

Cybersecurity and “kill switches”

© **Rob Hulsebos**

Version 11 June 2025

Introduction

In the beginning of 2025, there were rumours that the F-35 fighter plane had a “kill switch”, theoretically allowing the plane to be disabled upon the whims of the US. Earlier in 2024 there was also a mention of a kill switch present in the very advanced semiconductor machines of ASML installed in Taiwan, with the purpose of remotely disabling these machines in the event of a Chinese invasion.

In both cases, the presence of such kill switches is theoretical. There would probably be easier ways to disable planes and machines. Also, the presence of a kill switch that can be activated remotely is a huge cybersecurity risk in itself; if its protection is breached an adversary could toggle the switch too.

Of course, a kill switch in the equipment above would not be a physical switch. But: physical switches to disconnect networks *do* exist! Not for military purposes, but for many applications where it is wanted to disconnect equipment (or complete networks) for various reasons.

The latest equipment with kill switches is rumoured to be: solar panel inverters.

The ‘kill switch’: solar panels as secret weapons

Secret ‘kill switches’ in Chinese solar panels pose a risk to our energy grid. Experts are sounding the alarm.

Published on May 28, 2025



Source: [ioplus.nl](https://www.ioplus.nl)

Different usage

In the examples above, a kill switch is a name for an electronic circuit meant to disable a certain type of device, either temporarily or permanently. It probably is not a physical switch as we know it (like used in your home to turn the lighting on/off).

But there is another type of kill switch, which may more resemble a switch. It is meant to disconnect a network, i.e.. from internet, or to disconnect a device from a network. There is **no** damage done; just no network communication is possible for as long as the kill switch is activated. For cybersecurity purposes, this can have good benefits.

Disconnecting networks and equipment

In cybersecurity, it is often mentioned that an "air gapped" network is the best protection to keep hackers out. But nowadays, real air gapped networks are scarce, for various reasons:

- Cloud access is needed
- Software updates must be downloaded
- Software tools want to check their license validity
- Internet access is needed by staff
- Remote diagnose access requested/demanded by vendors
- ...

Of course, various protective measures (firewalls, DMZ's, endpoint protection, zero trust, etc.) is possible to increase the level of protection, but... a certain risk remains. In some cases, a data-diode can help, allowing network traffic in one (outgoing or incoming) direction, but many network protocols cannot work over a data-diode.

A completely different way of thinking is to have an air-gap. But then sometimes we still want to communicate. For example, a back-up server can be kept (network-wise) offline, but brought online when back-ups are to be written (or read back), and later brought offline again when done. In this case, a ransomware malware that wants to encrypt all back-up server cannot reach it. By using a kill switch, the network communication can be enabled when needed, and later disables again.

Temporarily disconnecting

Crypto-key management systems play a vital role in having a secure digital communication environment. A hackers that can issue his own certificates, or can get access to a master certificate, allows his malware to be installed and/or trusted. Such systems are therefore best left offline for as long as possible.

Another reason to decouple a (part of a) network is in case of emergencies. Some malwares can spread very quickly, there is often not enough time to pull cables, or travel to remote locations. Just switching off equipment can help to contain malware, but may also cause damage to systems (especially in OT) or hurt people.

How to disconnect

For cybersecurity, nothing beats a physically disconnected network. Of course this can be done by plugging cables, but this is not reliable – someone can plug them in again "just for 5 minutes" and then forget to unplug it again. It also increases wear & tear on cables and connectors, which are not made for many plug/unplug cycles. Also, someone must be present in the vicinity of the equipment; it cannot be done remotely.

A different way of physically disconnecting equipment is to use a network "kill switch". It is a device inserted in the network path between A and B, and with a physical switch¹ the network

¹ A kill switch is **not** an Ethernet switch (i.e.; from Cisco), but it may look like one.

connection is broken / restored. On a larger scale, a “kill switch” is not a single device but the measure to shut down internet access in a country².

Below, I will show how a kill switch can be made, but this is for hobbyists only (first chapter). You can also buy professional equipment (later chapters). Note that this equipment is almost never called “kill switch”. However, in this article I will continue to use that term, to avoid confusion with all other possible designations.

D o-it-yourself kill switches

It is not too difficult to make your own kill switch, at least if you’re handy with a soldering iron. One example can be found on <https://makezine.com/projects/internet-kill-switch/>, another example on https://www.youtube.com/watch?v=vhFKb8b_UAY.



Figure: DIY project from MakeZine

The protective red cap gives it a serious look; even more dramatic looks this one:



Figure: DIY project from
<https://www.printables.com/model/68530-internet-kill-switch>

² See https://en.wikipedia.org/wiki/Internet_kill_switch and [https://en.wikipedia.org/wiki/Killswitch_\(film\)](https://en.wikipedia.org/wiki/Killswitch_(film))

The manual kill switches shown above are easy to make, but they do have a disadvantage that you should be aware of: the interrupting of just 1 of the 4 Ethernet signal (at 10 or 100 Mbit/s) wires disrupts network traffic in one direction only. For most network protocols, this is sufficient to cause them to stop operating. But some network protocols (i.e. like UDP) and broadcast/multicast traffic can continue to operate. So these kill switches still allow traffic (although limited). Another disadvantage is that, depending on the physical switch being used, the Ethernet signal quality may be influenced negatively (due to resistance, impedance) and contact bounce.

A bit more fancy is the home-brew blocker found on <https://github.com/roblatour/esp32NetworkBlocker> with a serial interface that can be controlled externally. Hardware-wise, a relay blocks two of the 8 Ethernet signal wires. The advantage of this device is that, based on external events (i.e. as detected in a firewall) network access can be blocked automatically.

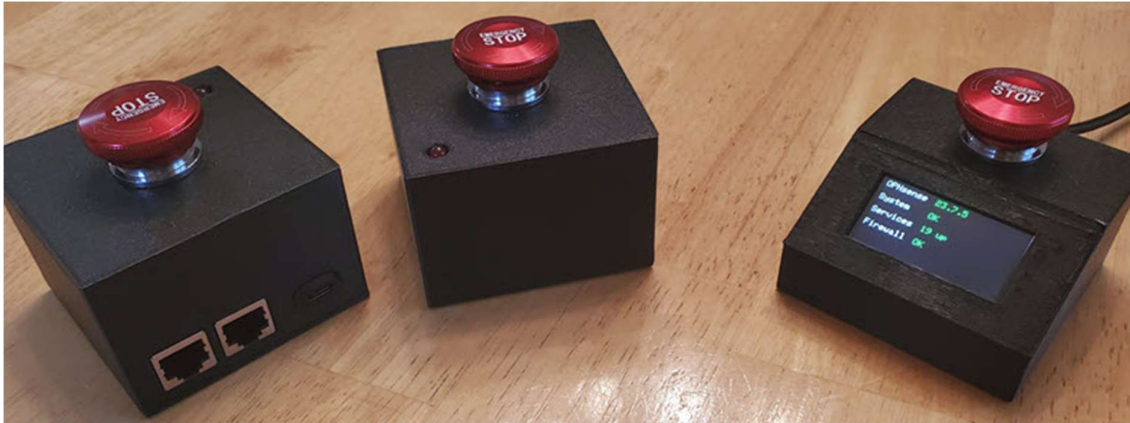


Figure: a kill switch that can be remotely controlled

On internet, a lot more projects can be found, apparently making a kill switch is a popular hobby. In case you are interested in more electronic details, see <https://www.techliminals.com/electronics/ethernet-toggle-switch.php>.

Personally, I prefer an interruption of **all** Ethernet signal wires. A kill switch which interrupts all the 8 wires can be found on InternetSwitches (<https://www.internetswitches.com/>, and also via Amazon (<https://www.amazon.com/Internet-CUT-OFF-Kill-Switch/dp/B00RQVFH24>). The documentation shows that it really interrupts 8 wires. And that for only € 15!

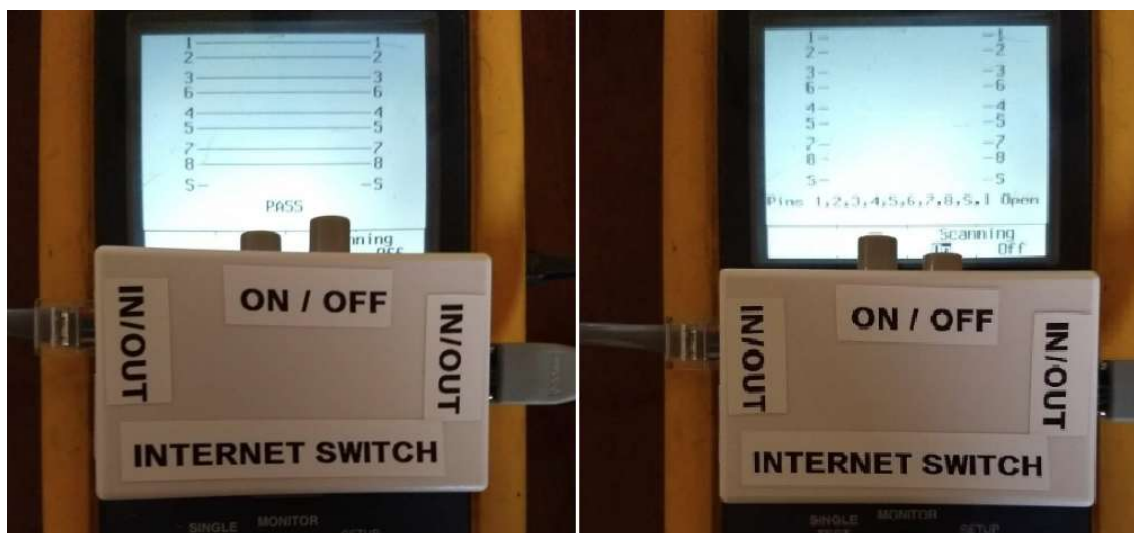


Figure: a Fluke cable tester shows that all 8 wires are interrupted.

Ready-made kill switches

Complete ready-made kill switches are less abundant than hobby projects, but they do exist. Many can be found via a search on "RJ45 Switch Box", "Ethernet Disconnect switch" or "Ethernet ON/OFF switch".

These are not meant as a kill switch, but allow two devices (A and B) to be connected to one switch port. So depending on the switch, there is traffic $A \leftrightarrow X$ possible or $B \leftrightarrow X$ (where X is then your local network, or internet).

The kill switch function is emulated by simply not connecting anything to port B. It so functions more or less identically to a KVM switch. Prices range from around \$2 to \$50.



Figure: some kill switches found via Google, Amazon and Alibaba

Professional kill switches

For professional applications, professional made products are preferred. Not just only 100 Mbit/s but also better housing, EMC compatibility, temperature range, remote control, etc. are just features not found in cheap products.

In this chapter, we'll discuss 3 professional products.

Goldilock "FireBreak"

Goldilock (<https://www.goldilock.com>), a UK company, brings the "FireBreak" device on the market. It looks very much like a switch, but of course isn't. It can control 12 network connections, either individually, or per group. Each network connection can be disabled remotely.



Figure: the Goldilock product

Network signals (8 per RJ45) are passed from connector A to connector B via 8 "reed" switches. A reed switch is an electromagnetic switch which opens or closes under influence of an external magnetic field.

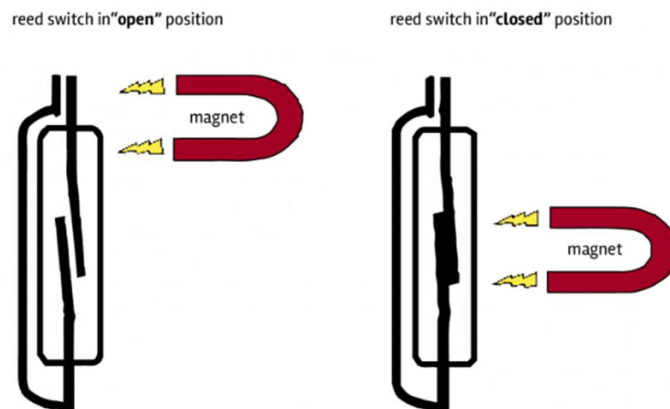
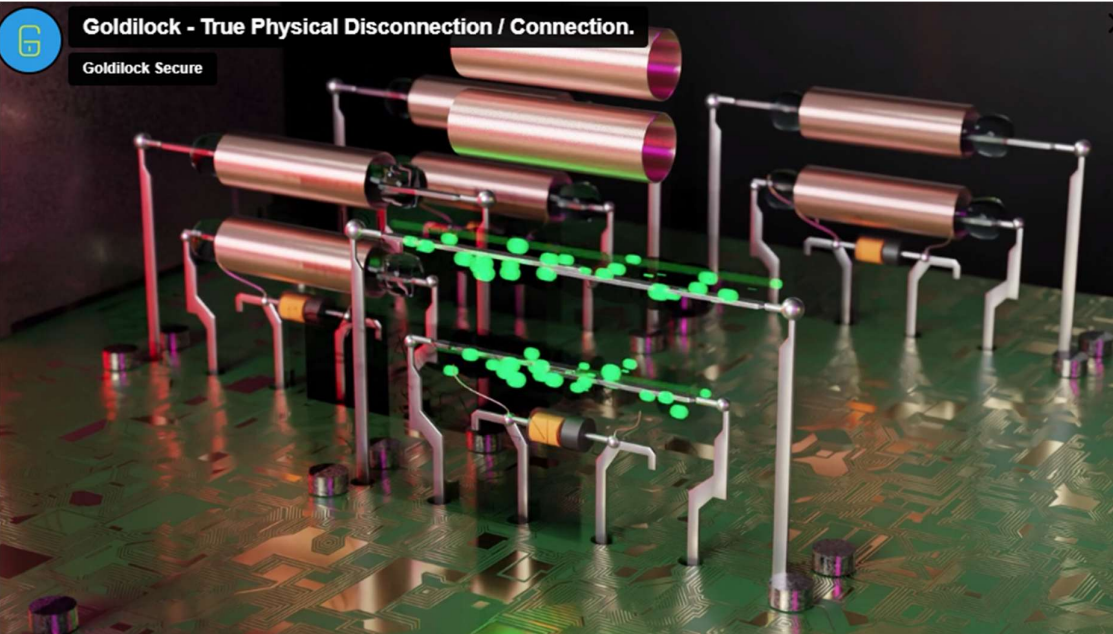


Figure: principle of a reed switch (source: deeterelectronics.com)

Goldilock - True Physical Disconnection / Connection.

Goldilock Secure



It is possible to remotely control each of the 12 network interfaces via the mobile network, preconfigured SMS with number filtering, and with 2FA.

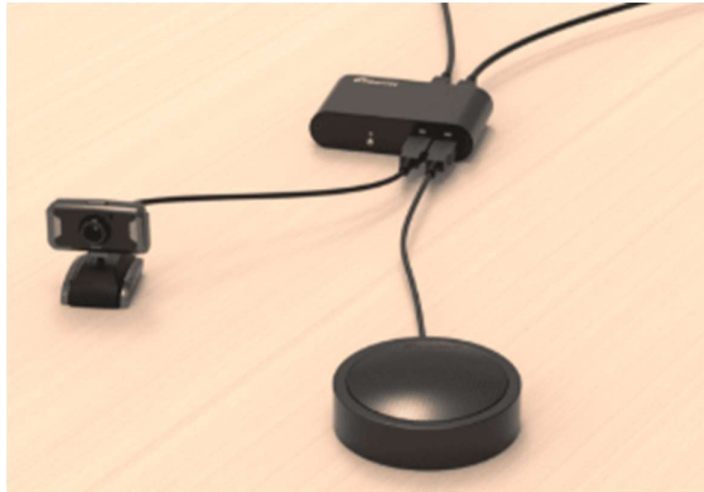
ValiantCom

<https://www.valiantcom.com/cyber-security/data-sheets/network-kill-switch.pdf>



USB Kill switch

Ethernet kill switches (v1)



Source: fibernet-tech.com

This article is likely not complete in describing all possible kill switch solutions on the market. If you have any suggestions, comments or additions, please do not hesitate to contact me (email: [rh\[at\]enodenetworks.com](mailto:rh[at]enodenetworks.com)).