3-14-13 Petition to the Chairman of the Nuclear Regulatory Commission to Establish a Substantive Regulation (ML13079A299)

Submitted by Dr. Alan Morris, P.E., Morris and Ward, Consulting Engineers, Chevy Chase, Maryland USA, Tel: 301-654-3606, email: morris.ward@verizon.net

(A) Petition

(1)   The petition is to install new-design programmable logic computers in the control systems of critical infrastructure facilities, which facilities in this case would be nuclear power plants, to block malware attacks on the industrial control systems of those facilities.

(2) Text of Proposed Rule: Install new-design programmable logic computers in the control systems of nuclear power plants, and train power plants staff in the programming and handling of the non-rewriteable memories.

(3) Interest is in protecting the critical infrastructure of the United States. The corporation that will head the implementation will buy the patents owned by the submitter.

(4) The Stuxnet malware attack conducted in mid-2010 against the programmable logic computers, which programmable logic computers, like all programmable logic computers then and now, had re-writeable memories, caused destruction of the centrifuges of the nuclear enhancement plant in Natanz, Iran. Since that time, the industrial control systems of all facilities have increasingly been enveloped in computer networks, all of which themselves are vulnerable to hacking, and which afford more and more pathways to the re-writeable memories of the programmable logic computers of the control systems.

(B) Potential Impact of Proposed Action

(1) The costs are quantifiable, and the do-nothing choice is to allow malware to maliciously reprogram the re-writeable memories of the present programmable logic computers.   The threat could even be from non-state expert hacker teams who have no fear of being caught. If an attack would be launched against a nuclear power plant, there could be effects of extensive physical damage and of fatalities.

(2) For the facility owners/operators, be they State, or Federal, or private, see (B)(1) above.

(3) Cost burden would be born by owners/operators.   Costs would be related to numbers of control systems per nuclear power plants, and to training of power plant staff.

(4) Nuclear power plants staffs would be trained to maintain and secure records of all memory programming, and maintenance in secure storage of programmed memories which may be again employed, as the control systems of critical facilities are essentially steady-state.

(5) Reduce impact on quality of the natural and social environments by stopping disastrous events at critical facilties.

Related to 3-14-13 Petition to Chairman of Nuclear Regulatory Commission

Topic: UPDATES FOR WINDOWS 7   (Sampling of recent security updates)

Cumulative Security Update for Internet Explorer 9 for Windows 7 for x64-based Systems (KB2809289)

Installation date: 3/12/2013 7:28 PM

Installation status: Successful

Update type: Important

Security issues have been identified that could allow an attacker to compromise a system that is running Microsoft Internet Explorer and gain control over it. You can help protect your system by installing this update from Microsoft. After you install this item, you may have to restart your computer.

More information:
http://go.microsoft.com/fwlink/?LinkId=279923

Security Update for Windows 7 for x64-based Systems (KB2799494)

Installation date: 2/14/2013 4:06 PM

Installation status: Successful

Update type: Important

A security issue has been identified that could allow an authenticated local attacker to compromise your system and gain control over it. You can help protect your system by installing this update from Microsoft. After you install this update, you may have to restart your system.

More information:
http://go.microsoft.com/fwlink/?LinkId=278914

Email: Sat 8/17/2013 2:29 PM
Subject: Protecting Critical Infrastructure Facilities (ML13249A304)

Dear Ms. Bladey:

This email is written in response to R.W. Borchardt's NRC letter to me of 8/9/13.
Critical infrastructure facilities include, for example, nuclear power plants (104 in the US) and hydroelectric dams (4300 in the US). The machinery of all these facilities is governed by a programmed computer (PLC) that is the heart of the industrial control systems at each of these facilities. For your information, the average nuclear power plant has 30 PLCs, each PLC with its own equipment group. Every PLC made, and every newly manufactured PLC, are equipped with a rewriteable memory that is programmed, and repeatedly reprogrammed, by the Operator in the Control Room, using a wire connected between the Operator's PC and the remotely located PLC.

The prime example of reprogramming of PLC rewriteable memories took place in mid-2010 in the control system of the nuclear enhancement plant in Natanz, Iran, accomplished, not by a Control Room Operator, but instead by malware. If the memory of the PLC had been non-rewriteable, the malware attack would have failed. This is the basic point that I made in the petition that I submitted to the NRC. Some in the regulatory agencies, e.g., NRC, FERC, decided my plan was correct, for they asked me to write a paper about non-rewriteable PLC memories, a paper which appeared in the DHS' ICSJWG Quarterly Newsletter of June 2012. In that paper, it was mentioned that the non-rewriteable, thus preprogrammed memories, would be taken by a Technician from the Control Room, where the memory was programmed, to the PLC, and insert the memory into the protected connection socket of the PLC. This action would require a brief, computerized safe shutdown of the zone of equipment controlled by the PLC. Shutdowns of plant equipment are also made by systems such as Bently Nevada shaft vibration monitors and set-point excursion monitors.

The same firms which make defensive software for protection of digital storage and digital networks, make defensive software for ICS and SCADA industrial systems. The types of defensive software are: firewalls, deep packer inspectors, whitelisters, and airgaps. The last mentioned, airgaps, are now in disrepute as reported in a paper in the August 2013 issue of the "Communications of the Association for Computing Machinery." It is important to note that digital storage and digital networks are daily hacked in the US.

The defensive software as applied to industrial control systems are meant to protect a single component from corruption, namely, the rewriteable memories of the PLCs. Hacking is becoming the province of the terrorists, placing critical infrastructure facilities at risk. For example, the news on 8/15/13 reported that in secretive chat rooms and on encrypted Internet message boards, al-Qaida fighters have been planning and coordinating attacks —the call to arms by the al-Qaida leaders uses a multilayered subterfuge to pass messages from couriers to tech-savvy underlings to attackers. The jihadists "tech-savvy underlings" employ sophisticated technology to avoid detection or cracking by NSA programs that were designed to uncover terror plots. Readily available devices, such as Shodan, aid hackers in finding pathways through defensive software.

If critical facilities find it unwarranted to replace their PLCs with a modern PLC, one with provision with exchangeable memories, and find it unwelcome to have scheduled brief shutdowns in one zone of equipment or another, then the critical facilities can wait until a hacker reprograms the rewriteable memories, with disastrous results.

Sincerely,
Alan Morris
Morris and Ward
Consulting Engineers
301-654-3606

Email: Wed 8/21/2013 10:19 AM
Subject: Proposed resolution (ML13249A314) Plus Attachment, 3 pages (ML13249A328)

Dear Ms. Bladey:

The corporations which know all details of my hacker-blocking technology (they all are active in cybersecurity) do not see a way ahead because sales, obviously to be kept confidential, would have to be done facility, by facility.   You recognize that the typical sales technique of advertising would serve to alert presently unaware hackers and tech-savvy terrorists about the crucial exploit to be taken advantage of. The most public analysis of the Stuxnet event was the web-published report of Symantec Corporation entitled "Stuxnet Dossier." Yet even as intelligent a corporation as Symantec did not specifically lay blame upon the underlying *rewriteable characteristic of the memories* of the PLCs (see, in the report, p.35 and following).

Our estimate of costs, for the 104 nuclear power plants, including 30 new-design PLCs per plant, installation of those PLCs, training of the Control Room staff in lock-down procedures for the SD memories when completing the programming of the memories, and the training of the Technician who will take the programmed memory from the Control Room, would be $550 million.

But the costs would increase because of the quiet, slow, individualized marketing approach. This then makes clear that the resolution is for the Government to buy my patent and technology (see 3pp. description attached), fund the application and filing of the International Patent, issue the regulation, and then contract with one of the corporations to implement my technology as set forth in the preceding paragraph, or, for the Government to allocate the funds to one of the corporations, which corporation would then buy my patent and technology, and move ahead with implementation once the regulation is issued.

Sincerely,
Alan Morris
301-654-3606

Title: Blocking Malware Attacks on Programmable Logic Controllers (PLCs) of Industrial Control Systems

A. Abstract:

The patent is for non-rewriteable memories, here used with PLCs, for providing means for monitoring from without that the preprogrammed memory is inserted into the socket within the closed, locked, alarmed cover of the PLC, and, for providing means for monitoring from without the specific identity of the inserted memory.

B. Introduction:

1. An industrial control system (ICS) is used to control equipment in a local area such as a production plant, while a supervisory control and data acquisition (SCADA) system is used to control equipment in a wide geographical area such as an electric power grid.   A SCADA system can be thought of as a subset of ICS.   For purposes of this document, reference will be made to ICS as the general case.

2. The basic element of an ICS is an industrial controller known as a Programmable Logic Computer (PLC).   Programmed into the memory of the PLC are the operations of the equipment in the ICS. When PLCs were developed in the early 1970's, they were used to replace racks of relays in control systems for automobile assembly lines. In more recent times, while PLCs are still utilized, there have emerged combinations of PLCs with other units such as programmable automation controls (PACs) and programmable fieldbus controllers (PFCs).   For purposes of this document, reference will be made to PLC as the general case.

3. Malware and viruses are developed by hackers and hacker teams to attack the ICSs of critical facilities, so as to destroy equipment and threaten human life.   The attacks can be carried out by state and non-state teams with little or no risk of detection or attribution. Critical facilities include, for example, nuclear power plants, hydroelectric dams, oil/gas pipelines.   An example of a destructive malware attack is the 2010 Stuxnet malware attack on the ICS of the Natanz nuclear enhancement plant in Iran. There, Stuxnet was designed to alter the programming stored on the memories of the PLCs of the Natanz ICS, to cause dangerous changes in rotational speeds of the refining centrifuges, causing 1,000 centrifuges to destruct.

4. Stuxnet was able to alter the programming stored on the memories of the Natanz PLCs because the memories were rewriteable.   PLCs with rewriteable memories were originally developed in an era that was free of malware attacks. This rewriteable characteristic is the same for the memories of all extant PLCs in ICSs around the world, and is the same for PLCs now being produced and sold.   Alternatively, a PLC memory having a non-rewriteable characteristic, once programmed, cannot be written-to again, and will block malware from altering the programming stored on that memory.

5. Facilities seek to protect their ICSs against malware attack with defensive software, including firewalls, deep packet inspectors, and whitelisters.   Hackers teams have computerized methodology, such as fuzzing and Shodan, to find connectivity paths and zero-day faults through which to reach their targets of rewriteable PLC memories.

6. The rewriteable memories of PLCs are fixed-in-place on a circuit board of the PLC, are programmed-in-place, and are reprogrammed-in-place.   When, instead, non-rewriteable memories are utilized in PLCs, the PLC must be configured such that a programmed non-rewriteable memory can be inserted into, or removed from, an exterior socket on the PLC.

C. Non-Rewriteable Media as the Memory in a PLC:

1.   Non-rewriteable data storage media are available as solid state, non-volatile memories, which presently include NOR Flash, and SD Cards. However, NOR Flash and SD Cards are not inherently non-rewriteable; both require dedicated programming steps to become non-rewriteable. Connecting sockets are available for NOR Flash memories and for SD Card memories.

2.   The non-rewriteable memories of a new design PLC must be removable and insertable, using connecting sockets in the PLC. The memory connecting socket is necessary because, once programmed, the program stored on the non-rewriteable memory cannot be rewritten.   If change of programming for the memory in a PLC is needed, a new non-rewriteable memory will have been programmed, and taken by the Technician to the PLC, for insertion in the socket of the PLC.

D. Concept PLC:

1. The concept PLC will have an exteriorly located socket for insertion of a non-rewriteable memory. The socket will have a hinged cover which, when open, will make the socket available to the Technician for removal of an inserted memory, and for insertion of a memory. The hinged cover will have features such as being gasketed and lockable, with the cover and lock alarmed against tampering.

E. Operational Aspects:

1. The programming of the non-rewriteable memory could take place in the Control Room of the ICS. The memory programming methodology, and the needed circuitry for programming, will be in accordance with the manufacturer's procedures for the type of solid state memory being utilized. The lock-down, or write-protect, of the blocks or sectors of the memory will be instituted during the programming procedures of the memory.   There will be a programming box with socket for the memory. The box will be placed adjacent to, and connected to the Control Room Operator's PC. The box will contain the circuitry for programming of the memory.

2.   Solid-state memories, because of their small physical size, or of their connecting pin fragility, or of potential static electricity damage, may need to be handled, in accordance with the memory manufacturer's recommendations, using a grounded tool, when, for example, the memory is being inserted into, or removed from, a socket, or being placed into, or removed from, a container.

3. After the memory is programmed, and lock-down or write-protect is performed, the data stored on a block or sector, or the entire data storage on the memory, will be checksummed in accordance with the memory manufacturer's checksum procedure for the type of memory being utilized.   The calculated datum from the checksum algorithm will be stored in the Control Room for record purposes.

4. The programmed non-rewriteable memory will be placed into a shielded box for transport by the Technician from the Control Room to the designated PLC. The shielded box for the memory will prevent pin damage from handling, and will prevent potential static electricity damage.   If there is a memory presently inserted in the PLC, the Technician will also take a second, empty shielded box.

5. Before the programmed non-rewriteable memory can be removed from the PLC, and a subsequent programmed non-rewriteable memory inserted into the PLC, there must be a safe shutdown of the equipment in the zone of the ICS controlled by the PLC.

6. For the unlocking and opening of the PLC's cover, and for the changing of the memory within the PLC, the Technician can be in telephony contact with the Operator in the Control Room, until such time as the memory changing task is completed.   The Technician will remove the present memory from the PLC and place it into the empty shielded box for return to the Control Room. The Technician will insert the newly programmed memory into the socket within the PLC. The PLC cover will be closed, locked, and the cover lock security alarm will be set.

7.   After the memory is in the socket within the closed, locked, alarmed cover of the PLC, the PLC will be powered on, but the Command for the PLC to run will not be authorized by the Operator. There will first be a checksum procedure of the storage on the memory in the socket locked within the PLC, that being the memory that had been checksummed in the Control Room after programming procedures for that memory had been completed. This confirmation checksumming will be done by cable connection to the Control Room. If the checksum datum agrees with the checksum that had been calculated and stored in the Control Room, that would mean that the memory locked within the PLC is the specific memory, and that the Operator can issue the Command for the PLC to run, and for the equipment in the zone controlled by the PLC to restart.

F.   Modified Production PLC:

1. Certain modern production PLCs have been evaluated by independent testing staffs and found to be free of exploits.   The PLC enclosures have on their exterior a memory socket into which a non-rewriteable memory would be inserted. The wiring of the socket would be connected to a new memory circuit board within with short connecting wires. Further modification features of a production PLC can include, a hinged cover over the memory socket that is gasketed, lockable, and the lock alarmed against tampering (as described above in D1).

2.   Because of facility environmental conditions in which PLCs are utilized, the PLC enclosure and its components will be designed and tested so as to function properly in expected ranges of facility temperature, humidity, and vibration

Email: Wed 8/21/2013 1:43 PM
Subject: Symantec W32 Stuxnet Dossier (ML13249A334)

Dear Ms. Bladey:

I located one of the Symantec Stuxnet Dossier reports on the web. In this report, the description of "Modifying PLCs" starts on p. 36:
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Note that Symantec employs the word "modifying," for even Symantec doesn't know that what is actually taking place is due to the fact that the program written on the *rewritable* PLC memory is being *rewritten*. Here is what Symantec states at the beginning of p. 36:

Modifying PLCs

Resource 208 is dropped by export #17 and is a malicious replacement for Simatic's s7otbxdx.dll file. First, it's worth remembering that the end goal of Stuxnet is to infect specific types of Simatic programmable logic controller (PLC) devices. PLC devices are loaded with blocks of code and data written using a variety of languages, such as STL or SCL. The compiled code is an assembly called MC7. These blocks are then run by the PLC, in order to execute, control, and monitor an industrial process. The original s7otbxdx.dll is responsible for handling PLC block exchange between the programming device (i.e., a computer running a Simatic manager on Windows) and the PLC. By replacing this .dll file with its own, Stuxnet is able to perform the following actions:
Monitor PLC blocks being written to and read from the PLC.•
Infect a PLC by inserting its own blocks and replacing or infecting existing blocks.•
Mask the fact that a PLC is infected

Sincerely,
Alan Morris
301-654-3606

Email: Wed 8/21/2013 6:43 PM
Subject: Far simpler plan (ML13249A344)

Dear Ms. Bladey:

It occurred to me that there is a far simpler action plan. NorthropGrumman has a cybersecurity department headed by Michael Papay. He is well acquainted with my technology.   NGC cybersecurity has set up teamship with Areva.   Areva is a facilities service corporation, headquartered in Paris, with US offices in NewportNews, Virginia. All that need be done is for NRC to request NGC to buy my patent and technology, and move ahead, with Areva, to implement my technology in the nuclear power plants. This, of course, requires that my petition to NRC be made into a regulation, so that both NGC and Areva can move ahead.

Please contact Mike via email at: Michael.Papay@ngc.com   When Mike contacts me, I will send him update information.

Sincerely,
Alan Morris
301-654-3606

Email: Fri 8/23/2013 9:33 AM
Subject: Digital Bond's comments (ML13249A346)

Dear Ms. Bladey:

Dale Peterson, of Digital Bond, has commented on ICS security for many years.   This week, while studying the new GE RTU device, stated as follows:

> "The asset owner is also supported by a conspiracy of silence perpetrated by the automation press, vendors, industry organizations and government organizations (DHS et al). They all say critical infrastructure is essential, but they never actually say out loud these insecure by design devices and protocols need to be replaced or upgraded now. "

"Asset owner" is the owner of the critical facility, e.g., nuclear power plant. "Conspiracy of silence" is obvious. "They all say critical infrastructure is essential" but they "never say out loud these insecure devices need to be replaced……"

You can see that my hacker-blocking technology cannot be sold door-to-door, not only from what I have stated in my petition and in my emails, but now also as stated so clearly by Peterson.

Help is needed.

Sincerely,
Alan Morris

Email: Tue 8/27/2013 11:38 AM
Subject: Additional email for "Petition for Nuclear Power Plants 3-14-13" (Edit change in 2nd and 3rd lines) (ML13249A347)

Dear Ms. Bladey:

Here below is the announcement by ISA of the publication of their new standard that addresses risk from the growing use of *business IT* in dangerous ICS systems.   My view is that IT connectivity of ICS systems leads to more and more pathways for hackers to exploit, meaning it is increasingly important that the memories of the PLCs be changed to non-rewriteable, in accordance with the Petition of 3-14-13.

New ISA99 cyber security standard defines key technical requirements for secure industrial control systems

Research Triangle Park, North Carolina, USA (20 August 2013) – The ISA-62443 series of standards, being developed by the ISA99 committee of the International Society of Automation (ISA) and adopted globally by the International Electrotechnical Commission (IEC), is designed to provide a flexible framework to address and mitigate current and future vulnerabilities in industrial automation and control systems (IACS).

A newly published standard in the series, ISA-62443-3-3-2013, *Security for Industrial Automation and Control Systems Part 3-3: System Security Requirements and Security Levels,* addresses risks arising from the growing use of business information technology (IT) cyber security solutions to address IACS cyber security in complex and dangerous manufacturing and processing applications

Sincerely,
Alan Morris

Please docket as PRM-73-17 the attached document as PRM-73-17. It has been added to ADAMS under ML13079A299. The Petition and associated documents are in ADAMS package ML13249A306.

Cindy

Cindy Bladey, Chief
Rules, Announcements, and Directives Branch
3WFN 06-B02
301-287-0949
cindy.bladey@nrc.gov

AMENDMENT TO PETITION DATED DECEMBER 19, 2013

From: Morris and Ward [mailto:morris.ward@verizon.net]
Sent: Thursday, December 19, 2013 5:21 PM
To: Bladey, Cindy
Subject: RE: Petition

Dear Ms. Bladey:

The comments are going to be cruel, because I forgot to mention in the petition the safe, programmed shutdown for changing of the preprogrammed, non-rewriteable memories. Recall I wanted to add that sentence to the petition, but it was ruled too late to add. The standard shaft vibration detection systems, installed for maintenance guidance for plant motors and generators, have those custom shutdown programs, and all that need be done is to utilize those extant programs.

Here was the added paragraph 5 for Section A:

(5) Before the programmed non-rewriteable memory can be removed from the PLC, and a subsequent programmed non-rewriteable memory inserted into the PLC, there must be a safe, programmed shutdown of the zone of equipment controlled by the PLC. This is analogous to the safe, programmed shutdowns commanded by shaft vibration monitors and set-point excursion monitors

Sincerely,
Alan Morris