EDP
IT-PRODUCTS

19“-Schranklöschsysteme

Lösung für Server- und Netzwerkracks

Einsatzgebiete:

- Serverracks
- Netzwerkschränke
- Telekommunikation

Vorteile:

- Selbstmontage möglich
- Kompakte Bauweise mit nur 3HE
- Wartungsfreundlich
- Einfache Bedienung
- Leichtes Wiederherstellen nach Auslösung
- In beinahe jedem Schrank einsetzbar
- Mit einer Anlage können mehrere Schränke versorgt werden

Optionen:

- SNMP Alarmierung
- Weitere Rauchmelder und Löschgeneratoren zur Schutzbereichsvergrößerung
- Generatoren-Kits zur Wiederinbetriebnahme nach Auslösung

CE

Einbaubeispiel

19“-Schranklöschsysteme

Lösung für Server- und Netzwerkracks

Funktion:

Zwei Rauchmelder steuern die Auslösung der Löschanlage. Sollte ein Rauchmelder ansprechen, wird ein Voralarm über eine LED Anzeige ausgegeben.

Löst ein weiterer Rauchmelder aus, wird nach Ablauf einer Zeitverzögerung ein Hauptalarm ausgegeben und die Auslösung der Löschanlage aktiviert. Nach Auslösung wird der Löschbereich mit Löschaerosol geflutet. Über einen Zeitraum abhängig der Löschbereichsdichte (empfohlen IP54) wird das Löschmittel im Löschbereich bleiben und sofort jeden Brand komplett löschen.

Nach der Löschung kann der Schrank geöffnet werden und das Löschmittel verflüchtigt sich im Raum und kann zum Beispiel über ein geöffnetes Fenster ins Freie geleitet werden.
Nach einem Reset durch die Taste an der Löschanlage, können die Aerosol Löschgeneratoren einfach abgesteckt und neue angesteckt werden. Die Anlage ist sofort wieder voll funktionstüchtig.

Eine Deaktivierung der Anlage über einen Türkontaktschalter ist möglich. Dieser stellt sicher, dass die Anlage unscharf ist, wenn eine Türe im Schrank geöffnet ist.

Löschaerosolfunktion:

Aerosol-Löschanlagen arbeiten mit einer festen, aerosolbildenden Verbindung, die sich nach Aktivierung in ein schnell expandierendes, trockenes Löschaerosol auf der Grundlage von Kaliumverbindungen umwandelt.

Nach Auslösung wir das Löschmittel auf Mikro partikel-Basis verteilt und freigesetzt. Das Aerosol bekämpft und löscht das Feuer nicht durch Erstickung (Wegnahme von Sauerstoff) oder Kühlung, sondern durch Hemmung der chemischen Verbrennungsreaktion auf Molekularbasis.
Durch dieses Verhalten ist es möglich, mit äußerst geringen Löschmengen Feuer zu löschen.

Vorderansicht im Detail

Rückansicht mit Löschgenertoren

Monitoring Unit VT825+

The unit is used in data centers, remote & industrial facilities, oices. Can connect up to 30 sensors, 12 dry contacts, two 12V alarm beacons, GSM modem, USB-cam, SD card, 1-Wire board (instead of VT18) for reader connection. There are built-in servers and agents like HTTP, HTTPS, SNMP v1, 2c, 3, SMTP, Radius, Syslog, FTP, DHCP, Watchdog.

Connectable Sensors

- Analog sensors
- CAN sensors
- 1-Wire sensors
- AC / DC meters

Virtual sensors and elements

- Group, E-mail, SNMP trap, SNMP Get, SMS, IP cams, PINGs, Triggers, Timers

Notiications

- E-mail, SMS, Syslog, Event log, SNMP Trap, SNMP Get

Device management

- Web, SNMP, manually via SMS (using external USB modem)

Network protocols

- DHCP, HTTP, HTTPS, SNMP, SMTP, SSL, FTP, Syslog, CAN, Get SNMP, TLS
- RADIUS access with Login
- Supports SNMP v.1, v.2c, v.3

Web interface

- Sensor graphing
- Multi language support
- User Access and Permissions
- Conigurable embedded logic

Alert types

- FTP, Syslog, SMTP or SNMP, SMS (Using external USB modem)

Built-in functions

- Built-in clock time synchronization
- Built-in watchdog timer

Extensions

- GSM modem (VT700)
- Extension board (VT10)

Support & Origin

- 2 Year warranty (extended possible)
- Manufactured in E.U.

Processor	ARM926EJ 300MHz
Operating system	Linux 3.10.32
Memory	ROM: 512 Mbit NAND Flash, RAM 64 Mb
Inputs	CAN open port for digital sensors x8 AutoSense RJ-12 ports x12 dry contact inputs
Outputs	x2 12V 0.25A outputs x2 loads (latching relays with LEDs indicators)
LED status indicators	Power, Network, Relays & Error, CAN
Network interface	Ethernet 10-100 Mbit/s
Built-in sensors	Temperature sensor (1%) Power supply voltage sensor (1%)
Other connectors	USB (for camera, modem or Flash)

Power requirements	90-240V, IEC C14, Fuse 2A
Power consumption	12 Watt, 2 A
Operating temperature	Min. -10° C, Max. +80° C
Operating humidity	Humidity : Min. 5%, Max. 80% (Non-Condensing)
Dimensions	440 x 44.45 x 79.4 mm
Mounting	19" Rack mount (1U), Desktop (Rubber foot included) Wall mounting using VT112
Expansion devices	VT10 / 1-Wire Board (ordered separately)
Weight	1.5 kg
Other	External enclosure earthing, 12V DC power backup terminal

Rack Monitoring Solution

Computer room servers, rack mounted equipment and cabinets are an expensive asset in IT infrastructure. It is imperative to insure that the rack and it's equipment are performing fault-free, and as eicient as possible. With Vutlan monitoring systems and sensors, it is easy to evaluate environmental data in a straightforward way to prevent failure of equipment.

Sensor extension unit

VT408 allows to increase the number of sensors connected to any monitoring unit. Adds up to 8 sensors.

Vibration sensor

VT540 detects vibration.

Monitoring unit

VT805 / Environmental monitoring unit actively monitors the conditions in your rack, alert and notify facility managers.

GSM modem

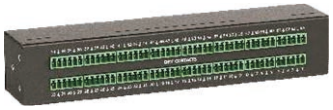
VT700 is needed when LAN is absent for sending SMS and voice messages.

Rack control unit

VT430 includes an access sensor for rack door control, x2 dry contacts for side walls, temperature and humidity sensors.

Sensor extension unit

VT408 allows to increase the number of sensors connected to any monitoring unit. Adds up to 8 analog sensors.



Dry contacts unit

VT440 adds 32 or 64 dry contacts inputs.

AC voltage monitor

VT520 is needed for measurement of AC 90-250V.

Software scalability options

Tables below depict the most common general software scalability options available for Vutlan monitoring unit.

Web interface

- Full monitoring and control over IP
- 3-Tier user access
- Time synchronization
- Day / night cycles
- Seasonal time setup
- Multi language interface
- System & Group trees
- Dashboard and stats
- Dry contacts panel
- Outlets / Relays panel
- Event log panel
- Logic scheme panel
- Access panel
- Graphs panel

Cameras

- IP cameras
- USB camera
- Send JPEG stream on event

SNMP agents

- Supports SNMP v1, v2c, v3
- Infrastructure monitoring program NagiosQL
- Nagios plugins
- Infrastructure monitoring program OpenNMS

Logs

- Logs, sensor data, coniguration elements
- FTP, Syslog server export
- Syslog server export
- Export sensor data in XML or CSV format
- Save logs to SD card or disk
- RSS export

Networking

- DynDNS
- RADIUS

Sensors

- 4-level threshold controls
- Plug & Play
- Formulas to adjust sensor values
- Graphs and Multi-graphs
- Sensor data import

Equipment control

- Relay switching
- Outlet switching
- Change state by SMS
- Change impulse by SMS

Virtual sensors

- PING
- Timer
- Logic schemes

Backup

- Logs export
- Daily backup of settings on FTP

Notiications

- E-Mail
- SNMP trap
- SMS notiications
- SNMP get

Access

- User keys
- Access GUI panel

Control by SMS

- Read sensor data
- Set state of relay / outlet
- Set impulse of relay / outlet
- Program to send SMS from PC

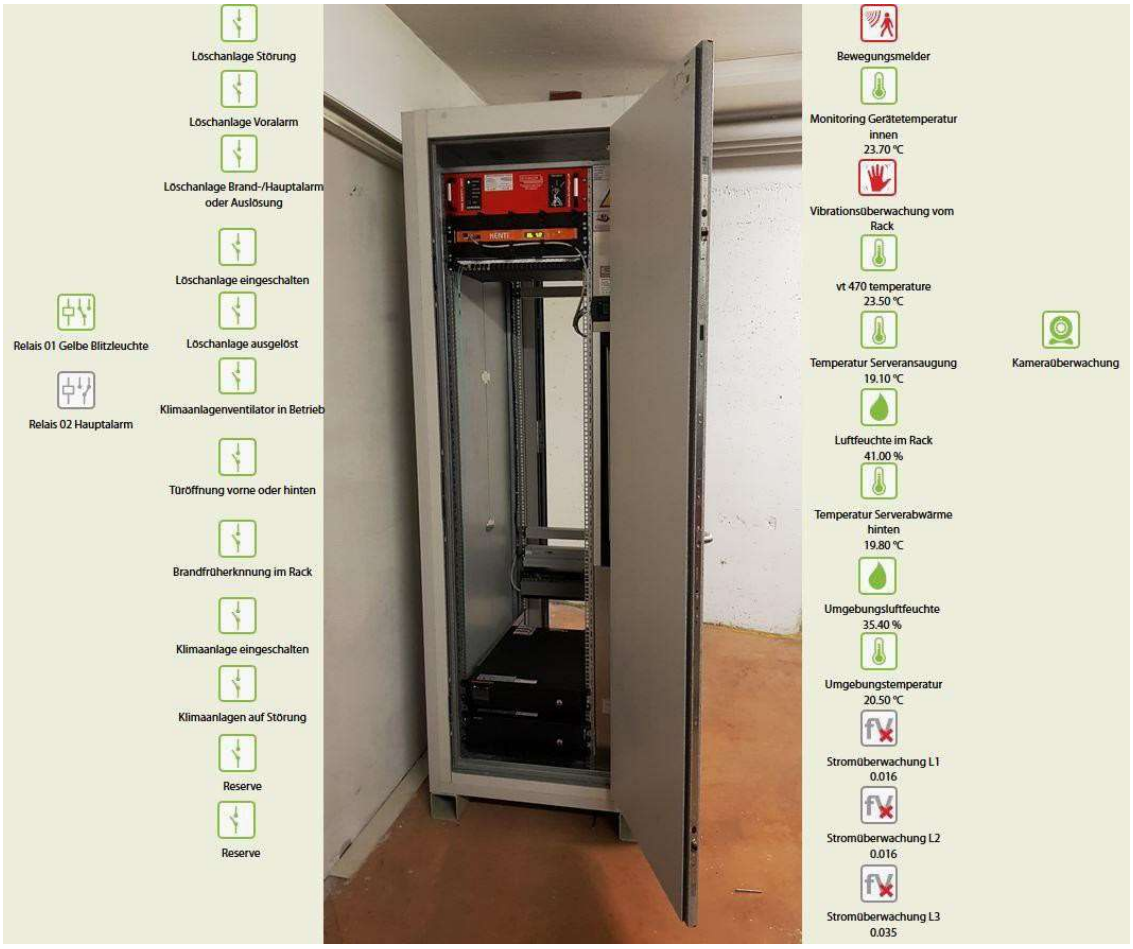
Other

- Upgrade via USB, FTP or HTTP
- Clone settings of multiple systems using “Duplicator” software

Unterschiede einer Brandvermeidung zu einer Aerosol Brandlöschung im Serverschrank!

	Brand-vermeidung	**Brand-löschung**
Vorbeugender höchster Brandschutz aller Systeme	JA	NEIN
Permanete sauerstoffreduzierte Atmosphäre im Schrank 15% O^2	JA	NEIN
Erhöhte Rauchgasentwicklung im Brandfall	NEIN	JA
Rückstände durch die entstandenen Brandrauchgase	NEIN	JA
Erneuerung des Löschmittels und Rauchmelder nach Auslösung	NEIN	JA
Erneuerung der Löschgeneratoren nach Ablaufdatum	NEIN	JA
Arbeitsschutz und Personenschutzgesetze zu beachten	NEIN	JA
Überdruckklappen notwendig	NEIN	NEIN
Entstehende Flusssäure bei Löschung	NEIN	NEIN
F-Gasverordnung	NEIN	NEIN
EN Zertifikate	JA	JA
GWP	0	0
ODP	0	0
ALT	0	unerheblich
Leitfähigkeit	keine	keine
Toxisch	NEIN	NEIN
Schutzbereiche abgedichtet bei Auslösung	JA	JA
Korrosiv	NEIN	NEIN
Rohrleitungen notwendig	NEIN	NEIN

Ansicht: SMARTRACK Monitoring nach IT-Grundschutz inklusive Serverraumkamera




FIRE SAFETY UNIT
AEROSOL

Vorgaben vom BSI.

INF.2.A1 Festlegung von Anforderungen [Planer, IT-Betrieb, Informationssicherheitsbeauftragter (ISB), Haustechnik]

Für ein Rechenzentrum MÜSSEN angemessene technische und organisatorische Vorgaben definiert und umgesetzt werden.

Wenn ein Rechenzentrum geplant wird oder geeignete Räumlichkeiten ausgewählt werden, MÜSSEN potenzielle Gefährdungen durch Umgebungseinflüsse sowie das Sicherheitsniveau der IT-Komponenten (insbesondere Verfügbarkeit) mitbetrachtet werden. Weiterhin MÜSSEN auch Schutzmaßnahmen vor potenziellen internen und externen Angriffen in die Gesamtbetrachtung einfließen.

Ein Rechenzentrum MUSS insgesamt als geschlossener Sicherheitsbereich konzipiert werden. Es MUSS zudem unterschiedliche Sicherheitszonen aufweisen. Hierfür MÜSSEN Verwaltungs-, Logistik-, Technik- und IT-Flächen klar voneinander getrennt werden. Im Falle eines Serverraums SOLLTE geprüft werden, ob unterschiedliche Sicherheitszonen umsetzbar sind.

Auch MUSS darauf geachtet werden, dass Versorgungsleitungen (z. B. für Wasser oder Gas) möglichst nicht in unmittelbarer Nähe von schutzbedürftigen Technikkomponenten verlaufen. Vorhandene Versorgungsleitungen MÜSSEN zumindest an den kritischen Stellen regelmäßig überprüft werden, ob sie noch dicht sind.

INF.2.A2 Bildung von Brandabschnitten [Planer]

Es MÜSSEN geeignete Brandabschnitte für die Räumlichkeiten eines Rechenzentrums festgelegt werden. Schutzziel für die Brandwand bzw. den Brandabschnitt MUSS nicht nur der Personen- und Gebäudeschutz, sondern auch der Schutz des Inventars und dessen Verfügbarkeit sein. Somit MUSS nicht nur verhindert werden, dass sich ein Brand durch Flammen und heiße Rauchgase ausbreitet, sondern es MÜSSEN auch die Wärmestrahlung und die Ausbreitung von kaltem Rauch blockiert werden. Im Falle eines Serverraums SOLLTE geprüft werden, ob geeignete Brandabschnitte für die Räumlichkeiten umsetzbar sind.

INF.2.A3 Einsatz einer unterbrechungsfreien Stromversorgung [Haustechnik]

Für alle betriebsrelevanten Komponenten des Rechenzentrums MUSS eine unterbrechungsfreie Stromversorgung (USV) installiert werden. Da der Leistungsbedarf von Klimatisierungsanlagen oft zu hoch für eine USV ist, MUSS aber mindestens die Steuerung der Anlagen an die unterbrechungsfreie Stromversorgung angeschlossen werden. Im Falle eines Serverraums SOLLTE je nach Verfügbarkeitsanforderungen der IT-Systeme geprüft werden, ob der Betrieb einer USV notwendig ist.

Die USV MUSS ausreichend dimensioniert sein, sodass alle Komponenten bei einem Ausfall der Versorgung so lange mit Strom versorgt werden, dass kein Datenverlust entsteht.

Bei relevanten Änderungen MUSS überprüft werden, ob die vorhandenen USV-Systeme noch ausreichend dimensioniert sind. Die Batterie der USV MUSS im erforderlichen Temperaturbereich gehalten werden und vorzugsweise in einem getrennten Bereich platziert sein.

Die USV MUSS regelmäßig gewartet und auf Funktionsfähigkeit getestet werden. Dafür MÜSSEN die vom Hersteller vorgesehenen Wartungsintervalle eingehalten werden *(*siehe *INF.2.A10 Inspektion und Wartung der Infrastruktur)*. Um sicherzustellen, dass die USV die erforderliche Stützzeit bereitstellt, MUSS regelmäßig sowie zusätzlich, wenn sich bei den Verbrauchern etwas ändert, die tatsächliche Stützzeit ermittelt werden.

Wenn IT-Geräte über eine USV versorgt werden, DÜRFEN diese NICHT über geschirmte Leitungen mit weiteren IT-Geräten verbunden werden.

INF.2.A4 Notabschaltung der Stromversorgung [Haustechnik]
Für den Notfall MUSS es geeignete Möglichkeiten geben, das Rechenzentrum spannungsfrei zu schalten. Dafür SOLLTE beispielsweise ein Not-Aus-Schalter installiert werden. Ein solcher Schalter MUSS nicht nur die externe Energieversorgung abtrennen, sondern auch die komplette USV-Anlage abschalten. Alle Not-Aus-Schalter MÜSSEN so geschützt sein, dass sie nicht unbeabsichtigt betätigt werden können.

INF.2.A5 Einhaltung der Lufttemperatur und -feuchtigkeit [Haustechnik]
Um IT-Systeme entsprechend den Hersteller-Empfehlungen zuverlässig betreiben zu können, MUSS sichergestellt werden, dass die Lufttemperatur und Luftfeuchtigkeit im IT-Betriebsbereich innerhalb der vorgeschriebenen Grenzen liegen.
Die tatsächliche Wärmelast in den gekühlten Bereichen MUSS in regelmäßigen Abständen und nach größeren Umbauten durch Berechnung oder Messung überprüft werden.
Auch MUSS eine eventuell vorhandene Klimatisierungseinrichtung regelmäßig gewartet werden.
Wenn die beiden Parameter "Temperatur" und "Feuchtigkeit" vom Normwert abweichen, MÜSSEN sie über eine repräsentative Dauer hinweg in einem der Situation angepassten Zeitintervall aufgezeichnet werden.

INF.2.A6 Zutrittskontrolle [IT-Betrieb, Informationssicherheitsbeauftragter (ISB), Haustechnik]
Für den Schutz gegen unbefugten Zutritt zu einem Rechenzentrum MUSS es eine Zutrittskontrolle geben.
Durch eine auf die jeweiligen Erfordernisse abgestimmte Zutrittsregelung MUSS für eigene Mitarbeiter und für nur zeitweilig Beschäftigte sichergestellt werden, dass sie keinen Zutritt zu IT-Systemen außerhalb ihres Tätigkeitsbereiches erhalten.
Außerdem MUSS sichergestellt werden, dass Besucher und Fremdpersonal während aller Arbeiten im Rechenzentrum von der Zutrittskontrolle individuell erfasst sowie beaufsichtigt werden.
Zudem MÜSSEN alle Zutrittsmöglichkeiten zu einem Rechenzentrum überwacht werden. Die Anforderungen der Institution an ein Zutrittskontrollsystem MÜSSEN in einem Konzept ausreichend detailliert dokumentiert werden. Im Falle eines Serverraums SOLLTE geprüft werden, ob eine Überwachung aller Zutrittsmöglichkeiten sinnvoll ist.
Weiterhin MUSS geregelt werden, welche internen und externen Personen für welchen Zeitraum Zutritt erhalten. Dabei MUSS sichergestellt sein, dass keine unnötigen oder zu weitreichenden Zutrittsrechte vergeben werden. Es MUSS regelmäßig kontrolliert werden, ob die Regelungen zum Einsatz einer Zutrittskontrolle eingehalten werden.

INF.2.A7 Verschließen und Sichern [Mitarbeiter, Haustechnik]
Alle Türen des Rechenzentrums MÜSSEN stets verschlossen gehalten werden. Fenster sind möglichst schon bei der Planung zu vermeiden. Falls sie doch vorhanden sind, MÜSSEN sie ebenso wie die Türen stets verschlossen gehalten werden. Türen und Fenster MÜSSEN einen dem Sicherheitsniveau angemessenen Schutz gegen Angriffsversuche und Umgebungseinflüsse (z. B. Feuer und Rauch) bieten. Hierbei ist zu beachten, dass die bauliche Ausführung aller raumbildenden Elemente in Bezug auf die Sicherheit, vor allem hinsichtlich der Sicherheitszonen, gleichwertig sein MUSS.

INF.2.A8 Einsatz einer Brandmeldeanlage [Planer]
In einem Rechenzentrum MUSS eine Brandmeldeanlage installiert werden. Diese MUSS alle Flächen überwachen. Alle Meldungen der Brandmeldeanlage MÜSSEN geeignet weitergeleitet werden (siehe dazu auch INF.2.A13 *Planung und Installation von Gefahrenmeldeanlagen*). Die Brandmeldeanlage MUSS regelmäßig gewartet werden. Es MUSS sichergestellt werden, dass in Räumen, die im Brandabschnitt des Rechenzentrums liegen, keine besonderen Brandlasten vorhanden sind.

INF.2.A9 Einsatz einer Lösch- oder Brandvermeidungsanlage [Planer]
In einem Rechenzentrum MUSS eine Lösch- oder Brandvermeidungsanlage nach aktuellem Stand der Technik installiert sein.
In Serverräumen SOLLTEN hierfür Handfeuerlöscher in ausreichender Zahl und Größe benutzt werden. Die Feuerlöscher MÜSSEN so angebracht werden, dass sie im Brandfall leicht zu erreichen sind. Jeder Löscher MUSS regelmäßig inspiziert und gewartet werden, um die Funktionsfähigkeit im Ernstfall zu gewährleisten. Alle Mitarbeiter MÜSSEN in die Benutzung der Handfeuerlöscher eingewiesen werden.

INF.2.A10 Inspektion und Wartung der Infrastruktur [IT-Betrieb, Haustechnik, Wartungspersonal]

Für alle Komponenten der technischen Infrastruktur MÜSSEN mindestens die empfohlenen oder durch Normen festgelegten Intervalle und Vorschriften für Inspektion und Wartung eingehalten werden. Um nachvollziehen zu können, wann welche Arbeiten durchgeführt wurden, MÜSSEN Inspektionen und Wartungsarbeiten protokolliert werden.

Kabel- und Rohrdurchführungen durch Brandwände MÜSSEN regelmäßig daraufhin geprüft werden, ob die Schotten normgerecht und unversehrt sind. Die Ergebnisse MÜSSEN dokumentiert werden.

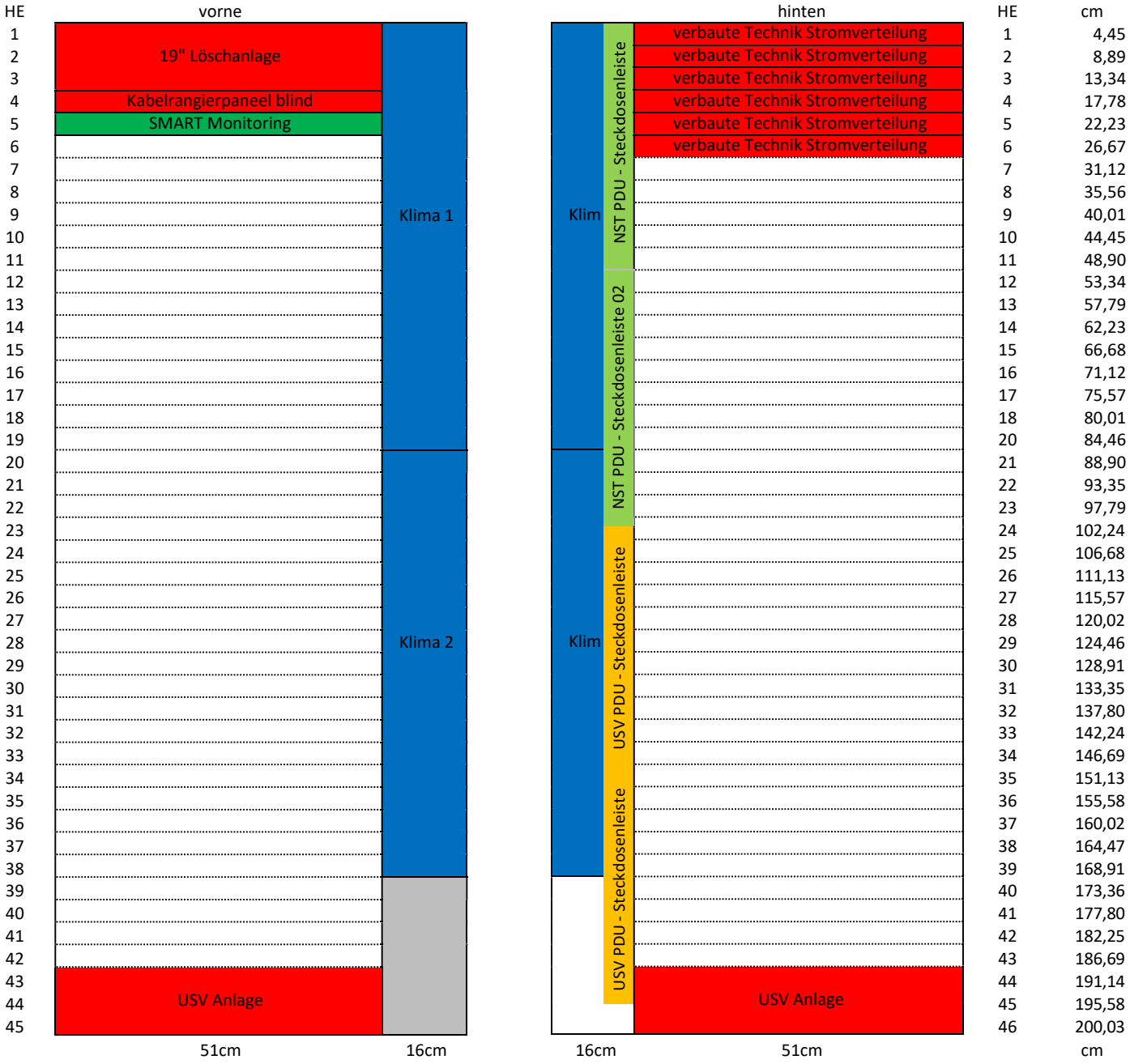
INF.2.A11 Automatisierte Überwachung der Infrastruktur [IT-Betrieb, Haustechnik]

Alle Störungsmeldungen der Infrastruktur, z. B. Leckageüberwachung, Klima-, Strom- und USV-Anlagen, MÜSSEN automatisiert überwacht und schnellstmöglich in geeigneter Weise weitergeleitet werden, z.B. über ein Monitoringsystem.

Im Falle eines Serverraums SOLLTEN IT- und Supportgeräte, die nicht oder nur selten von einer Person bedient werden müssen, mit einer Fernanzeige für Störungen ausgestattet werden. Die verantwortlichen Mitarbeiter MÜSSEN zeitnah alarmiert werden.

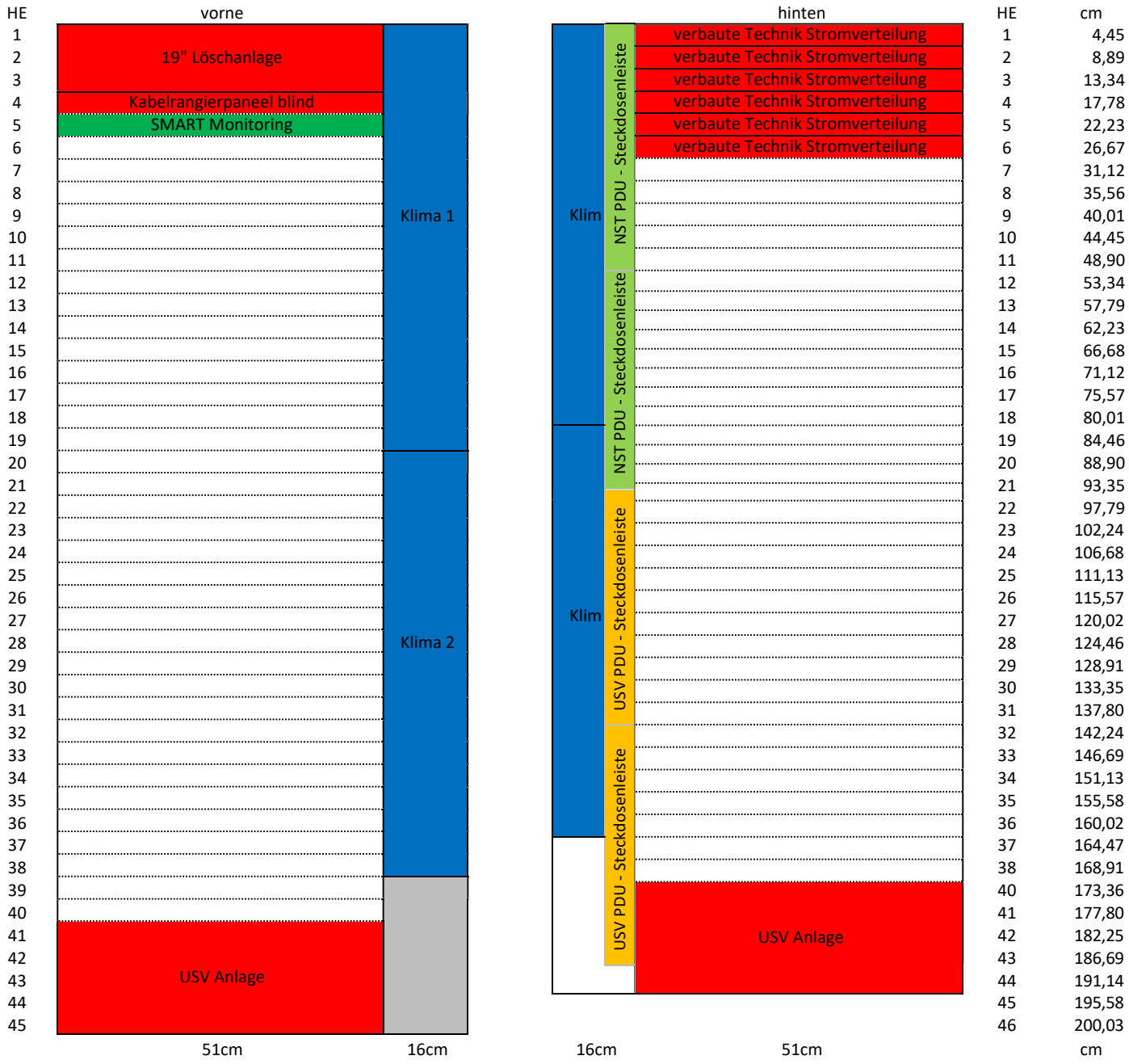
Übersicht: Höheneinheiten SMARTRACK IP54 SMARTR4.01

Projekt: SMARTRACK IP54, **4,3kW** einfache oder redundante Klimatisierung, **19" Löschanlage**



Projekt: SMARTRACK IP54, 5,9**kW** einfache oder redundante Klimatisierung, **19" Löschanlage**

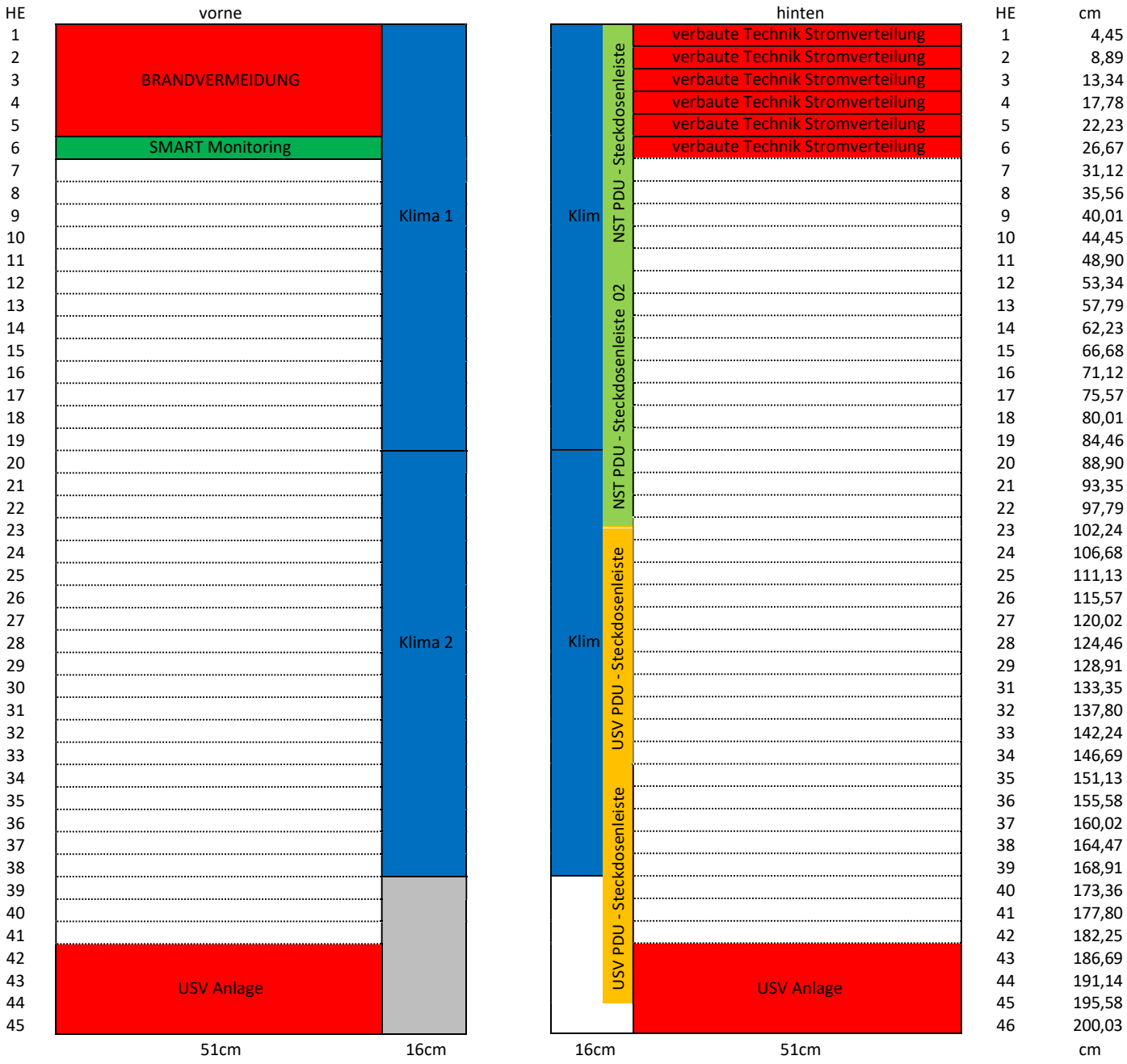
SMARTR4.02



HE	cm
1	4,45
2	8,89
3	13,34
4	17,78
5	22,23
6	26,67
7	31,12
8	35,56
9	40,01
10	44,45
11	48,90
12	53,34
13	57,79
14	62,23
15	66,68
16	71,12
17	75,57
18	80,01
19	84,46
20	88,90
21	93,35
22	97,79
23	102,24
24	106,68
25	111,13
26	115,57
27	120,02
28	124,46
29	128,91
30	133,35
31	137,80
32	142,24
33	146,69
34	151,13
35	155,58
36	160,02
37	164,47
38	168,91
40	173,36
41	177,80
42	182,25
43	186,69
44	191,14
45	195,58
46	200,03

Projekt: SMARTRACK IP54, **4,3kW** einfache oder redundante Klimatisierung, **Brandvermeidung**

SMARTR4.03



Projekt: SMARTRACK IP54, 5,9**kW** einfache oder redundante Klimatisierung, **Brandvermeidung**

SMARTR4.04