der Front über die LEDs rechts neben dem Ein- / Aus-Schalter angezeigt.

An der linken Seite ist das Safe-Sicherheits-Schloss angebracht. Der Zustand ist an den vorderen linken LED‘s (#1 & #2) zu erkennen (Rot/#1 = Hardwareschreibschutz ist aus = Veränderungen am System sind z.B. geplant und möglich **ODER** Grün/#2 = Hardwareschreibschutz ist an = keine permanenten Änderungen möglich = SICHER)

Rückseite

1. Optional 1 bis 2 WLAN-Antennen

2. Stromversorgungsanschluss (8-24 Volt, wide range)

Um die Servicefreundlichkeit zu erhöhen wurde bewusst ein Mainboard mit externer Stromversorgung gewählt. Weiterhin wird wegen des relativ breiten Eingangsspannungsbereiches die Abhängigkeit von spezifischen kostenintensiven Netzteilen beseitigt.

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-Sicherheits-Verschlussklappe; dahinter das schreibgeschützte herausnehmbare Medium für Betriebssystem und Software und die separate leicht herausnehmbare SSD für Benutzerdaten

Gehäuse

- das Gehäuse besteht aus kräftigem Aluminium mit präzise gefrästen Details

- die internen Wärmeleitsysteme sind im Hause entwickelt und präzisionsgefertigt

- auch zur Wandmontage geeignet

- zur Diebstahlsicherung befindet sich an der rechten Seite eine Aufnahme für ein „Kensington-Lock“

- optional ist eine Unterstützung für ein senkrechtes Aufstellen erhältlich

- optional kann der an der Vorderseite verfügbare Platz mit eigenem Logo versehen werden

- optional kann die Montage einer separat erhältlichen VESA-Halterung vorbereitet werden

- das System ist in verschiedenen wohl gewählten Oberflächen- und Farbkombinationen erhältlich; optional kann die Farbe mittels RAL-Code frei gewählt und somit den eigenen Bedürfnissen angepasst werden

Mainboard

Das Mainboard wurde in Deutschland entwickelt und hergestellt. Nachfolgend gibt es ein paar erwähnenswerte Hinweise.
- 1x M.2 Key M Sockel (max. 2230), wird für Wifi/BT verwendet
- 1x M.2 Key B Sockel (max. 2280 bzw. 2260, oder 2242), Key B; SATA and PCIe x1, Key B and Key B+M modules useable (z.B. Intel OptaneTM SSD 800P-Serie, bootbar, …)

Einschränkungen (engl., direkt vom Hersteller):

- 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

Zusatzinformationen Software

Beim Betriebssystem und der installierten Software handelt es sich um eine angepasste Standard-Installation der aktuellen Ubuntu LTS Version (long term support, 18.04.3). Die vorgenommenen Änderungen sind auf dem System nachvollziehbar.

Der Kaufpreis deckt vollständig die komplette Hardware und einen geringen Teil der Entwicklungskosten ab. Weiterhin wird ein Teil für die Weiterentwicklung der spezialisierten Hardware und ein zukünftiges Bereitstellen einer jeweils weiterentwickelten und aktualisierten Referenzimplementierung verwendet. Dieses kommt allen bestehenden Kunden zugute.

Das Betriebssystem und die installierte Software gibt es ohne Zusatzkosten als Referenzimplementierung. Werden in Zukunft andere Referenzimplementierungen entwickelt, können diese von bestehenden Kunden vom Hersteller bezogen werden.

Es gibt für dieses System mindestens einmal im Jahr eine auf der jeweils aktuellen Ubuntu LTS Version basierende Referenzimplementierung. Dieses ist für einen Zeitraum von mindestens 5 Jahren ab Kaufdatum gewährleistet. Sie kann von bestehenden Kunden vom Hersteller bezogen werden.

Das Betriebssystem und die installierte Software können nach temporärem „Aufschließen mit dem Safe-Sicherheits-Schlüssel“ manuell oder automatisch aktualisiert werden. Dazu können die gängigen Mechanismen des Distributors Verwendung finden. Weiterhin sind so auch eventuell gewünschte Anpassungen und das Installieren zusätzlicher Software ohne Probleme möglich. Bei besonderen, klar definierbaren Anforderungen können der Hersteller oder entsprechende Partner Unterstützung anbieten.

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+ Denkanstöße

Lesen Sie nicht unbedingt weiter, wenn Sie sich bereits für dieses System entschieden haben. Falls Sie noch nicht ganz sicher sind, mag es noch den einen oder anderen Denkanstoß geben.

Wenn ich ein funktionierendes System habe und es all meine Anforderungen erfüllt, warum soll ich es dann täglich aktualisieren und sporadisch und unkontrollierbar Funktionen hinzufügen, entfernen oder ändern? Ist es nicht viel besser, das System einfach in diesem Zustand zu belassen und Änderungen auszuschließen (das Gerät zu „verschließen“)? Macht es nicht auch Sinn, exakt die Zeitfenster zu kennen, wann Änderungen des Systems geplant durchgeführt wurden? Ist es nicht auch schön, wenn ich mit wenigen Handgriffen (Austausch des System-Mediums gegen eine aktuelle Referenzimplementierung oder gegen ein selbst erzeugtes Backup-Medium) ein komplett aktuelles System habe oder jederzeit auf den entsprechenden Stand zurückgehen kann?

Angenommen, ich spiele seit längerem mit dem Gedanken, mir ein Windows in einer virtuellen Maschine zuzulegen. Ich habe einen Teil der unschlagbaren Argumente verstanden, konnte mich jedoch noch nicht für eine Lösung entscheiden. Wenn Geld keine Rolle spielt, ist VMware sicherlich eine sehr gute Wahl. Wenn ich die komplette VM (virtuelle Maschine) jedoch bereits komplett vorbereitet (zur Verwendung oder auch als Beispiel für das Erstellen weiterer VMs) mit dem „A4F Safe II+“ in der Referenzimplementierung erhalte, dann kann KVM eine sehr gute Wahl sein. In der vorgegebenen Konstellation ist die Windows-VM im Wesentlichen nur eine Konfigurations- und eine Festplatten-Datei. Ist die VM ausgeschaltet, kann man innerhalb weniger Minuten eine komplette Kopie vom vollständigen Windows-System erstellen und hätte so auch eine Möglichkeit, dieses Windows-System innerhalb weniger Minuten komplett wiederherzustellen.

Es wurden bereits für verschiedene Kunden spezielle Konfigurationen entwickelt, welche zusätzlich einen sicheren Schutz der Benutzer-Daten ermöglichen. Wenn Sie besondere Anforderungen haben, so setzten Sie sich bitte mit einer entsprechenden Definition mit dem Hersteller in Verbindung.

Gesellen Sie sich zu den Menschen, die ein Computersystem einfach nur als Werkzeug (oder Spielzeug oder Arbeitsmittel etc.) und einfach nur zuverlässig verwenden möchten. Machen Sie sich keine Sorgen mehr vor einer ungewollten Veränderung des Betriebssystems und seiner Komponenten. Vorbei sind die Ängste, dass im Hintergrund oder beim Neustarten oder Ausschalten etwas am System „verdreht“ wird. Es wird keine unpassenden Zeitpunkte mehr geben, an denen man versucht zu verstehen, wer denn heute was von wem warum verändert hat und warum der Unterschied zwischen Theorie und Praxis in der Praxis meistens viel größer ist.

Vielen Dank auch an die Oerties GmbH (www.oerties.com)