Institute for Science and International Security

ISIS Report

Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?

By David Albright, Paul Brannan, and Christina Walrond
December 22, 2010
Preliminary Assessment

In late 2009 or early 2010, Iran decommissioned and replaced about 1,000 IR-1 centrifuges in the Fuel Enrichment Plant (FEP) at Natanz, implying that these centrifuges broke. Iran's IR-1 centrifuges often break, yet this level of breakage exceeded expectations and occurred during an extended period of relatively poor centrifuge performance.

Although mechanical failures or operational problems have often been discussed as causing problems in the IR-1 centrifuges,[1] the crashing of such a large number of centrifuges over a relatively short period of time could have resulted from an infection of the Stuxnet malware.[2] This malicious code seeks to take over an industrial control system in order to destroy equipment while hiding its presence.[3] Given Stuxnet's much greater prevalence in Iran compared to other countries, it is likely that this malware was aimed at Iran. Stuxnet covertly changes the frequencies of certain types of frequency converters, which control the speed of motors. The frequencies listed in Stuxnet's attack sequences, including the nominal frequency of a motor, imply that a target is the IR-1 centrifuge.[4] However, Stuxnet's exact purpose or its overall effect on the FEP remains hard to assess. If Stuxnet's goal was the destruction of all the centrifuges in the FEP, Stuxnet failed. But if its goal was to destroy a more limited number of centrifuges and set back Iran's progress in operating FEP while making detection of the malware difficult, it may have succeeded, at least for a while.

Iranian Statements

Although Iran has not admitted that Stuxnet attacked the Natanz centrifuge plant, it has acknowledged that its nuclear sites were subject to cyber attacks. President Mahmoud Ahmadinejad recently admitted that a software attack affected Iran's centrifuges. "They succeeded in creating problems for a limited number of our centrifuges with the software they had installed in electronic parts," he told reporters at a media conference.[5]

[1] David Albright and Christina Walrond, "Iran's Gas Centrifuge Program: Taking Stock," Institute for Science and International Security, February 11, 2010: http://isis-online.org/isis-reports/detail/irans-gas-centrifuge-program-taking-stock/8. See also supplement to this report at http://isis-online.org/isis-reports/detail/supplement-to-irans-gas-centrifuge-program-taking-stock/8.

[2] Stuxnet is called malware in this report, although media reports refer to it as a worm or a virus. The more general term is used since Stuxnet appears to contain several types of malware.

[3] Stuxnet is analyzed in Nicolas Falliere, Liam O. Murchu, and Eric Chien, *W32.Stuxnet Dossier version 1.3* November 2010; and by Ralph Langner, see www.langner.com.

[4] *W32.Stuxnet Dossier version 1.3*, op. cit.; and Albright and Andrea Stricker, "Stuxnet Worm Targets Automated Systems for Frequency Converters: Are Iranian Centrifuges the Target?" ISIS Report, November 17, 2010 (corrected): http://isis-online.org/isis-reports/detail/stuxnet-worm-targets-automated-systems-for-frequency-converters-is-irans-ce/8

[5] "Iran says cyber foes caused centrifuge problems," Reuters, Nov 29, 2010.

The timing of the removal of about 1,000 centrifuges is consistent with another Iranian official's statement of when Iran suffered a cyber attack. On November 23, 2010, Ali Akbar Salehi, then head of Iran's Atomic Energy Organization and current acting foreign minister, confirmed to IRNA that malware had indeed reached Iran: "One year and several months ago, Westerners sent a virus to [our] country's nuclear sites." If an attacker succeeded in introducing Stuxnet in early or mid-2009 into vulnerable Iranian personal computers connected to the internet, the malware could have taken months to arrive at the Natanz centrifuge control systems. Because the Natanz control systems are not connected to the internet, Stuxnet would have needed to travel on a removable drive from an infected computer to the Natanz control system. Natanz personnel could have unknowingly transported Stuxnet after using infected personal computers. Perhaps the attackers first targeted the personal computers of Natanz personnel.

Iran has downplayed the significance of any cyber attack. Salehi in his November 23 statement said, "We discovered the virus exactly at the same spot it wanted to penetrate because of our vigilance and prevented the virus from harming [equipment]." As discussed above, President Ahmadinejad characterized the damage as confined to a limited number of centrifuges. However, if Stuxnet did attack Natanz, the data collected by the International Atomic Energy Agency (IAEA) implies far more serious disruption and damage.

Supporting Data from IAEA Safeguards Reports

Quarterly IAEA safeguards reports shed some light on disrupted centrifuge operations at Natanz. Table 1 tabulates information from these reports on the number of cascades enriching, under vacuum, or installed during several reporting periods in modules A24, A26, and A28 at the FEP. Centrifuges spin when they are enriching and usually spin when they are under vacuum but not being fed with uranium hexaflouride (UF_6). The data is given by cascade, where each cascade contains 164 IR-1 centrifuges. Therefore, 1,000 centrifuges correspond to about six cascades and represent over ten percent of the peak number of centrifuges installed at the FEP.

The February 18, 2010 IAEA safeguards report on Iran indicates that centrifuges in 11 of the 18 cascades in module A26 were disconnected, and these cascades were by implication no longer under vacuum. A module contained a total of 2,952 IR-1 centrifuges in 18 cascades; these 11 cascades contained 1,804 IR-1 centrifuges. Six cascades in module A26 continued to be fed with uranium hexafluoride. All but one cascade in module A24 continued to be listed as enriching uranium. In addition, cascades in module A28 were not under vacuum or being fed uranium hexafluoride, but centrifuges in two cascades were being removed.

By contrast, the previous safeguards report, dated November 16, 2009, reflected the steady increase in the number of centrifuges installed at the FEP, reaching a peak of 8,692 IR-1 centrifuges (see figure 1). For several months, however, the FEP had experienced operating problems that reduced the number of centrifuges enriching uranium but did not stop Iran from continuing to install centrifuges in module A28.

The most noticeable impact was on module A26, which was the second module installed at the FEP, A24 being the first. The installation of centrifuge cascades in A26 was underway by early 2008. The commissioning proceeded well and by June 2009, 12 cascades were enriching and six others were under vacuum. Then by August 2009, there were two fewer cascades being fed with uranium hexafluoride and two more under vacuum but not enriching. In November 2009, the number enriching had decreased further to six cascades, with 12 cascades under vacuum. Some type of problem likely accounted for the decrease in the number being fed with uranium. Sometime between November 2009 and late January 2010, module A26 suffered a major problem with at least 11 cascades directly affected.

The cascades being fed with uranium may have likewise suffered excessive breakage and operational difficulties. The FEP is designed to allow rapid replacement of broken centrifuges, since the IR-1 centrifuge breaks relatively frequently under normal operations. Officials close to the IAEA have stated that the failure rates can amount to ten percent per year. It is possible that the enriching cascades in A26 and perhaps A24 experienced disruptions, but the plant operators made it a priority to replace broken centrifuges in these cascades quickly and continued feeding these cascades with uranium hexafluoride.

Any effect is camouflaged since the rate of low enriched uranium (LEU) production increased significantly during the three month reporting period between November 2009 and February 2010. This gain was sustained in the months afterwards (see figure 2). However, this rate is far below what the IR-1 centrifuges were designed to achieve. Thus, Iran may have failed to achieve its expected LEU production levels.

Traditional Reasons for Centrifuge Problems

Iran's centrifuges, particularly those installed in module A26, could have suffered from a systemic problem in manufacturing components or assembling centrifuges, leading to large-scale breakage in late 2009 or early 2010. One suggestion is that module A26 is filled with centrifuges that were poorly manufactured or assembled, making them vulnerable to crashing, which finally occurred on a large scale. It would be unusual, although not impossible, for the second module to be composed of centrifuges made more poorly than those in the first module, A24, which has run relatively well. This may indeed be the case, but this does not explain why it took so long for the A26 centrifuges to fail.

Another possibility is that contrary to Iranian statements, module A26 was the first one Iran built from domestically manufactured centrifuge components, and at least some of these parts suffered from serious flaws. Although Iran told the IAEA that it manufactured the centrifuges in A24, it is conceivable that the Khan network provided far more centrifuges than the 500 P1 centrifuges, renamed IR-1, acknowledged by both Pakistan and Iran. However, there is no evidence of such a transfer, which would entail the provision of up to 2,500-more P1 centrifuges, since module A24 holds almost 3,000 centrifuges.

Link of Stuxnet to the IR-1 Centrifuges

Given the questions about more traditional explanations of the problems in module A26, it is natural to consider whether Stuxnet impacted the performance of this module. Symantec has identified at least two distinct infection sequences in Stuxnet that could destroy centrifuges.[6] These two sequences, called A and B by Symantec, are similar in nature but differ depending on the type and number of frequency converters, one type of which is manufactured by the Iranian firm Fararo Paya, and the other by the Finnish company Vacon. In centrifuge cascades, frequency converters drive individual centrifuge motors and precisely control the rotational speed of a rotor.

However, ISIS could find no confirmation that the FEP has these types of frequency converters. The types of frequency converters used at the FEP are not discussed in IAEA safeguards reports. Moreover, according to officials close to the IAEA, although Iran declared much of its centrifuge-related equipment in the FEP in the mid-2000s, it did not declare the source or types of frequency converters used there. The IAEA is unaware of the exact ones used at the FEP, according to these officials. If Stuxnet targeted the FEP, its authors would have used information not available to the IAEA.

In the Stuxnet code, there are two specific links to the IR-1 centrifuge. In one subsequence of Stuxnet's infection sequence A, the nominal frequency of the motor is listed as 1064 Hz.[7] In this same subsequence, after commanding a reduction in the frequency, Stuxnet returns the frequency to this nominal value of 1,064 Hz. According to a senior official close to the IAEA, the nominal frequency of the IR-1 is 1065 Hz, which corresponds to an IR-1 centrifuge wall speed of 334 meters per second. An official from a government that

[6] *W32.Stuxnet Dossier version 1.3*, op. cit., p. 35.

[7] *W32.Stuxnet Dossier*, op. cit., table 12. These values appear in infection sequence A, sequence 2, subsequence 2 (or Frames 2.2) against Vacon NX frequency converters.

closely tracks Iran's centrifuge program stated in a mid-2008 interview with ISIS staff that the IR-1 centrifuge's nominal frequency is 1064 Hz. He noted that Iran kept the actual frequency lower in an effort to reduce the number of centrifuges that break; an official close to the IAEA said that Iran often runs its centrifuges at 1007 Hz, or a wall speed of 316 meters per second. This 2008 interview, before Stuxnet is believed to have been introduced into Iran, confirms that even without the malware's effect, Iran's centrifuges experienced an unusual amount of breakage and that breakage was sensitive to the centrifuge's frequency of rotation.

Another link between the IR-1 centrifuge and Stuxnet is the maximum frequency listed in one of the attack sequences. Stuxnet commands an increase in the frequency to a maximum of 1410 Hz. For the IR-1 centrifuge rotor, this frequency corresponds to a tangential wall speed of 443 meters per second, very close to the maximum speed the spinning aluminum IR-1 rotor can withstand mechanically. The rotor tube of the IR-1 centrifuge is made from high strength aluminum and has a maximum tangential speed of about 440-450 meters per second, or 1,400-1,432 Hz, respectively.[8] As a result, if the frequency of the rotor increased to 1410 Hz, the rotor would likely fly apart when the tangential speed of the rotor reached that level.

Ambiguity about Stuxnet's Attack Sequences

The specific goals of Stuxnet's attacks are not fully understood. Likewise, very little is known about the actual progression of each attack and the FEP's counter-measures to an attack. But Stuxnet at a minimum appears intended to disrupt operations and increase the number of centrifuges that fail while carefully disguising the malware's presence from the operator. To that end, each attack sequence sends commands to shut off the frequency converters' warning and safety controls aimed at alerting operators of the speed up or slow down.

Each attack could destroy large numbers of centrifuges. Prominent in the code is the term "DEADFOO7," which could stand for dead foot, an aviation adage used to denote a dead engine.

Based on Symantec's deciphering of infection sequence A, which is the attack involving a preponderance of Finnish frequency converters, Stuxnet can destroy centrifuges.[9] In sequence A, there are two specific attacks that are separated by about a month.[10] The first, called sequence one, would raise the speed of the centrifuge as high as a frequency of 1,410 Hz during a 15 minute attack, before the malware returns the control system to normal operation. After waiting about 27 days, Stuxnet would launch attack sequence two. The first part of this attack would lower the frequency toward 2 Hz and last 50 minutes. The second part would raise the frequency back to the nominal frequency of 1,064 Hz. After another 27 days, the first attack sequence would start again; followed by sequence two 27 days after that.[11]

However, Stuxnet's effects may also be more subtle, disrupting operations without destroying all the centrifuges in the plant. For example, the time for an attack is limited. During the fifteen minute attack that raises the frequency to 1,410 Hz, the motor (or the centrifuge) may not reach this maximum frequency that would guarantee its destruction. The attack appears to end before this maximum is obtained, although the

[8] Iran's IR-1 rotor tubes use 7075-T6 aluminum. The IR-1 has four such tubes connected by three maraging steel bellows.

[9] Infection sequence A is better understood than infection sequence B, which focuses on the Iranian frequency converters. In particular, the specific attack sequences in B are not yet deciphered.

[10] For more detail on infection sequence A, see *W32.Stuxnet Dossier*, op. cit., pp 35-42, especially pp. 40 and 42.

[11] Despite progress in deciphering Stuxnet, there remain significant questions about the impact of infection sequence A on centrifuges. For example, subsequence two of attack sequence one is not deciphered. After raising the speed to 1,410 Hz during attack subsequence one, which lasts 15 minutes, does the second subsequence order a return to the nominal frequency? Or does Stuxnet just seek to destroy the greatest number of centrifuges in the first part of attack sequence one? If so, a return to a nominal frequency in the second subsequence may have been viewed as unnecessary? In that event, however, the purpose of attack sequence two is difficult to understand, since it would be superfluous or far less destructive in nature than sequence one. In addition, the alternating of sequences one and two every 27 days could imply a strategy of disruption rather than quick destruction of centrifuges.

speeds achieved are so great that destruction may be guaranteed in any case.[12] In the attack that lowers the frequency to a minimum of 2 Hz, the slowdown time may be so long that the frequency can be reduced by less than 200 Hz before the attack ends. In addition, the FEP may have control systems that act independently of the Stuxnet malware to protect the centrifuges.

During an attack, Stuxnet seizes control of a specific, but widely possessed, Siemens central processing unit (CPU) that must also be connected to a particular communication processor that in turn controls the frequency converters. Iran obtained this general type of Siemens CPU in 2002 or 2003, and the IAEA established that Iran likely diverted these controllers to its nuclear program. Siemens subsequently stopped selling its controllers to Iran. If Iran obtained more, it did so through illicit trade or smuggling operations. Although Iran could very well have succeeded in acquiring this control equipment illicitly after 2003, it would be less likely to reveal such purchases to the IAEA, which regularly inspects the FEP. Iran has never allowed the IAEA to view the FEP's control equipment in sufficient detail to learn the exact type of controllers used, according to an official close to the IAEA. If Stuxnet's target were the FEP, its authors apparently would have known that this Siemens CPU and associated communications modules controlled the plant's frequency converters.

An important question is whether the targeted Siemens CPUs control all the module's operations. In particular, it is unclear whether Stuxnet seizes control of the entire module's control systems or only a portion of them. Other control systems may inhibit Stuxnet from destroying centrifuges during an attack sequence. For example, if a centrifuge rotor assembly were to run down with the uranium hexafluoride inside, the rotor could become unbalanced and "crash," or break. As a result, in the event of a malfunction, the safety systems are designed to quickly empty the centrifuges of uranium hexafluoride.[13] Symantec stated in a comment to ISIS that its researchers found no code in Stuxnet that would block the dumping of uranium hexafluoride from the centrifuges. Thus, it remains unclear whether safety systems independent of the control system targeted by Stuxnet would intervene to save the centrifuges or reduce the number destroyed. In this case, the FEP's operations would be disrupted and likely slowed.

Was Module A24 Attacked?

While the breakage in module A26 may indicate that Stuxnet affected its centrifuges, this malware may have also attacked module A24. The effects may not have been apparent if Iran rapidly replaced any broken centrifuges. However, module A24's lack of any obvious, widespread damage could also mean that its control system was not infected. It may use control units not listed as targets in Stuxnet. Alternatively, its cascades might not use enough of certain types of frequency converters to trigger an attack by Stuxnet. Before

[12] The malware instructs the Vacon frequency converters to speed up at a rate of 0.3525 Hz per second during the bulk of the attack. There remains uncertainty about whether the increase is described linearly throughout its range or has an S-shape at the beginning and end. However, the effect of an S-shape curve is to reduce somewhat the top frequency obtained during the attack. A more fundamental problem is that this attack subsequence does not give the starting frequency. If the speedup rate is linear and the starting frequency is 1,007 Hz or 1,064 Hz, after 15 minutes the frequency would be 1,324 Hz or 1,381 Hz, respectively. These frequencies imply a fast rotor speed, but they are below the maximum frequency of 1,410 Hz or a rotor speed which would certainly result in the rotor breaking from material considerations alone. However, these frequencies may exceed the first flexural resonant frequency, in which case the rotor would also break.

[13] For example, each IR-1 centrifuge has a vibration sensor, and any vibration over a certain tolerance can cause the control system to isolate the centrifuge and transfer the uranium hexafluoride gas in the cascade to a dump tank. The reason is that the IR-1 is vulnerable to vibrations that if left unchecked can destroy the centrifuge. The shock wave from a crashing centrifuge can destroy other centrifuges in the cascade. In addition, the control system may automatically reduce the centrifuge's speed in a controlled manner. If this command originated in another control system, would Stuxnet override this command?

launching an attack, the malware searches for sufficient number of Fararo Paya and Vacon frequency converters.[14]

In fact, Iran obtained frequency converters from a variety of overseas suppliers, including German and Turkish companies. Some Turkish frequency converters in use at the Natanz pilot centrifuge plant reportedly experienced sabotage by a foreign intelligence service, although the damage was limited.[15] Iran has depended on its smuggling networks to obtain centrifuge-related goods illicitly. In its pursuits to purchase this component, it has changed suppliers several times. The FEP may thus have large numbers of these frequency converters, whose presence could in effect suppress a Stuxnet attack. Moreover, during an attack, this type of frequency converter may not be ordered to change its frequencies.

Post-Event Impact

President Ahmadinejad said that Iranian experts discovered the cyber attack and took steps to prevent it from having an impact or from recurring. [16] However, it remains unclear when Iran learned the FEP could be under cyber attack, and whether its computers and control systems at Natanz are now clear of Stuxnet. Western cyber experts are skeptical that Iran's centrifuge program is free of Stuxnet.[17]

The data in the IAEA reports show that as of August 2010, the number of cascades under vacuum in module A26 had not yet returned to November 2009 levels. Six cascades were still not under vacuum or being fed uranium hexafluoride. Data about specific modules is not included in the November 2010 IAEA safeguards report. This report states that Iran has increased the number of centrifuges being fed with uranium hexafluoride by about 1,000, but it does not state whether these centrifuges are in module A26 or A28.

After February 2010, the rate of LEU output remained steady for many months, although still far below optimal levels. However, Iran fed proportionally more uranium hexafluoride into its cascades to get this LEU output (see figure 3). The amount of uranium hexafluoride feed proportionate to LEU output increased between the date of the February 2010 report and the August 2010 report, as compared to three months up until February 2010. This could indicate that Iran's centrifuges did not enrich efficiently during this extended period. Whether this is due to Stuxnet is unknown.

In mid-November 2010, Iran temporarily halted enrichment at the FEP following widespread fluctuations in centrifuge operations. It did not give any reason for this unusual action. Was this shutdown necessitated due to damage from Stuxnet, or was it an attempt by Iran to purge Stuxnet from the FEP? The latter would certainly be an Iranian priority.

Conclusion

Although Stuxnet is a reasonable explanation for the apparent damage to module A26, questions remain about this conclusion. The attacks seem designed to force a change in the centrifuge's rotor speed, first raising the speed and then lowering it, likely with the intention of inducing excessive vibrations or distortions that would destroy the centrifuge. But still unknown are parts of the attack sequences and possible responses by the FEP

[14] *W32.Stuxnet Dossier version 1.3*, op. cit. Vacon NX frequency converters and Fararo Paya part number KFC750V3 are searched for by Stuxnet. Before Stuxnet launches an attack, it looks for a range of criteria, including counting at least 33 times the Profibus identification numbers of these two types of frequency converters. Each cascade would be expected to have at least two frequency converters, implying that Stuxnet targets modules.

[15] *The New York Times* reported on January 3, 2010 that one foreign intelligence operation involved sabotaging "individual power units that Iran bought in Turkey" for its centrifuge program. These power units are interpreted to be frequency converters.

[16] "Iran says cyber foes caused centrifuge problems," Reuters, Nov 29, 2010.

[17] Langner, www.langner.com

control system. These responses could act during the attack to reduce the magnitude of the change in frequency or otherwise act to protect the centrifuges. A priority is better characterizing Stuxnet's attack sequences and determining Stuxnet's goals in a centrifuge plant. If its goal was to quickly destroy all the centrifuges in the FEP, Stuxnet failed. But if the goal was to destroy a more limited number of centrifuges and set back Iran's progress in operating the FEP, while making detection difficult, it may have succeeded, at least temporarily.

A Final Concern

For many years, governments have pursued methods to disrupt Iran's ability to procure goods illegally overseas for its nuclear programs, particularly its gas centrifuge program. Such overt and covert disruption activities have had significant effect in slowing Iran's centrifuge program, while causing minimal collateral damage. In contrast to overt military strikes, there is an appeal to cyber attacks aimed at a centrifuge plant built with illegally obtained, foreign equipment, and operating in defiance of United Nations Security Council resolutions. However, Stuxnet appears to have spread unintentionally and well beyond its targets. Part of the reason is in the design of Stuxnet, which needs to spread in order to increase its chance of infecting an industrial control system via a removable drive used with an infected computer. It is important for governments to approach the question of whether using a tool like Stuxnet could open the door to future national security risks or adversely and unintentionally affect U.S. allies. Countries hostile to the United States may feel justified in launching their own attacks against U.S. facilities, perhaps even using a modified Stuxnet code. Such an attack could shut down large portions of national power grids or other critical infrastructure using malware designed to target critical components inside a major system, causing a national emergency.

Table 1: Number of Centrifuge Cascades enriching, under vacuum, installed, or with centrifuges disconnected, January 31, 2010

	Fed with	Under	Installed, not	With Centrifuges	Total
	UF_6	Vacuum	Under vacuum	Disconnected	
Module A24					
Aug. 12, 2009	18	0	0	0	18
Nov. 2, 2009	18	0	0	0	18
Jan. 31, 2010	17	1	0	0	18
May 24, 2010	18	0	0	0	18
Aug. 28, 2010	17	0	1?	0	18
Module A26					
Aug. 12, 2009	10	8	0	0	18
Nov. 2, 2009	6	12	0	0	18
Jan. 31, 2010	6	1	0	11	18
May 24, 2010	6	7	0	5	18
Aug. 28, 2010	6	6	6	6	18
Module A28					
Aug. 12, 2009	0	0	14-15	0	14-15
Nov. 2, 2009	0	0	17 (1 being installed)	0	18
Jan. 31, 2010	0	0	16	2*	18
May 24, 2010	0	0	16	2?	18
Aug. 28, 2010	0	0	18	0	18

* In these two cascades in module A28, Iran had removed all the centrifuges in one cascade and was removing the ones in the other one.

Figure 1: Centrifuge Operation and Installation at Natanz

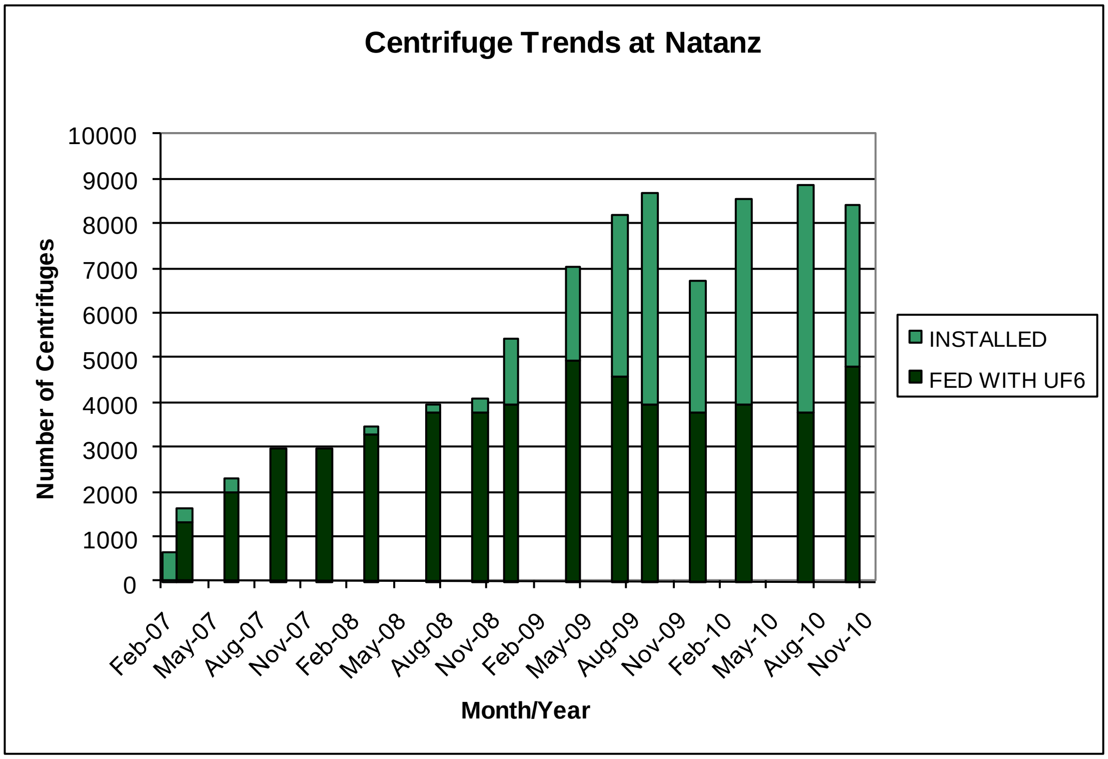


Figure 2: LEU Production at Natanz

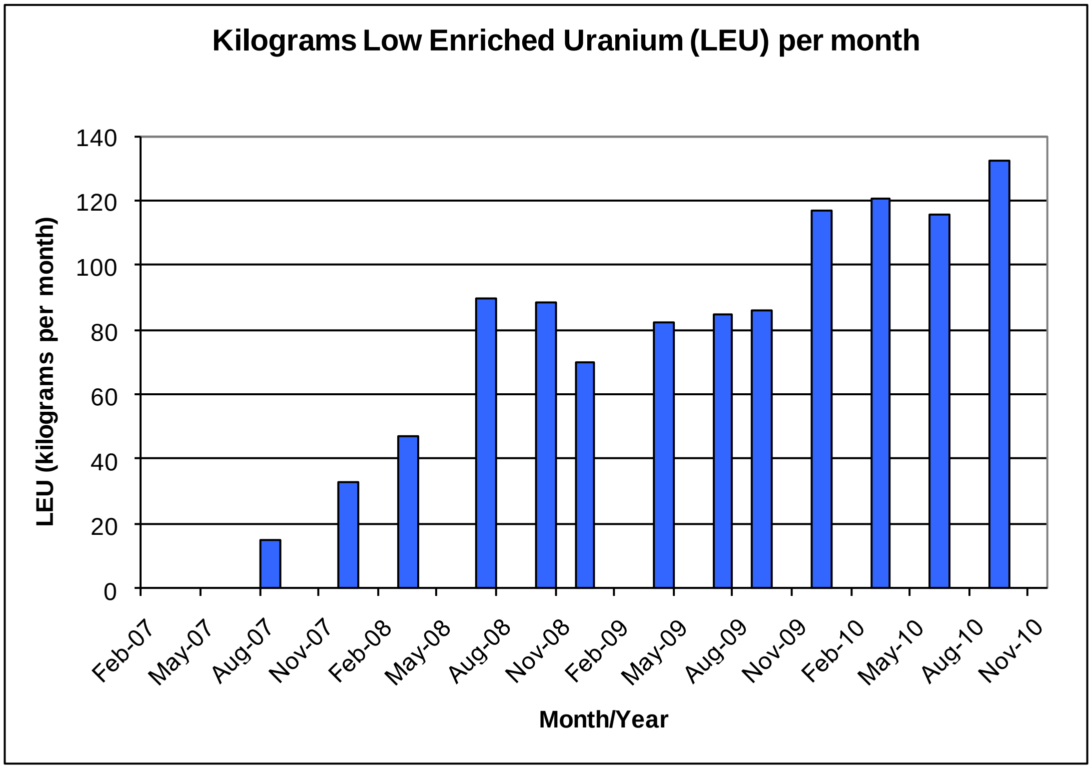
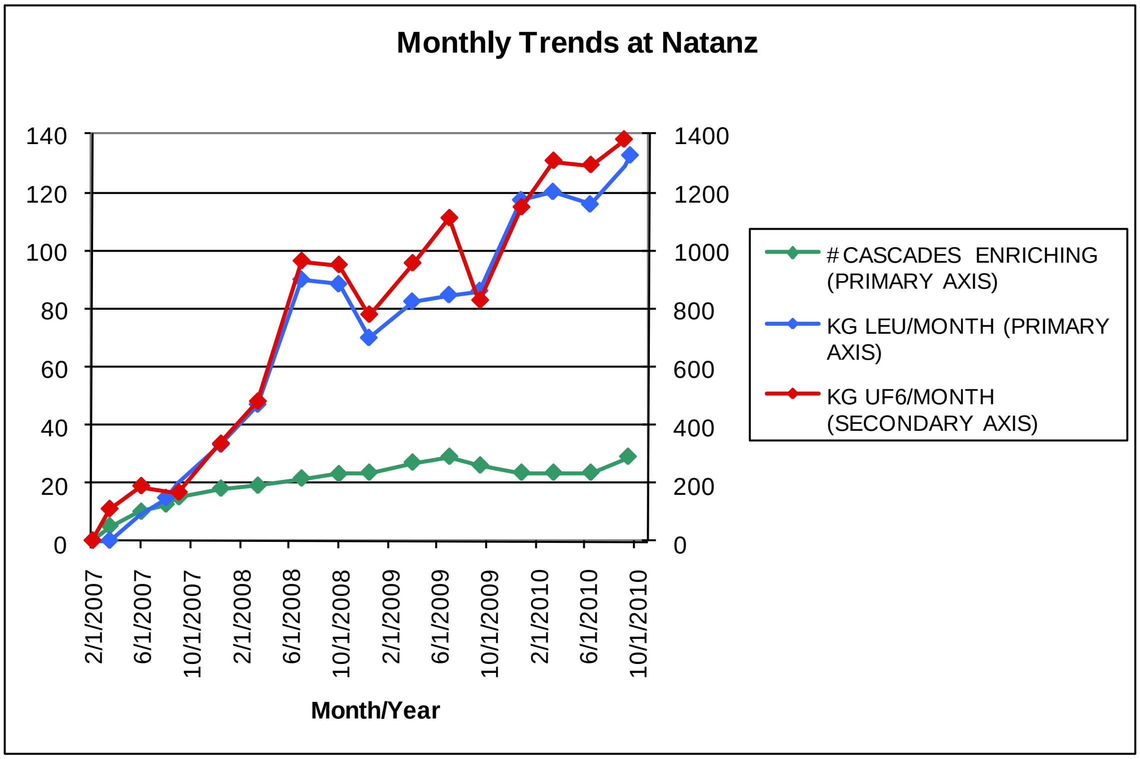


Figure 3: Operating Trends at Natanz


Monthly Trends at Natanz
2/1/2007
6/1/2007
10/1/2007
2/1/2008
6/1/2008
10/1/2008
2/1/2009
6/1/2009
10/1/2009
2/1/2010
6/1/2010
10/1/2010
Month/Year
# CASCADES ENRICHING (PRIMARY AXIS)
KG LEU/MONTH (PRIMARY AXIS)
KG UF6/MONTH (SECONDARY AXIS)