Late-April 2020, a Stuxnet-like attack on Israel's water facilities underpinned the vital necessity for level-0 monitoring.

Monitoring the electric signals transmitted directly from the critical assets is by far the most viable and reliable method to detect any malicious cyber-attack on operational machinery and equipment. Unlike any other cybersecurity product that monitors the IT network, and are therefore blind to the actual process, 'SigaGuard' diagnoses the un-filtered and un-hackable electric signals directly from level 0, delivering bulletproof protection to the mission-critical operational assets.

The most recent Israeli cyber-attack highlights the vulnerability of global water infrastructure. The apparent goal was to raise the level of chlorine in the water supply by changing the logic of the PLC without raising any alarms. According to cybersecurity experts "… they were trying to manipulate the chlorine levels and at the same time send operators a signal that the chlorine levels were fine".

SigaGuard offers absolute reliability for real-time detection of any cyber-attack on critical infrastructure.

- ✓ Totally autonomous / 100% Out-of-band
- ✓ Detection of preconfigured & "hidden" cyber events at OT level.
- ✓ Cannot be circumvented or compromised
- ✓ Independent validation of PLC output
- ✓ Data Archive - analysis, forensics & fast recovery
- ✓ Seamless installation / intuitive UI