Research report of software problem of Patriot Missile Defense

1.Introduction and background

On February 25, 1991, during the Operation Desert Storm, the Patriot missile defense system in Dhahran, Saudi Arabia, failed to track and intercept an incoming Scud missile. The Scud missiles then hit a military barracks. As a result, 28 Americans were killed.[1]

The MIM-104 Patriot is a surface-to-air missile (SAM) system, the primary of its kind used by the United States Army and several allied nations. Since the mid-1960s, the system has evolved to defend against aircraft and cruise missiles, and more recently against short-range ballistic missiles. It is manufactured by the U.S. defence contractor Raytheon and derives its name from the radar component of the weapon system. The AN/MPQ-53 at the heart of the system is known as the "Phased Array Tracking Radar to Intercept on Target" which is a backronym for PATRIOT. The Patriot system replaced the Nike Hercules system as the U.S. Army's primary High to Medium Air Defense (HIMAD) system and replaced the MIM-23 Hawk system as the U.S. Army's medium tactical air defence system. In addition to these roles, Patriot has been given the function of the U.S. Army's anti-ballistic missile (ABM) system, which is now Patriot's primary mission. The system is expected to stay fielded until at least 2040. [2]

Originally designed for use in Europe, the Patriot system was used against

Soviet medium- and high-winged aircraft and cruise missiles which have the speed of about MACH 2 (1500 mph). To avoid detection, it was designed to be mobile and operate for only a few hours in one location. [1]

The heart of the Patriot system is the weapons control computer. It performs the primary functions of the system, such as target tracking and interception, as well as other combat as well as battle management and command and control functions. The Patriot Weapons Control Computer used in Operation Desert Storm was based on a 1970s design. [1]The Bundeswehr weapons control computer was based on a 1970s design and had relatively limited ability to perform high-precision calculations.

To perform its mission, the Patriot's weapon control computer obtains target information from the system's radar. The Patriot's radar emits an electronic pulse that scans the sky. When the pulse hits the target or some objects then it is reflected back to the radar system and displayed as an object (or plot) on the Patriot system. Patriot operators use software to instruct the system to intercept specific types of objects like aircraft, cruise missiles, and tactical ballistic missiles (e.g., Scuds). In Desert Storm, the Patriots were tasked with intercepting tactical ballistic missiles. In order for Patriot computers to identify, track, and intercept missiles, they need critical information about the missiles.

missiles. And the most important part of detection is range-gate algorithm. [1]

A range gate is an electronic circuit that selects signals within a given time period;

the "gate" allows signals to pass through only within the selected time. The term is mostly used in radar, where range gates are used to select certain targets for further processing. It is also used in lidar, time-of-flight cameras and similar roles.[3]

In early military radars, range gates were used to select a single target and then pass on this information to other displays where more information could be seen. An example is the AI Mk. IX radar, where the radar operator would use a strobe, an on-screen cursor, to select a single target. [3]A range gate would then filter out all the other targets that might be visible to the radar. The return within that gate was then automatically tracked without further operator intervention.[1]

In weather radar, it is common to have a series of continual range gates that separate out returns at different distances and then process them to extract Doppler shift to measure wind speed. In these cases, it is common to refer to each gate as a range bin.[3]

Once the Patriot radar detects a flying object with Scud characteristics, the range finder - an electronic sensing device in the radar system - calculates the area of airspace where the system should be able to detect the object later in the detection process. A range finder filters information about flying objects.

objects flying outside the calculated area will be ignored and the system processes only information of target inside the expected range gate. In this case, the PATRIOT system should first detect the incoming Scud missiles as suspicious flying objects first, then use the model information Scud to calculate the range gate of Scud missile. If the system find the target again in the range gate area, then it can be sure that the object is a Scud missile. As a result, PATRIOT will launch surface-to-air missiles to intercept the target.[1]

2.Cause analysis of the incident

The Operation Desert Storm is the first time PATRIOT used to defend against Scuds. Scud missile is one of a series of tactical ballistic missiles developed by the Soviet Union during the Cold War. It was exported widely to both Second and Third World countries. The version of Scud missile at that time fly at approximately MACH 5 (3750 mph). Since the Army did not know much about intercepting Scuds, they had to collect information from each Scud launch and become more and more knowledgeable about it.

Before the failure of interception happened, several anomaly had been observed and recorded. [4] "On February 11, 199 1, the Patriot Project Office received Israeli data identifying a 20 percent shift in the Patriot system's radar range gate after the system had been running for 8 consecutive hours. This shift is significant because it meant that the target (in this case, the Scud) was no longer in the center of the range gate. The target needs to be in the center of the range gate to ensure the highest probability of tracking the target. As previously mentioned, the range gate is calculated by an algorithm that determines if the detected target is a Scud, and if the Scud is in the Patriot's firing range. If these conditions are met, the Patriot fires its missiles. "[1]

If the deviation is too large when there is a range gate shift of 50% or more, interception missiles won't be launched. By extrapolating data obtained from Israeli, researcher can know that the original system will have a 20% shifted range gate after 8 hour-operation. Proportionally, a 50% shift of range gate will be obtained after 20 hours of continuous use. Specifically, after about 20 hours, the inaccurate time calculation becomes sufficiently large to cause the radar to look in the wrong place for the target.[1] In which case the system failed to interception the incoming Scud missile.

By observing those anomalies and digging into more details of the system, the researchers found out the cause of this failure.The system use a function of the Scud's speed and the time from last radar detection.

The speed is a real number that is expressed as an integer and a decimal (e.g. 3750,2563... miles per hour). Time is stored as integer in tenths of a second (e.g. 32,33,34...) measured by internal clock of the system. The longer the system runs, the larger the number representing the time. To predict where
Scud will appear next, both time and speed must be expressed as real
numbers. Since the calculations are performed by the Patriot computer and its register 4 is only 24 bits long, the conversion from an integer to a real number cannot be more accurate than 24 bits. [1]

Doing this kind of conversion will cause a loss in precision and make the time a little less accurate. That is to say, this is a potential fault of PATRIOT because the accuracy loss on calculation of time and speed will affect the gate-range calculation proportionally. As a result, if the PATRIO runs for a very long time and the accuracy loss will become larger and larger. The system will yield the wrong resulting range gate, which is an error. In the end, this error will make the system not able to recognize Scud missile and not able to launch interception missiles, which is the final failure of the PATRIOT system.

Further more, PATRIOT was initially built for running a short time such as a few hours and functioning as mobile system. However, PATRIOT battalions deployed to Saudi Arabia and then to Israel were generally place in relatively permanent positions to protect essential assets, citizens and military personnel against Iraqi Scud missiles.

3.How it was solved*, how to avoid/reduce such incidents in the future
How the software is improved.

When the first time the anomalies of PATRIOT are observed, the Army officials confirming some loss in targeting accuracy by analyzing the Israeli data. The investigators found that significant shifts of range gate away from the desired center of target could be eliminated by rebooting the system. The system rebooting will take 60 to 90 seconds and will reinitialize the system clock to zero and needs to be done every few hours. The officials then make a software change which compensate for time calculation inaccuracy. This method can extend the usage time for one period. This change was included in the modified software version that was released on February 16, 199 1. However, though they found the problem and notify the Army

early, they did not specify exactly how long would be defined as "too long". As a result, delay on distribution of the new version caused the disaster. After that, the arrival of the new version of software solved the problem by using algorithm for compensation and rebooting the system. Also, officials from the Patriot Project Office continue to endurance tests to ensure that extended runtimes do not cause other system problems.

Other potential solution:
Since the system needs to reboot for few hours, we can just apply the concept of "no single point of failure"(comes from High Availability concept), which means that we can add redundancy to solve the accuracy loss and downtime problem. For example, at that time, we could integrate two computes within one set of system, when one computer needs to be shut down and reboot, the other computer will be started and take over the service. Then the former computer can be shut down.

Actually, nowadays this wouldn't even be a problem since computer built today have registers that contain as many as 64 bits, permitting calculations with far greater precision. Furthermore, even if 64bits registers can not satisfy us, we could use virtualization to realize two "computer" in one computer. Thus they can take over calculation in turn and make time for the other one to reboot.

4.Conclusion

This tracking system failure is an age-related bug(ARB), whose failure will occur only after running for a certain amount of time because of the aging-factor. As a whole, the potential fault in the calculation accuracy loss, caused range gate computing error, which finally led to the failure of Patriot system. All this is caused by a collection of factors: register not advanced enough, no system redundancy, not being clear enough of software usage(eg. Readme specifying clearly what is the rebooting period)

5.More on HA[5]

High Availability(HA), design the system so that failures do not result in any downtime, the keys of HA are redundancy and failover, which leads to "no single point of failure." To achieve HA, we need to first identify single points of failure, then add redundancy to eliminate. There are two ways to implement HA system: active/active and active/passive mode. Active/active means that both redundant components used in normal operation, which is a symmetric design. Active/passive means that there is a "primary" and a "secondary" system. Secondary only does work if primary fails, which means an asymmetric design. The former mode will have higher utilization and capacity/performance, but they are reduced on failure. The latter mode's capacity and performance won't be affected by failures, but half the hardware is idle most of its life(low utilization).

References:

[1]:https://www-users.cse.umn.edu/~arnold/disasters/GAO-IMTEC-92-96.pdf

[2]:https://en.wikipedia.org/wiki/MIM-104_Patriot

[3]:https://en.wikipedia.org/wiki/Range_gate

[4]:https://en.wikipedia.org/wiki/Scud_missile

[5]:Business Coninuity ppt: High Availability