

The Car Hacker's Handbook: A Guide for the Penetration Tester - Craig Smith (2016)

Chapter 13. PERFORMANCE TUNING

by Dave Blundell



Performance tuning, frequently referred to simply as *tuning*, involves altering an engine's operating parameters to improve vehicle performance. In today's vehicles, this usually means modifying an engine computer, even for mechanical modifications.

Performance tuning is necessary for most automotive racing. This huge industry—worth around \$19 billion annually

worldwide, according to the Performance Racing Industry—draws almost half a million people yearly to compete in auto races in the United States alone. And these figures don't even include the many modified vehicles that compete in amateur racing around the world.

Most performance tuning involves nothing more than changing the operating conditions of an engine to achieve goals different than those of the original design. Most engines have substantial room for improvement in power or economy if you're willing to give up a little safety or use a different fuel than the engine was originally tuned with.

This chapter offers a high-level overview of engine performance tuning and the compromises that must be made when deciding which aspects of an engine's operation to modify. Here are some representative examples of the uses and accomplishments of performance tuning:

- After a different rear axle gear was installed in a 2008 Chevy Silverado to improve the truck's ability to tow heavy loads, the speedometer was thrown off because of the change in gear ratio, the transmission was shifting too late, and the antilock braking system was inoperable. The engine computer had to be reprogrammed to make the speedometer read correctly, and the transmission controller needed to be reprogrammed to make the truck shift properly. After proper calibration, the truck was able to work

correctly.

- Changing from summer to winter tires in a 2005 Ford F350 required reprogramming the engine and transmission computers in order to ensure speedometer accuracy and appropriate transmission shifting.
- As an alternative to junking a 1995 Honda Civic when the engine blew, a 2000 Honda CR-V engine and transmission were installed. The original engine computer was reprogrammed and tuned to match the new engine. This vehicle has since driven almost 60,000 miles after replacement of the motor.
- Adjusting the timing of transmission shifts and the engine's use of fuel and spark in the factory computer made a 2005 Chevrolet Avalanche more fuel efficient. These changes improved fuel economy from a 15.4 mpg to a 18.5 mpg average while maintaining Louisiana emissions testing compliance.
- The factory computer was reprogrammed in a 1996 Nissan 240 to match a newly installed engine and transmission. Before the reprogramming, the car could barely run. After the reprogramming, the car ran as though it had come from the factory with the new engine.

WARNING

Almost every nation has its own emissions laws that tend to prohibit tampering with, disabling, or removing any emissions-related system. Many performance modifications, including engine computer tuning, involve changing the operation of or removing emissions components from the vehicle, which may be illegal for vehicles operated on public roads. Consider local laws before performance tuning any vehicle.

Performance Tuning Trade-Offs

If performance tuning is powerful and offers so many benefits, why don't cars come from the factory with the best possible settings? The short answer is that there is no best setting; there are only trade-offs and compromises, which depend on what you want from any particular vehicle.

There's always an interplay between settings. For example, the settings for getting the most horsepower out of a vehicle are not the same as the settings that deliver the best fuel economy. There's a similar trade-off between lowest emissions, maximum fuel economy, and maximum power. In order to simultaneously increase fuel economy and power output, it is necessary to increase the average pressure from combustion, which means the engine will be operating closer to the edge of safe operating conditions. Tuning is a game of compromises in which the engine is configured to achieve a specific goal without self-destructing.

For manufacturers, the order of priority when designing engine capabilities is to ensure

1. that the engine operates safely,
2. that it complies with emissions standards set by the EPA, and
3. that the fuel efficiency is as high as possible.

When manufacturers design certain performance-oriented vehicles, such as the Chevrolet Corvette, power output may also be a high priority, but only once emissions requirements have been met. Stock settings typically stop an engine short of achieving maximum power, usually in order to reduce emissions and protect the motor.

When performance tuning an engine without modifying mechanical parts, the following compromises are generally true:

- Increasing power lowers fuel economy and generates higher hydrocarbon emissions.
- Increasing fuel economy can increase NO_x emissions.
- Increasing torque increases the force and stress on a vehicle's engine and structural components.
- Increasing cylinder pressure leads to a higher chance of

detonation and engine damage.

That said, it is actually possible to gain more power *and* improve fuel economy—by raising the brake mean effective pressure (BMEP). The BMEP is essentially the average pressure applied to the pistons during engine operation. The trade-off here, however, is that it's hard to raise BMEP significantly without also increasing the peak cylinder pressure during a combustion event, and so increasing the chance of detonation. There are firm limits on the maximum peak pressure in a given situation due to the motor's physical construction, the fuel being used, and physical and material factors. Increasing peak cylinder pressure beyond a certain limit will generally result in combustion without spark due to *autoignition*, also known as *detonation*, which will typically destroy engines quickly.

ECU Tuning

Engine computers are the vehicle computers most commonly modified for performance tuning. Most performance modifications are designed to change an engine's physical operation, which often requires a corresponding change to the calibration of the engine computer to achieve optimal operation. Sometimes this recalibration requires physically modifying a computer by removing and reprogramming chips, known as *chip tuning*. In other cases, it's possible to reprogram the ECU by

communicating with it using a special protocol instead of physically modifying it, which is called *flash programming* or just *flashing*.

Chip Tuning

Chip tuning is the oldest form of engine computer modification. Most early engine controllers used dedicated ROM memory chips. In order to change a chip's operation, you had to physically remove the chip, reprogram it outside the ECU, and then reinstall it—a process called *chipping*. Users who expect to make repeated modifications on older vehicles often install sockets in place of the ROM to allow easier insertion and removal of chips.

Automotive computers use many different kinds of memory chips. Some can be programmed only one time, but most can be erased and reused. Some older chips have a window on them and require UV-C light—a sterilizer—in order to erase them.

EPROM Programmers

Chip tuning generally requires an *EPROM programmer*, a device that reads, writes, and—if supported—programs chips. When chip tuning, be very careful to make sure that the programmer you buy works with the type of chip you intend to modify. There's no such thing as a truly universal

chip programmer. Here are a couple of popular EPROM programmers:

BURN2 A relatively cheap basic programmer (about \$85) that supports common EPROMs used in chip programming. It features a USB interface with an open command set, along with many tuning applications that already have native support (<https://www.moates.net/chip-programming-c-94.html>).

Willem Another popular ROM burner (from \$50 to \$100, depending on the model). The original Willem used a parallel port interface, but newer versions use USB. (Look for the Willem on Ebay or MCUMall.com.)

Almost all EPROM programmers support only dual in-line package (DIP) chips. If your vehicle's computer uses surface mount-style chips, you'll probably need to purchase an appropriate additional adapter. It's generally a good idea to get any adapters from the same source as the programmer to ensure compatibility. All adapters should be considered custom hardware.

Figure 13-1 shows a ROM adapter board installed in a Nissan ECU. The two empty 28-pin sockets in the lower-left corner have been added to the original ECU. Some soldering is often required to modify and add ROM boards such as this one.

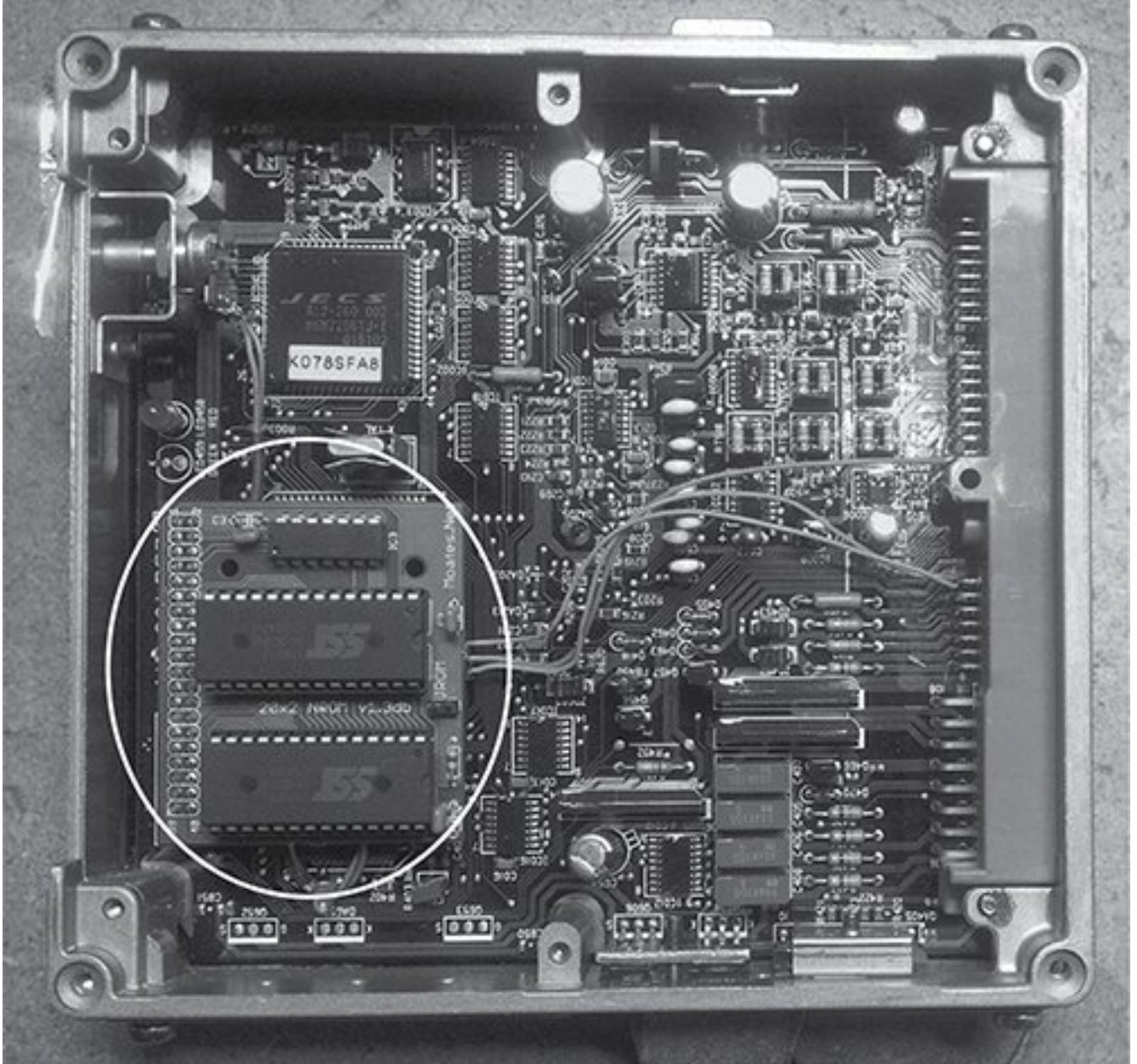


Figure 13-1: A 1992 S13 Nissan KA24DE ECU with a Moates ROM adapter board installed

ROM Emulators

One of the big advantages of chip tuning over other tuning methods is that it allows the use of ROM emulators, which store the contents of ROM in some form of nonvolatile read/write memory so that you can make instant modifications to ROM. By allowing more or less instant

changes, ROM emulators can greatly reduce the amount of time required to tune a vehicle compared to flash tuning, which is usually much slower for updates.

ROM emulators generally use a USB or serial connection to a PC and software that updates the emulator to keep it synchronized with a working image on the PC. The following are recommended ROM emulators:

Ostrich2 A ROM emulator designed for 8-bit EPROMs ranging from 4k (2732A) to 512k (4mbit 29F040) and everything in between (27C128, 27C256, 27C512). It is relatively inexpensive at about \$185, and features a USB interface with an open command set, as well as many tuning applications that already have native support (<https://www.moates.net/ostrich-20-the-new-breed-p-169.html>).

RoadRunner A ROM emulator aimed at 16-bit EPROMs, like 28F200, 29F400, and 28F800 in a PSOP44 package (see [Figure 13-2](#)). It is also relatively inexpensive at about \$489 and features a USB interface with an open command set and many tuning applications that already have native support (<https://www.moates.net/roadrunnerdiy-guts-kit-p-118.html>).

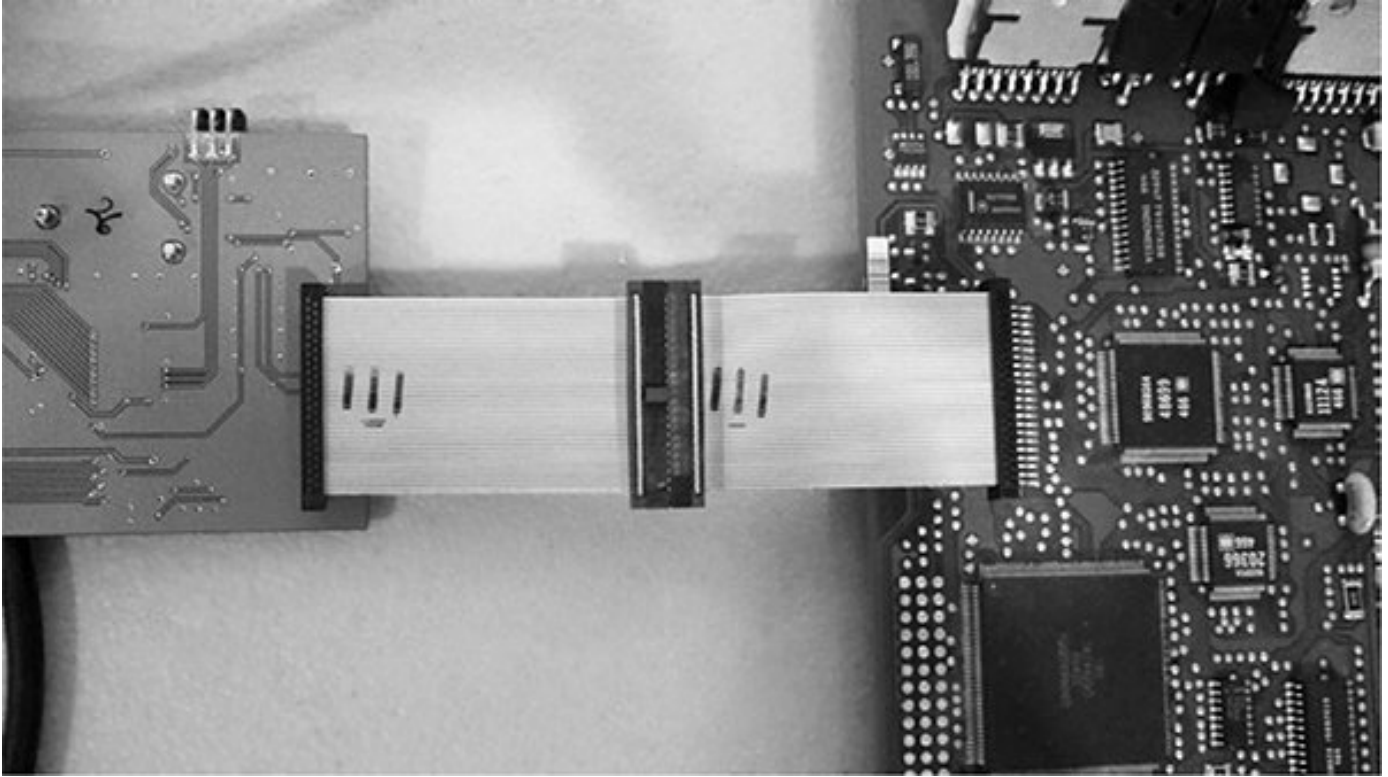


Figure 13-2: The RoadRunner emulator connected to a Chevrolet 12200411 LS1 PCM

OLS300 An emulator that works with only WinOLS software. It is around \$3,000 (you have to get a quote) and emulates a variety of 8-and 16-bit EPROMs natively (<http://www.evc.de/en/product/ols/ols300/>).

Flash Tuning

Unlike chip tuning, flash tuning (also known as flashing) requires no physical modifications. When flashing, you reprogram the ECU by communicating with it using specialized protocols.

The first flashable ECUs became available around 1996. J2534 DLLs combined with OEM software provide access to

a method of flash programming, but most tuning software bypasses this entirely and communicates natively with the ECU. Most aftermarket tuning packages—such as HP tuners, EFI Live, Hondata, and Cobb—use a proprietary piece of hardware instead of a J2534 pass-through device. The Binary Editor (<http://www.eecanalyzer.net/>) is one example of software that offers J2534 as an option for programming Ford vehicles using supported J2534 interfaces.

RomRaider

RomRaider (<http://www.romraider.com/>) is a free, open source tuning tool designed for Subaru vehicles. With that, you can use the Tactrix OpenPort 2.0—a piece of pass-through hardware (<http://www.tactrix.com/>, about \$170) that works well with RomRaider. Once you have a pass-through cable hooked up to the ECU, RomRaider allows you to download the ECU's flash memory. You can then open these flash images with a *definitions* file, or *def*, which maps the locations and structure of parameters within the image, and provides the formulas to display data in a human-readable format. This mapping lets you quickly locate and change engine parameters without having to disassemble the flash. Figure 13-3 shows RomRaider with a flash image and definition loaded.

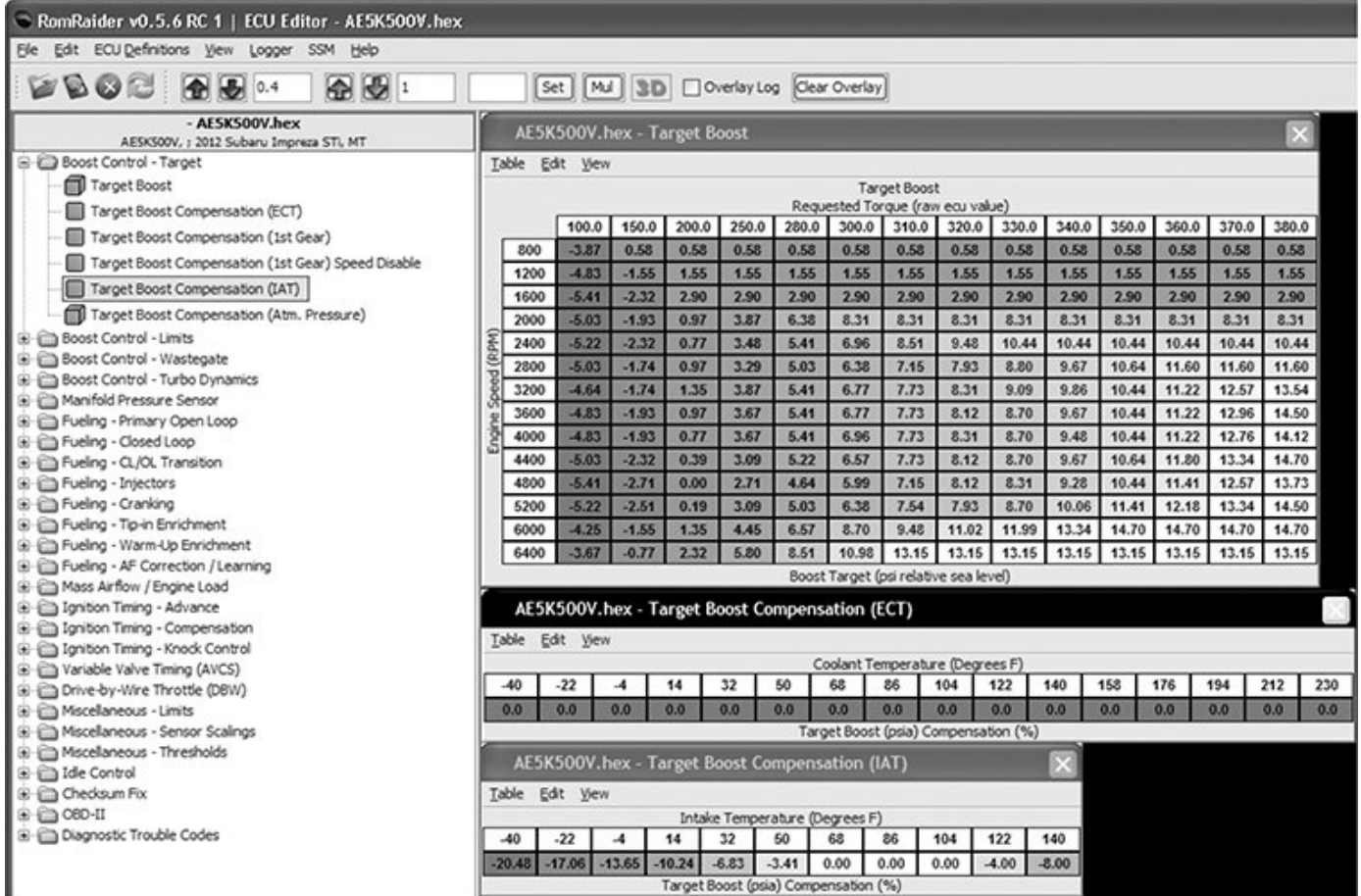


Figure 13-3: RomRaider ECU editor

Stand-Alone Engine Management

One alternative to reverse engineering factory computers is to simply replace them with an aftermarket part. A popular stand-alone engine computer is the MegaSquirt (<http://megasquirt.info/>), which is a family of boards and chips that will work with just about any fuel-injected engine.

MegaSquirt has its roots in the DIY community and was designed to enable people to program their own engine computers. Early MegaSquirt units typically required you to assemble the board yourself, but these versions often resulted in confusion, with many competing user-assembled

hardware designs that were not quite compatible. Current designs have therefore moved toward a pre-made format in order to provide a more consistent and uniform hardware platform.

There are several multiplatform tools available for use with the MegaSquirt hardware. Figure 13-4 shows the most popular one: TunerStudio

(<http://www.tunerstudio.com/index.php/tuner-studio/>, around \$60). TunerStudio lets you modify parameters, view sensors and engine operating conditions, record data, and analyze data to make targeted changes.

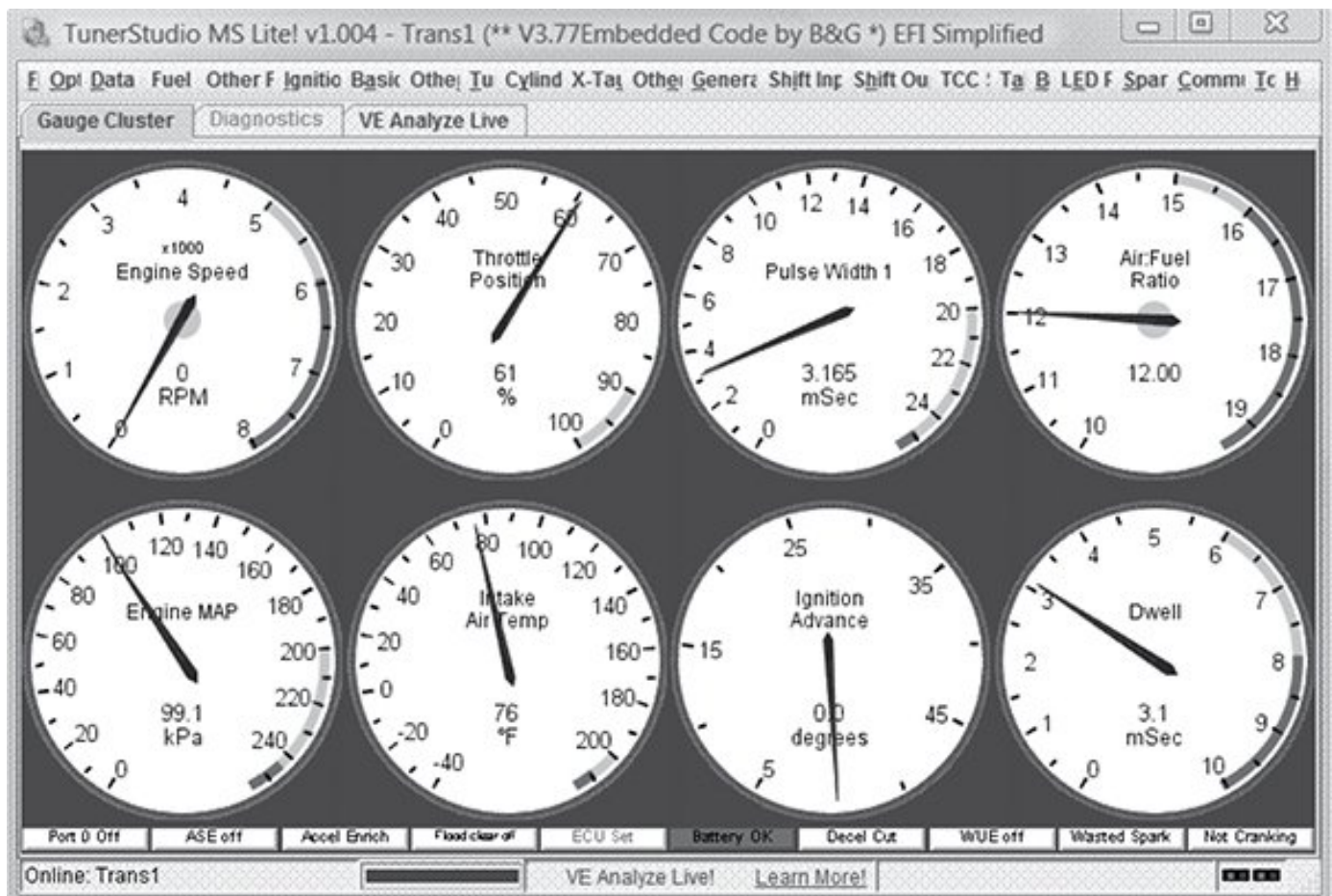


Figure 13-4: TunerStudio gauge cluster

Summary

This chapter shows how an understanding of a vehicle's embedded systems can be used to change its behavior. We've seen how almost any changes made to a vehicle, even mechanical modifications, require some reprogramming of the vehicle's computer. We've looked at how alterations in standard factory settings result in performance trade-offs and compromises, such that the "best" settings for a vehicle will always depend on your specific goals. We've also shown a few examples of performance tuning methods, including chip and flash tuning, and presented some common hardware and software tools used for tuning cars.