



CNX SOFTWARE – EMBEDDED SYSTEMS NEWS

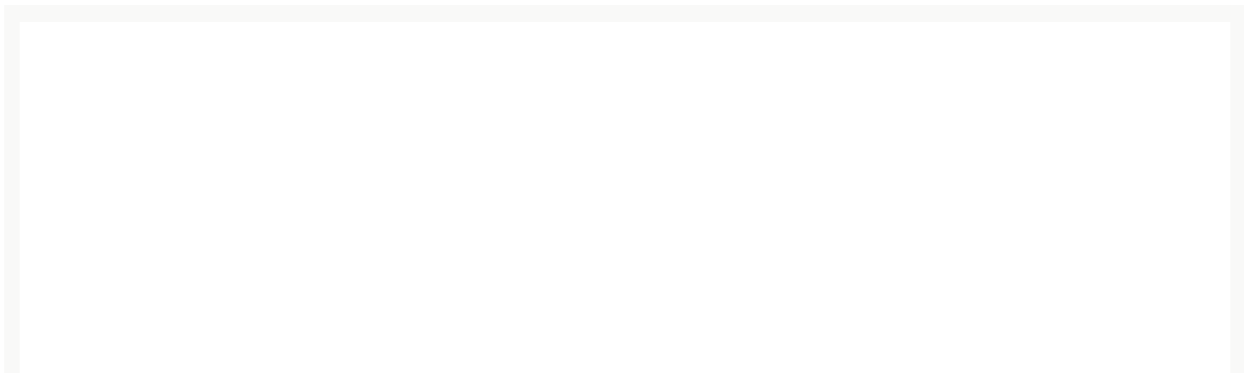
Reviews, tutorials and the latest news about embedded systems, IoT, open-source hardware, SBC's, microcontrollers, processors, and more


DECEMBER 15, 2021 BY JEAN-LUC AUFRANC (CNXSOFT) - 13 COMMENTS

BusKill USB kill cord protects data on Linux, Windows, Mac OS devices

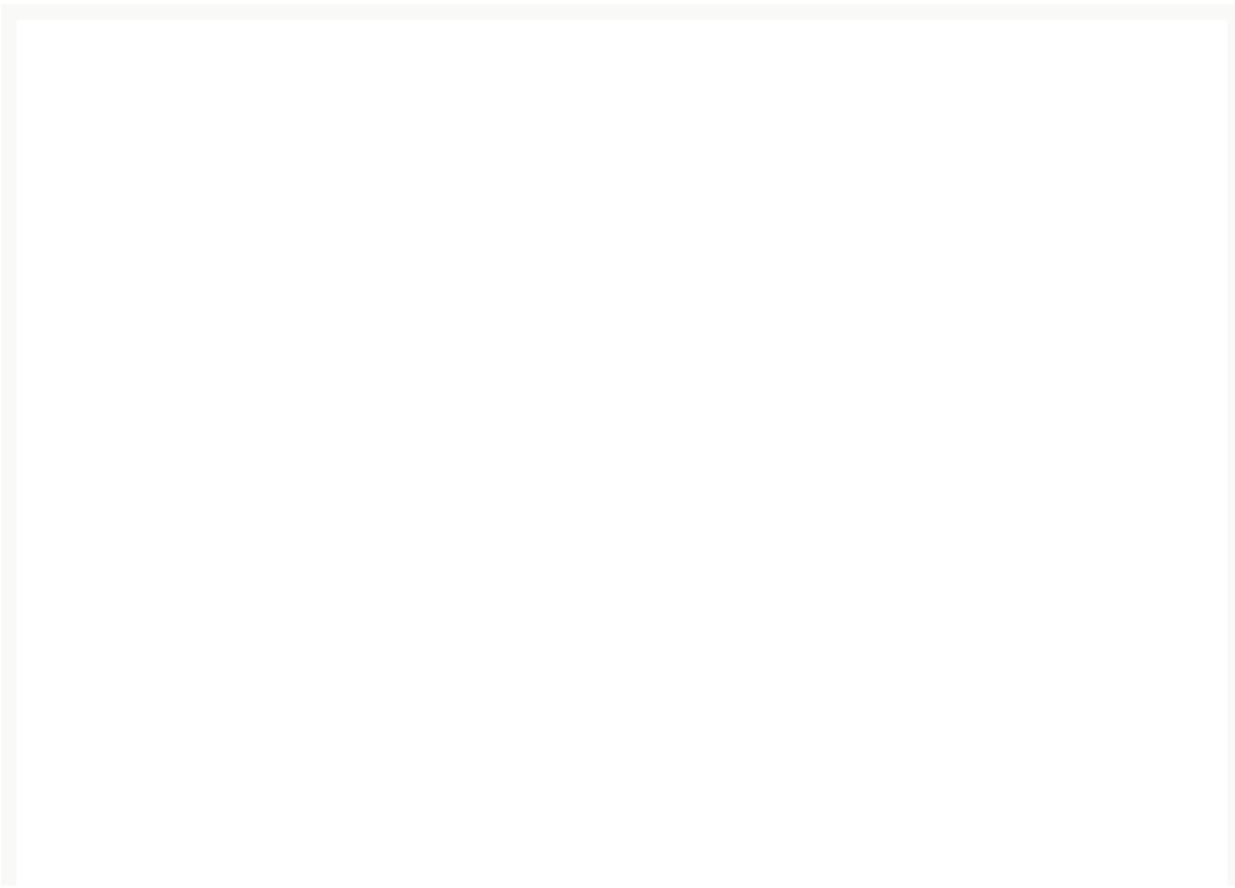
Data is can be extremely valuable, so Alt Shift designed the BusKill USB kill cord that will automatically execute a user-configurable trigger when your machine is physically separated from you. It can be especially useful to journalists and activists that may get their devices seized by the government, crypto traders, military personnel, or travelers with sensitive data.

BusKill is basically just a USB cable attached to the computer via a magnetic breakaway and to the user, for instance to a belt loop, and that will trigger a configurable Python script if the cable is detached while BusKill software is armed.





BusKill is made up of four hardware components with a custom magnetic breakaway, a standard USB extension cable, and a USB thumb drive attached to a carabiner via a keyring. I could not find a clear explanation for the USB thumb drive in this system, but I can only assume it's for USB removal/insertion. BusKill is fully open-source, and you'll find the python scripts and GUI, as well as OpenSCAD files for the magnetic breakaway on Github. A separate website also provides documentation with more details, such as the operating systems supported: Windows 10, Mac OS 10.05, as well as Ubuntu 20.04/18.04.



BusKill can be armed/disarmed from the command or the GUI program, and there are different levels of protection for your system. By default, the program will not destroy any data, and simply turn off your computer if the USB cable to disconnected while BusKill is armed. But the solution offers more flexibility, especially for advanced Linux users that can manually add auxiliary triggers, such as a self-destruct trigger that wipes the LUKS header, making the entire disk permanently inaccessible.

This brings the topic of accidental unplugging, where you could potentially get your data wiped out while forgetting your USB kill cord is attached to your computer. Alt Shift addresses that issue in a [FAQ](#):

BusKill's breakaway connector uses strong magnets that decreases the risk of false-positives.

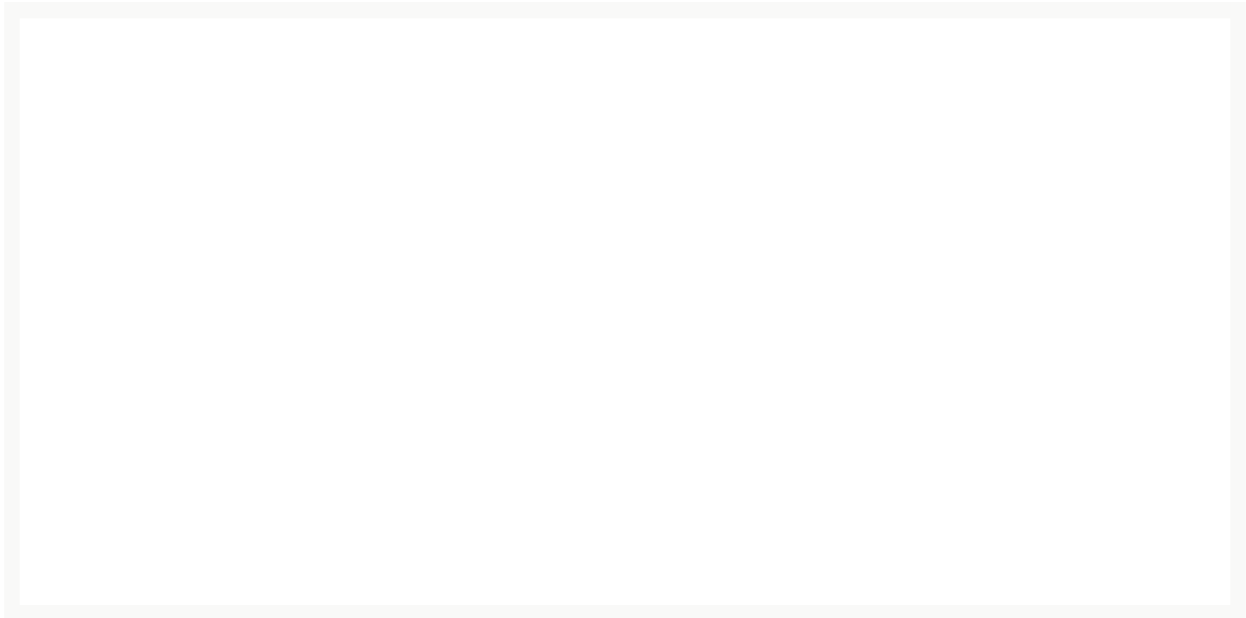
That said, it is designed to breakaway, so if you accidentally trigger BusKill (by, say, standing up to get a cup of coffee without disarming BusKill), then the worst that can happen (if you're using the BusKill app without manually adding auxiliary triggers) is that your computer will shutdown.

Here's some tips to avoid false-positives:

- When using BusKill, work on a sturdy table with a comfortable chair.*
- Avoid moving your laptop after arming BusKill in the app.*
- The first few days, limit yourself to just the lock screen trigger to avoid loosing your work as you get used to disarming BusKill before taking toilet breaks.*

Similar systems have been designed in the past with most relying on Bluetooth or 2.4 GHz ISM with solutions such as [DayTripper](#), but it may not be as secure due to

potential attacks like radio jamming and replay attacks.



The complete BusKill Kit has just launched [on Crowd Supply for \\$89](#) or the [company's own store](#) if you want to pay with cryptocurrencies. Shipping is free worldwide, and orders are expected to ship by June 2022.