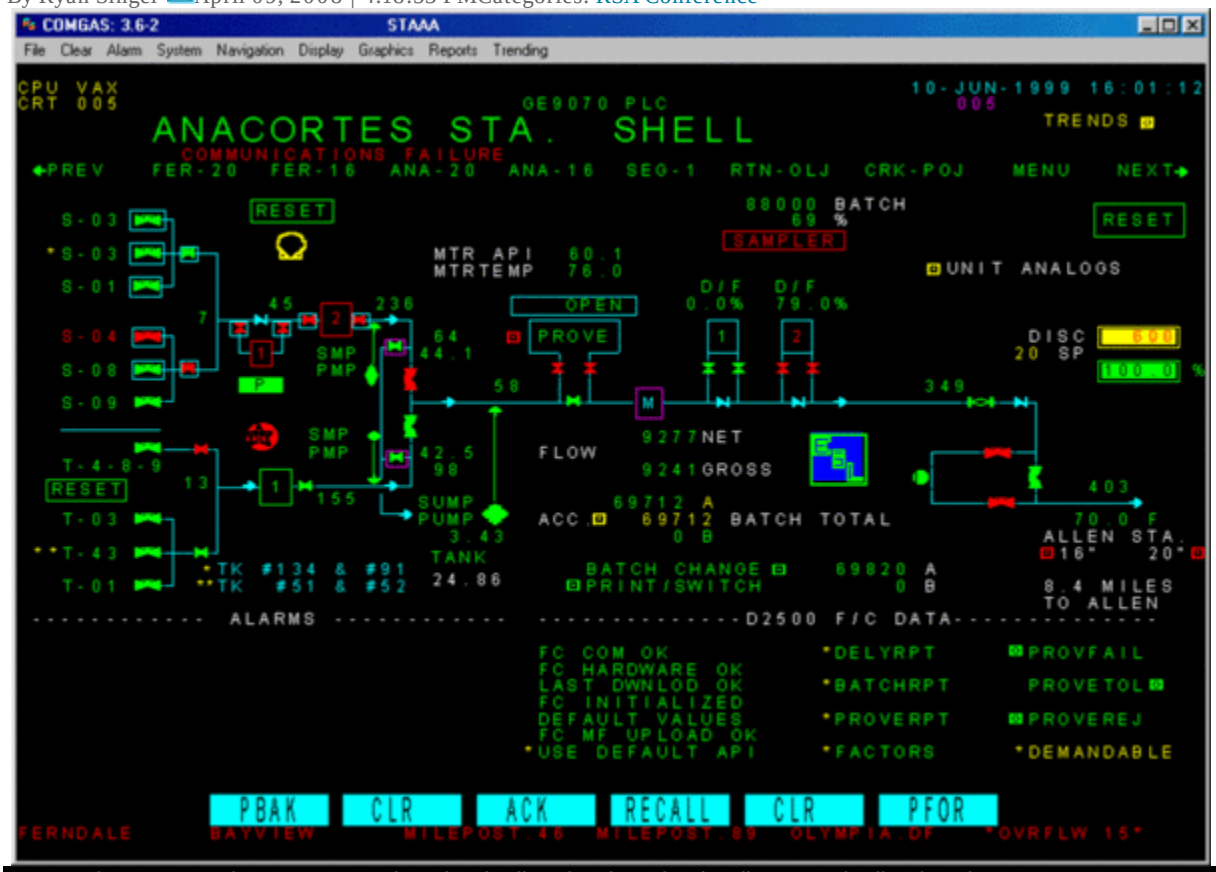
Industrial Control Systems Killed Once and Will Again, Experts Warn

By Ryan Singel April 09, 2008 | 4:18:53 PMCategories: RSA Conference



A control-system station screen at Olympic Pipeline the day of a deadly 1999 pipeline break.
Image: NTSB

On June 10th, 1999 a 16-inch diameter steel pipeline operated by the now-defunct Olympic Pipeline Co. ruptured near Bellingham, Washington, flooding two local creeks with 237,000 gallons of gasoline. The gas ignited into a mile-and-a-half river of fire that claimed the lives of two 10-year-old boys and an 18-year-old man, and injured eight others.

Wednesday, computer-security experts who recently re-examined the Bellingham incident called its victims the first verified human causalities of a control-system computer incident. They argue that government cybersecurity standards currently under debate might have prevented the tragedy.

"I've logged over 90 incidents in all industries worldwide," said Joe Weiss, managing partner at Applied Control Solutions, speaking at the RSA Conference in San Francisco. "The damage ranges from significant equipment failure to deaths."

Following the 1999 incident, a nearly three-year investigation by the National Transportation Safety Board concluded that multiple causes contributed to the deadly conflagration, including pipeline damage inflicted by construction workers years earlier, and a misconfigured valve.

But the factor that intrigues Weiss and fellow researcher Marshall Abrams, a scientist at MITRE, is a still largely unexplained computer failure that began less than 30 minutes before the accident and paralyzed the central control room operating the pipeline, preventing workers from releasing pressure in the line before it hemorrhaged.

With support from the U.S. National Institute of Standards and Technology, Weiss and Abrams pored over public government records on the incident, looking at it through the lens of a pending cybersecurity standard called NIST 800-53. The duo concluded that the requirements in the standard would have prevented the explosion from occurring.

"The NTSB concluded that if the SCADA system computers had remained responsive to the commands of the Olympic controllers, the controller operating the pipeline probably would have been able to initiate actions that would have prevented the pressure increase that ruptured the pipeline," reads the NIST report.

"These are the first fatalities from a control-system cyberevent that I can document, and for a fact say that this really occurred," Weiss said in an earlier interview with Wired.com.

Security experts and government investigators have long warned that the complex networks controlling critical infrastructures like the power grid, and gas and oil pipelines, were not built with security in mind -- a point driven home by several incidents of the systems failing. In January 2003, the Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant and disabled a safety-monitoring system for nearly five hours. Later that year, a software bug in a General Electric energy-management system contributed to a cascading power failure that cut off electricity to 50 million people in eight states and a Canadian province.

Piecing together the computer failure at Olympic is difficult. A system administrator, two control room operators and their supervisor all refused to testify in the resulting investigation, citing their Fifth Amendment right against self-incrimination. Several key system logs from the VAX VMS minicomputer from the time of the accident were missing or deleted, for reasons that have never been determined.

But the NTSB's original report faulted an unnamed computer operator for adding records to a database that was running on the pipeline monitoring system. The board also noted that the overall system had security design defects, since it had connections to the larger company network that was itself internet connected and had dial-up lines.

The board found no evidence of a computer attack from the outside, though. But Weiss, an outspoken evangelist for tighter control-system security standards, said he's suspicious of the NTSB's finding that the computer operator was at fault.

"The NTSB said he was doing database updates on the live system," Weiss said Wednesday. "What did he do on this day that he didn't do everyday?"

Abrams seems less convinced, suggesting the explosion was "probably" a combination of human error and a badly designed computer system, with a dose of bad luck thrown in for good measure.

Regardless, Abrams said the point is the same, and the casualties at Bellingham still count as victims of a cyber-incident.

"Control systems are just a special case of information technology," he said Wednesday.

The NIST 800-53 standard, which is due to be issued this year, will only be binding on federal agencies, but might be voluntarily adopted by critical infrastructure providers in the private sector. Included in the standard are immutable audit logs, individualized passwords, and user accounts that have only the permissions the person needs.

Bellingham had none of those precautions in 1999. Weiss said little has changed in the industry since then

"Until eight years ago, my whole life was making control systems usable and efficient, and, by the way, very vulnerable," Weiss said. "It is exactly what you will find today in many, many industrial applications. This isn't just 1999. No, this is June 2008."

(Kevin Poulsen contributed to this report)