Text material

Text

A train manufactured by a Polish company suddenly broke down during maintenance. The experts were helpless – the train was fine, it just wouldn't run. In a desperate last gasp, the Dragon Sector team was called in to help, and its members found wonders the train engineers had never dreamed of.

In this story, we will take you on an unusual journey. A journey full of unexpected discoveries and events, a journey under pressure of time and money, as well as unusual technologies. A journey in which the train plays the most important role – although unfortunately it doesn't move, even though it should. Fasten your seatbelts – or at least sit comfortably, because there are sharp turns ahead.

Winning the tender, losing the service

The story probably begins a little earlier, but we will enter the scene in spring 2022, when the maintenance for the first of eleven Impuls 45WE trains (made by Polish company Newag) operated by the Lower Silesian Railways ends. The maintenance is carried out by an independent train maintenance company called Serwis Pojazdów Szynowych, hereafter referred to as SPS, SPS won the tender to carry out the mandatory maintenance of the trains after a distance of 1,000,000 kilometres. The train manufacturer, Newag, also competed in the tender to carry out the maintenance, but the manufacturer's bid was about 750k USD higher and the tender was eventually won by SPS, which offered to carry out the maintenance of 11 trains for around 5.5 mln USD.

Maintenance a train is a complicated affair – it has to be taken apart, the parts sent to the various manufacturers, checked, sent back, the train put back together again and tested. The SPS carries out the maintenance procedures according to the relevant maintenance manual (some 20,000 pages) provided by the manufacturer, but the train does not start after being put together. The computer says everything is fine, the train is ready to run – but it does not run. The inverters are not supplying voltage to the motors and no one has any idea why this is happening. Maintenance technicians search, check, verify, consult the manuals – they find no answer.

Mysterious breakdowns

The Lower Silesian Railway has eleven Impulses and, according to the schedule, another one is about to be sent for maintenance, while the first – instead of returning to work – is still sitting in the workshop. The second train is undergoing an identical maintenance, with identical results. Before the maintenance it was operating, after the maintenance it no longer wants to run. The work on getting the first train up and running, like the train itself, has not progressed one millimetre, while the manufacturer refuses to help. Two immobile trains are already sitting in the workshop. The third misses its inspection due to battery failure, so a fourth train ("from the future") is sent to the maintenance instead. The maintenance company wants to take advantage of its presence to tow one of those that won't run. When the fourth (running) train is connected to one of the stationary ones, the running one also comes to a standstill (the reason for this has not yet been established). In addition, at another workshop in another Polish town, Szczecin, another Impulse breaks down in very similar circumstances – it does not start up after servicing.

Poland's top hackers

At a certain point, the problem becomes serious enough to be noticed by the media – the six longest trains of the Lower Silesian Railway out of service mean that timetables have to be reduced, replacement trains have to be sent to the tracks, and passengers travel in overcrowded, shorter trainsets. Newag explains that the trains were blocked by a "safety system" – but in the 20,000 pages of instructions, it is in vain to find even a mention of it. A day of train downtime in the workshop costs over 1000 USD in contractual penalties, and there are several trains stuck, so the tension level in the SPS is rising. Since neither the mechanics nor the electricians

have a solution, someone types “Polish hackers” into Google and comes across an article about the Dragon Sector group’s successes in the CTF arena at the top of the results list. SPS makes contact with DS, whose representatives at first can’t believe the proposal they hear. Train hacking? Well, why not. The parties sign a contract. Dragon Sector members Michał “Redford” Kowalczyk and Sergiusz “q3k” Bazański, known for hacking Toshiba laptops, take on the project, and Kuba “PanKleszcz” Stępniewicz, who has experience in industrial automation, joins in. The team set off briskly to work, with Kuba taking a trip to the workshop. On site, they get a train that doesn’t move, two spare computers and the computer manufacturer’s SDK files. They start the work by tapping into the CAN bus, but it’s difficult to read the traffic without documentation of the protocols. They take a long time trying to dump the embedded software from the on-board computer. They have no documentation of the computer and the SDK only allows uploading new software, with no option to dump existing software. As they experiment with the older version of the software they found, uploading it to the first spare computer causes it to stop responding – they are left with only one working spare computer. Eventually, they find a debugging interface and download the device’s memory byte by byte.

The computer is based on the TriCore architecture, like many similar solutions in the automotive industry. Unfortunately, there is a lack of good disassemblers, so the researchers are improving Ghidra a bit and can finally look into the code. Admittedly, strings are missing, but the work is slowly moving forward. A month and a half goes by when the SPS passes on the bad news.

As the deadline chases and trains break down

The Lower Silesian Railway, unable to wait for its trains, decides to cooperate with Newag on the repair of broken trainsets and their maintenance, including trains which, according to the original tender, were yet to be sent for maintenance at SPS. The rupture of the contract with SPS is expected to take place in a week’s time. As is well known, nothing affects the intensity of the work as much as a very close deadline by which the result has to be shown, so the researchers set to work with redoubled energy. In the course of their work so far, they have downloaded the memory contents of a number of computers, both trains that are working and those that should only be working. Comparing these images is an ordeal, as almost every train has a different set of functions and a different version of software, but slowly they are starting to get a feel for something. They identify values in the computers’ memory that are set in one train and zeroed out in another. They can run tests at their desks – the computer, even when taken out of the train, lets it run for a while (before realising it’s missing the rest of the train) to show whether it’s ready to run the inverters.

There is less than a day left until the deadline for completion when they find the configuration of flags that gives the train a chance to run. Unfortunately, during the experiments, the last working on-board computer burns out. Yes, it burns – a capacitor burns (a rather random occurrence). After another brainstorm and many attempts to put the two damaged computers into one, they manage to repair the burnt one and at 2am, the night before doomsday, the researchers configure a computer to start the train. One of the researchers boards a train (of a different operator) to arrive with the presumably working computer at the workshop just before the representatives of the Lower Silesian Railway, who have announced a visit for 9:30 a.m. Unfortunately, the train on which the researcher travels to the maintenance company is late. Eventually, in the morning, the researcher with the computer arrives at the site, connects the pray-it-works-computer to the broken-down train, but the train does not start. Another brainstorm identifies one flag that was forgotten and at 8:42 the train manages to start. The Lower Silesian Railway delegation, seeing at 9:30 that the trains have a chance of getting back to life after all, does not break the contract with SPS.

Why the train broke down

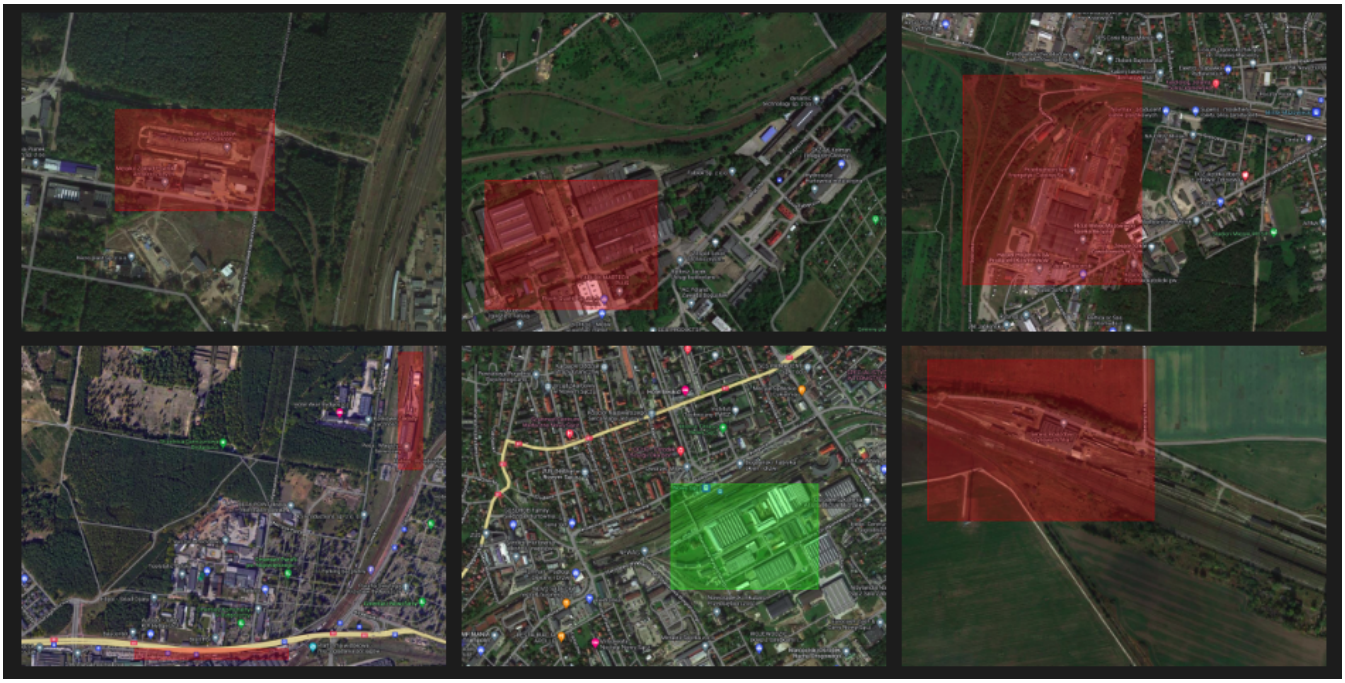
Figuring out how to get the train to run wasn’t even half the battle – you still had to figure out why it broke down, and this is where the thrill ride begins.

Months of analysis and reverse engineering uncovered some extremely interesting conditions written into the software code of various trains supplied by Newag. After hundreds of hours spent on code dumped from dozens of trainsets, it was possible to identify some very interesting mechanisms causing sudden train sickness.

The numerical values 53.13845 and 17.99011 found in the computer code seemed familiar at first glance. It soon became apparent that these were GPS coordinates pointing to the vicinity of Bydgoszcz Główny Railway Station, specifically the PESA (another Polish train producer and maintenance center) site located next to it. Soon the coordinates of other maintenance centers that could carry out train repairs and maintenance in Poland were also found. Below we show the pseudo-code of the algorithm (the names of the variables or functions are given by the researchers for clarity – we do not know what the original names were):

```
check1 = 53.13845 < lat && lat < 53.13882 && 17.99011 < long && long < 17.99837;
check2 = 53.14453 < lat && lat < 53.14828 && 18.00428 < long && long < 18.00555;
check3 = 52.17048 < lat && lat < 52.17736 && 21.53480 < long && long < 21.54437;
check4 = 49.60336 < lat && lat < 49.60686 && 20.70073 < long && long < 20.70840
        && (this->lock_function_test & 1);
check5 = 53.10244 < lat && lat < 53.10406 && 18.07817 < long && long < 18.08243;
check6 = 50.12608 < lat && lat < 50.12830 && 19.38411 < long && long < 19.38872;
check7 = 52.77292 < lat && lat < 52.77551 && 18.22117 < long && long < 18.22724;
```

Coordinate pairs define the workshop areas. A condition has been written in the computer code to disable the ability to run a train if it spends at least 10 days in one of these workshops. One of the workshops belongs to Newag itself – but a different logical condition was defined for its coordinates, presumably for testing purposes.



Other surprises were soon discovered. Among them was the blocking of a train when one of its components is replaced (verified by its serial number). An option to undo the lockout was also discovered – this did not require setting flags at computer memory level, just the right sequence of button clicks in the cab and on the on-board computer screen. When news of the successful launch of the Impulse hit the media, the trains received a software update that removed this ‘fix’ option. On another train, a code was found instructing it to ‘break down’ after a million kilometres.

Not only in Wrocław

Information that the SPS maintenance center succeeded in repairing Newag’s ‘broken’ trainsets quickly found its way to other companies as well. It turned out to be quite a common problem. In Wrocław they analysed 13 Impulses, but there were also broken ones running in Kolej Mazowieckie (one), two in Opole, four in Krakow, one in Zielona Góra, four in Szczecin and one in Warsaw. Fortunately, each was able to be repaired using a tool developed by our researchers that removes software locks from the on-board computer. In total, the researchers analysed the software of 29 trains and in all but five they found surprises beyond the official operating instructions.

We congratulate the best Polish hackers on their interesting discovery and professional execution of the assignment. Remember, nothing motivates you like a deadline tomorrow morning.