Modern cyber security and dealing with Secure Gateway Modules

As vehicles have more security sensitive systems incorporated into them, manufacturers have started to implement systems to secure them against unwanted access. Since around 2018, the Fiat Lancia Chrysler group introduced a Secure Gateway Module (SGW) into their vehicles. This prevented unwanted access to their systems. Workshops still had access to fault code reading for diagnostic testing, but are unable to delete faults or perform any adaptions or resets. This also included a basic service reset procedure, after maintenance work has been carried out. We often get calls asking why their diagnostic equipment will not perform basic deletion adaptions or resets on these 2018 and onwards vehicles.

We can see the need for this level of security against any form of cyber-attack into sensitive fly-by-wire systems, but there needs to be a level of access for independent workshops to continue with their diagnostic services, and even basic reset functions after repairs or maintenance. This is possible, but it requires the workshop to register with the scan tool manufacturer for a right of access. This is normally a paid service added to the tool software subscription. Up to now, only certain tool manufacturers have this right of access.

Fortunately, there is an alternative way to bypass the SGW module on Fiat Chrysler vehicles. A bypass lead has been produced that can be plugged in to perform the resets and programming, and then used to replace the module after the work is completed.

But as more manufacturers are moving over to Secure Gateway Modules, there may be a need for more research into methods of bypassing this level of vehicle security. This will work until they implement new, and more inventive ways to secure their systems.

One solution is to use a lead to bypass the Secure Gateway Module