National Aeronautics and Space Administration

NASA SAFETY CENTER

SYSTEM FAILURE CASE STUDY

April 2019 Vol. 12 Issue 1

Storm Clouds Over Stonehenge

UK WATCHKEEPER UAS MISHAP

Try to imagine a machine built today that does not involve software in some form. Can you do it? Even a two-piece, hinged metal can opener was likely conceived on a computer screen using a computer-aided design/computer-aided manufacturing program. Since software is pure design by nature, it cannot 'fail' in the classical sense. However, flawed design assumptions and a failure of imagination can lead to unintended or even fatal consequences. When short-sighted specifications or requirements reveal undocumented features, software performs exactly as designed — but not as intended. Accidents where nothing fails are called "systems accidents," a term that was coined by Yale sociologist Charles Perrow in his book "Normal Accidents." This study examines the circumstances surrounding a systems accident and the unexpected outcomes.

PROXIMATE CAUSE

The Vehicle Management System Computer (VMSC) commanded postlanding actions while Watchkeeper was airborne. The VMSC software logic was susceptible to sensing and latching a false Ground Touch.

UNDERLYING ISSUES

Causal factors included false readings from the laser altimeters, cloud cover and flawed VMSC software logic. Contributing factors included limited understanding of technical issues, lack of training, lack of communication regarding weather restriction and scarcity of landing phase documentation.

LESSONS LEARNED

Threatening conditions can lead human operators to make needlessly risky decisions when the current and optional modes of operation aren't fully understood. When system performance confuses an operator, the instinct is to simplify the system to regain control. Pushbutton software logic that lacks feedback short of a crashed aircraft demands a different, more intensive training focus.

When a nearly £6M British Army Unmanned Air Vehicle (UAV), tail number WK006, pitched down and smashed on to a wet Salisbury Plain runway on Nov. 2, 2015, no one should have been surprised. Another Watchkeeper UAV had committed suicide a year before in a similar way. The government investigation documented good reasons and recommended fixes. So why did another Watchkeeper dive to its death? NASA engineers and operators would do well to learn from this case study as we embark on more complex missions involving software, automation and human factors.

BACKGROUND

WATCHKEEPER PROGRAM

In 2005, the British Army needed an aerial platform to target weapons delivery during hostile day or night missions (similar to the U.S. Air Force Predator drone). They awarded Thales UK a prime contract to upgrade its own Hermes 450 platform. The program was named Watchkeeper.

A system of UAVs, optical and UAV radar sensors, data links, and ground control systems, Watchkeeper was designed to conduct Intelligence, Surveillance, Target Acquisition and Reconnaissance missions. Airborne mission requirements included high-desert weather flying and adverse takeoff/landing surfaces. However, according to the WK006 Service Inquiry report, the Release to Service document "did not contain any specific environmental limitations concerning, precipitation, cloud or visibility, during the recovery and landing phase."

Pilot experience and judgment were implicitly expected by Thales UK preceding a decision to launch and recover this expensive drone as such judgment was already required for Hermes. Neither Hermes nor Watchkeeper possessed traditional pilot joystick or pedal flight controls; all controls were pushbuttons that commanded software actions leading to hardware responses.

The Watchkeeper program started flying in 2010. Operated by a civilian crew from UAV Tactical System Ltd., WK031 crashed while making an approach to land at West Wales Airport (WWA) in October 2014. Crew operation of the Automated Takeoff and Landing System (ATOLS) and UAV response were both precursors to the WK006 mishap. Watchkeeper flying operations resumed from MoD Boscombe Down (BDN) military airport in March 2015.

Thales UK had conducted flight testing at WWA. Army Watchkeeper flight training occurred at BDN and was conducted by Royal Artillery. The Hierarchy of WK Rules and Regulations (1ISR Bde Flying Order Book) defined the hierarchy of orders pertaining to Army Watchkeeper operations. This document specified pilot currency requirements for live flying, simulator flying and simulator emergency training.

Figure 1: Watchkeeper aircraft components (Source: Service Inquiry report)

WATCHKEEPER SYSTEM

The Watchkeeper system included components and support equipment that enable preflight preparation, launch, operation and recovery, controlled from a Ground Control Station (GCS). Ground support equipment allowed transportation, storage and maintenance.

Major Unmanned Air System (UAS) components included the GCS, Ground Data Terminal and the ATOLS (comprised of the Arrestor System and Portable Aircraft Test Equipment).

Since manual stick-and-rudder flying skills were designed out of the GCS, crew training was assumed to be physically faster, cheaper and thus better.

VEHICLE MANAGEMENT SYSTEM (VMS)

The Unmanned Aircraft's (UA) VMS described the essential electronic installations within the UA and the associated top-level tasks it carries out. According to the Service Inquiry report, it consisted of a combination of Line Replacement Units, which were designed to fully prioritize and task the semiautonomous UA in providing monitoring and control, automated flight, instrument/sensor feedback, and navigation throughout all phases of flight.

Figure 2: Watchkeeper GCS operating position (Source: Service Inquiry report)

The VMS was controlled directly by software within the Vehicle Management System Computer (VMSC), which was mounted in the forward section of the fuselage. The VMS had full authoritative control of the UA wing and tail surfaces using onboard navigation instrumentation and sensors. Watchkeeper operators in the GCS made command inputs to the VMS via pushbutton commands sent to the UA. Under normal operation, onboard software rules prevented these indirect GCS commands from overstressing, stalling or crashing the UAV. Placing the onboard software in charge (even over the human pilot) was a similar design concept to the control laws design used by Airbus in its airliners with success. Unlike Watchkeeper, however, Airbus incorporates two-fault tolerance in hardware and software controls.

The VMS monitors and controls the various systems on the UA where real-time information was relayed via the data links to the GCS for display on the client server Human Computer Interface.

VMSC

The VMSC responded to the preprogrammed flight mission plan and reacted dynamically to real-time commands received from the GCS via the data links. From Engine Start to Engine Cut, it was designed to automate routine tasks through all phases of flight, including Automated Takeoff and Landing (ATOL).

The Watchkeeper's ailerons, flaps and twin V-Tails (which serve as a combined rudder and elevator) were moved by dual, electrically-redundant single-linkage electromechanical actuators (in the wings and rear fuselage), which were controlled by the VMSC.

Flight Control Software (FCS) within the VMSC maintained controlled flight within a predesignated operational envelope, providing a safety margin against structural and flight limitations. The FCS was programmed to protect against operation outside of the flight envelope design limitations. The Weight on Wheels (WoW) function was relevant to the mishap.

WoW SYSTEM

There were two separate WoW systems on the aircraft. The WoW1 was a pseudo WoW system, which determined via an algorithm (instead of sensing actual compression or 'squat' of landing gear against a surface) whether the UA was on the ground or in the air by determining Ground Touch and Air Jump — based on measured accelerations and rotation rate. A physical WoW squat switch had been incorporated into the initial design, but was removed when deemed unreliable during operations from rough, unprepared terrain. The pseudo sensing worked by doing the following:

- Once a Ground Touch had been sensed, the WoW1 could either declare the aircraft to be in Air Jump (if vertical acceleration meets a threshold) or on the ground.
- Once the vertical acceleration met the second threshold value for a period of time, Air Jump ended and the UA was declared to be on the ground. (There was a different set of parameters used to declare the UA airborne on takeoff.)

Two laser altimeters supplied accurate height measurements to the VMSC when the aircraft was close to the ground to ensure a smooth landing. To gauge height reference during flight, the aircraft used barometric altitude as the primary height reference within the Inertial Navigation System.

The Ground Flight Control Computer (GFCC) was responsible for processing all flight command instructions for the aircraft. It checked

Figure 3: ATOLS ground components: GBU (left) and GRU (right) (Source: Service Inquiry report)

the validity and safety of commands (e.g., terrain clearance, air-space compliance, etc.). The VMSC would only accept valid commands from the GFCC, thereby protecting the aircraft from "erroneous inputs."

The ATOLS had a Ground Radar Unit (GRU) and a Ground Beacon Unit (GBU) next to the runway. Based on the initial position data from the GCS, it tracked the position of the aircraft and provided steering information to the vehicle via the GCS and datalinks using the GBU as a surveyed reference to enable accurate target positioning. If the ATOLS failed/malfunctioned, the aircraft could still perform ATOL using a GPS Takeoff and Landing (GTOL) system. During the landing phase, the VMSC would select the ATOLS or GTOL system — based on the one that was more accurate.

WK031 MISHAP: THE PRECURSOR

On Oct. 16, 2014, one year and two weeks prior to the WK006 mishap, an accident occurred during the WK031 flight. Despite forecasted thunderstorms, the crew thought they could recover at WWA in between storms. The instructor pilot was using this flight to maintain 30-day sortie currency requirements. The student had flown five Watchkeeper training sorties and completed nearly eight hours in the Watchkeeper simulator.

On the day of the flight, briefings, engine start and takeoff occurred according to plan. As student training was completed, storms approached the airport and the crew elected to recover the UA. To preclude an abort over a wet runway, the crew selected ALT DiFF OVERRIDE with laser altimeter unreliability detected by the VMSC. Due to a thunderstorm upwind of the landing point (directly in the abort path), the student proposed and the authorizing officer agreed to select MASTER OVERRIDE to prevent the UA from entering the storm. On final approach, witnesses observed the UA pitch rapidly nose-down from 10 to 15 feet altitude and impact the runway at 11:13 a.m.

According to the MoD Service Inquiry into the WK031 mishap, the cause of the accident was as follows: "The sequencing of the landing logic within the Vehicle Management System Computer functioned as designed but not as intended. The VMSC commanded the post-landing actions (V-tail full deflection to pitch the nose down) whilst the UAV was still airborne, after recognizing a false 'Ground Touch.'" Simulator runs conducted after the mishap found that the UAV's landing algorithm tolerances appeared incompatible with both highly turbulent gusts of wind and very smooth air conditions.

The WK031 mishap report further stated: "The Panel established that the Designer predominantly operated the UAV with an External Pilot (EP) available if there was a requirement to land the UAV from the first approach. This is in contrast to the U-TacS [Army] standard operating procedure, where only ATOL is used, a practice driven by the Army's original requirement to have a fully automatic capability for Watchkeeper. Furthermore, the U-TacS [Army] did not have the trained personnel to use an EP. Since The Designer considered the use of MO [MASTER OVERRIDE] only for serious emergencies (e.g., engine fire), they had no requirement to specifically develop MO procedures …" According to the report, the "Designer had provided U-TacS [Army] employees with MS PowerPoint presentations during their initial training. These presentations contained one slide that gave limited information on the use of MO. In the Panel's opinion, given the intended operating procedure for UK Watchkeeper, there was insufficient information provided to the crews."

In a vacuum of manufacturer MASTER OVERRIDE information or procedures, Army students and instructors developed informal notes that the panel found 'normalized' the Army crews toward the use of MASTER OVERRIDE. ATOLS Abort and Override procedures contained multiple references to the use of MASTER OVERRIDE without enough facts about the system to understand its limitations. Further, MASTER OVERRIDE had been used 10 previous times without mishap — earlier and earlier in the recovery process. Crews gained confidence that it could be used in adverse situations without understanding the crash-preventive logic they were bypassing.

Following the incident, recommendations were made to improve software, hardware, training and procedures. Yet, an eerily similar mishap would unfold just over a year later.

WK006 SORTIE PREPARATION

The goal of the sortie was to provide currency training for two recent graduates of Watchkeeper Pilot Conversion to Type Training (CTT). It was the pilot and payload operator's first flight since completing Watchkeeper CTT in mid-October 2015. This would mark the beginning of an accelerated program to become Watchkeeper captains and instructors.

The WK006 flight plan included taking off from BDN between 11 and 11:30 a.m. The flight was scheduled to take place in segregated airspace, in the area of the Salisbury Plain Training Area (SPTA), which was approximately 12 kilometers northwest from BDN.

Figure 4: WK006 route (Source: Service Inquiry report)

According to the Service Inquiry report, the captain thought the overcast fog/cloud conditions presented an excellent opportunity to demonstrate to the crew the capabilities of the Synthetic Aperture Radar. The authorizing officer believed that the weather conditions allowed them to help the recent CTT graduates explore system functionality in poor weather, develop as aircraft captains and gain confidence in the system.

Figure 5: WK006 wreckage (Source: Service Inquiry report)

WK006 MISHAP: WHAT HAPPENED

On Nov. 2, 2015, preflight weather and mission briefings, engine start, and takeoff went as planned. However, the weather conditions were not favorable to flight. For example, surface visibility was 150 meters, with the sky obscured (so-called "RED conditions" where the lowest cloud base was below 200 feet and visibility was less than 800 meters). The cloud base and visibility did not improve during the course of the day. According to PrivateFly, crewed military aircraft do not usually launch in RED conditions in the U.K., but records of previous Watchkeeper flights using MASTER OVERRIDE showed eight aborted flights in RED (or nearly RED) conditions. This indicates that crews expected the UAS to take off and land in very low cloud cover and low visibility, which was not specified as a design requirement.

Shortly after the 11:05 a.m. takeoff, the External Air Temperature Sensor 1 and 2 failure message displayed to the crew as the aircraft climbed out to SPTA. The crew referred to Flight Reference Card (FRC) guidance and decided to continue the sortie. This warning was continuously displayed to the crew until the recovery began.

At 2:45 p.m., the recovery started after the main part of the sortie was completed. During this time, the crew found that the ATOLS was unusable in its normal mode, despite troubleshooting. Since ATOLS was unavailable, the crew decided to conduct its landing sequence using the backup GPS/inertial navigation GTOLS system. They selected the ATOL "Alt Dev" override per their FRC for the first attempted approach. However, the UA aborted the approach, displaying the LAND STATUS TIMEOUT caution alert. The UA navigated toward the beginning of its recovery profile despite the crew retransmitting the LAND command. A second approach was made but yielded the same results.

After the crew discussed the problem with the authorizing officer in the GCS, they selected MASTER OVERRIDE to preclude a UA abort. The UA flew a normal approach profile until over the runway at 23-feet altitude. At 3:50 p.m., WK006 abruptly pitched nose-down and impacted the runway at a 35-degree angle, just like WK031 had done in 2014.

PROXIMATE CAUSE

According to the Service Inquiry report, the VMSC commanded postlanding actions while the UA was airborne. The VMSC software logic was susceptible to sensing and latching a false Ground Touch.

UNDERLYING ISSUES

CASUAL FACTORS

The Service Inquiry report identified the following casual factors related to the mishap:

- **Use of the laser altimeter height at the Connect Point (CP) to open a Ground Touch identification time window:** False readings from the laser altimeters sent to the VMSC, after the CP was reached, initiated a chain of logic events that led to the loss of WK006. Laser altimeter readings were used by the VMSC to open a Ground Touch identification window. If readings of less than 1 meter had not been used by the VMSC, the window would not have been opened at the CP and a Ground Touch would not have been sensed.
- **Cloud at the CP:** Laser energy reflection from clouds at the CP caused the laser altimeters to mistakenly read less than 1 meter.
- **Flawed VMSC software logic:** The VMSC used laser altimeter readings to open a Ground Touch identification window. The VMSC's WoW1 logic sensed a Ground Touch, followed by an Air Jump and then declared that the UA was on the ground — all while the aircraft was still 300 feet Above Ground Level. The automatic protection measures were overridden by the selection of MASTER OVERRIDE. Once the aircraft reached the semi-flare point, postlanding actions were commanded, resulting in the pitch-down maneuver and impact with the ground. Basically, the VMSC software declared that the aircraft was on the ground and ultimately commanded postlanding actions while the aircraft was still in the air.

CONTRIBUTING FACTORS

The Service Inquiry report identified the following contributing factors associated with the mishap:

- **Limited U.K. understanding of the technical issues concerning the recovery of Watchkeeper:** According to the Service Inquiry report, "The Panel believe that in the absence of a detailed understanding, the Unmanned Air Systems Team could have been

Figure 6: Damage to the WK006 aircraft (Source: Service Inquiry report)

more questioning of the DAOS [Design Approved Organization Scheme] organisations and allowed an optimism bias to form, possibly in the face of program pressures." The report also mentioned that "… it would seem that this optimism bias percolated as far as the Captain of WK006, who having been involved in many of the post WK031 discussions concerning the use of MO [MASTER OVERRIDE], also believed that a repeat of the WK031 accident, even with MASTER OVERRIDE selected, would require a repeat of the same meteorological conditions."

- **Scarcity of information on the landing phase within the Aircraft Document Set:** According to the Service Inquiry report, the Interactive Electronic Technical Publication (IETP) 7.1 contained limited information about the landing regime and did not provide operators with sufficient information to deal with the landing of WK006. This contributed to the crew's limited understanding of the landing logic and messages displayed to the crew during the WK006 recovery.
- **The Unmanned Air Systems Team Type Airworthiness Authority (TAA) was not informed of the weather restriction in place at WWA:** Thales UK had been aware of the system limitations regarding cloud at/beneath the CP and had limited the operating envelope of Watchkeeper when operating from WWA under the Military Flight Test Permit. However, Thales UK did not communicate this increased limitation to the TAA. Also, "the opportunity to introduce similar weather limits" at BDN "was missed." The Watchkeeper was not an all-weather aircraft, and the quote above represents an indirect confirmation of that fact.
- **The absence of role-specific authorizing officer training:** The authorizing officer of WK006 had attended the Flight Authorizers Course but not the regulatory article authorizing officer briefing day. "The Panel found no evidence that the Authorizing Officer had received any further training for his role as an Authorizing Officer." The panel looked at other Remotely Piloted Air System units and established that their authorizing procedures were borne from many years of experience, both in the UA and manned aviation world.
- **Normalization of the use of the Low Cloud Recovery Procedure:** The IETP stated that due to changing weather, occasionally the aircraft may need to be recovered with cloud at or below the CP and directs crews "to perform the procedure for UAV recovery in low cloud conditions." The wording and lack of formal limitations led the crew to think they could routinely conduct flights when clouds were expected at or below the CP.
- **The decision to operate when low cloud was forecast during the planned recovery period:** According to the Service Inquiry report, the panel considered that the operation of Watchkeeper when low cloud was forecast during the planned recovery period made the accident more likely. The crew's preflight risk assumption of being able to make a safe landing during the allocated recovery period and in the prevailing conditions drove the decision to pursue landing attempts with cloud at the CP.
- **The decision-making process that led to the premature selection of MASTER OVERRIDE:** MASTER OVERRIDE, an emergency function, "had inhibited the protection measures that would otherwise have resulted in the final landing attempt being aborted by the system." Although the decision to use MASTER OVERRIDE was within FRC guidance, the use of MASTER OVERRIDE "was predicated on the decision to continue to attempt to land with cloud at the CP." As other options existed, the Panel believed that the decision to use MASTER OVERRIDE was premature given the warning about the potential loss of the UA within the FRC and in the context of the revised procedures introduced following the loss of WK031. According to the Service Inquiry report, "MASTER OVERRIDE did not cause the accident, but failed to prevent it in the same way that the absence of a manual abort action being taken after seeing the LAND STATUS TIMEOUT and Air Jump messages failed to prevent it."
- **The pitch down maneuver to intercept the glideslope following the CP:** According to the Service Inquiry report, the aircraft was designed to select the final waypoint on the recovery route to use as the CP (Waypoint 6). On each approach, the CP was declared approximately 300 meters before Waypoint 6. As the aircraft initiated a turn after declaring the CP, Waypoint 6 was never actually flown through. According to Thales UK, this was because the aircraft "declared waypoints within a lateral tolerance, which was a function of Ground Speed, where the faster the UA was moving the greater the tolerance." An analysis of the VMSC data showed that the UA was above the 3-degree glideslope when it declared the CP, which caused it to pitch nose-down to attain the glideslope. This, in turn, triggered the Ground Touch.

WK031 AND WK006 COMPARISON

According to the Service Inquiry report, both the WK031 and WK006 crashes were the result of the VMSC commanding postlanding actions while the aircraft was in flight. The apparent hazard that caused this was the VMSC software logic's susceptibility to sense and latch a false Ground Touch.

The hazard entry conditions surrounding both crashes were different. According to the Service Inquiry report, the Ground Touch identification window was opened using different logic and the Ground Touch was triggered by a VMSC commanded maneuver in the case of WK006, rather than a gust of wind in the case of WK031. The fact that different and unforeseen technical entry conditions exposed the system's vulnerability to falsely sense a Ground Touch demonstrated that mitigating the known hazard entry conditions alone was insufficient to prevent reoccurrence, as other hazard entry conditions existed. "The operation of WK [Watchkeeper] with the flawed VMSC logic carries, at present, an undefined safety risk, unless it can be demonstrated that there are no other conditions that exist that could lead to a false Ground Touch being sensed," stated the Service Inquiry report.

The WK031 causes related to WoW logic were not addressed prior to WK006. In addition, WK031 pointed to operator use of MASTER OVERRIDE to simplify the UAV and get it on the ground quickly. Although the operators wanted a way to manually land the WK006, they did not understand that without any safety controls, the flare-pitch down flaw was certain.

APPLYING LESSONS LEARNED TO CURRENT AND FUTURE NASA MISSIONS

In these two mishaps, Army crews normalized deviance. They increasingly used MASTER OVERRIDE to complete training and test flights under conditions where the manufacturer would not even operate the UAV. A limited number of successful outcomes established a false "normal" expectation among operators and deciders. Even after the WK031 mishap, crew behavior did not change.

A lack of training and comprehension concerning the software "defenses" normally intended to prevent a crash landing contributed to every previous flight decision to land using MASTER OVERRIDE. If the designer had used a hazard analysis method that included "non-fault" scenarios (where the Control Algorithm worked as built) it would have been possible to find out where the software worked as designed, but not as intended. Classic event-chain fault analyses cannot capture a non-fault situation where the system acts reliably but not safely. According to the Service Inquiry report, the WK031 investigators "had not been able to gain a full and detailed understanding of the VMSC landing logic and the flight control system …"

Many directions for learning stem from this case study. In a human-machine interface where automation plays a dominant controlling role, threatening conditions can lead the human operator to make needlessly risky decisions when the current and optional modes of operation aren't fully understood. Designers, planners or managers who assume that operators don't need to know such information are unintentionally but certainly building future failure modes.

When system performance confuses an operator, the instinct is to simplify the system to regain control. This is a sound concept, provided the new risks inherent in the simplified mode are understood. Stick-and-rudder controls become intuitive after training because feedback pressures inform the pilot; pushbutton software logic that lacks feedback short of a crashed aircraft demands a different, more intensive training focus.

QUESTIONS FOR DISCUSSION

- Where software logic controls your system's operation, can you identify each of the constraints required to maintain safety? (For example, WK006 needed constraints to prevent Controlled Flight Into Terrain (CFIT). One constraint should be that the VMSC should not cause or contribute to CFIT.)
- Above the level of software logic, which social systems govern safety constraints in your system? (One example would be the interaction between the project manager and the software development lead.)
- Within the aforementioned social structure, how can a lack of budget resources as well as payment milestones tied to project milestones prevent a software safety constraint from working, or even being developed or tested?
- For your system, when automated operation cannot meet a mission demand, will the manual mode(s) allow a human operator to adapt, complete the objective and recover safely?
- Are all system operating modes simple enough to train the human operator to choose the best mode for each contingency?

REFERENCES

a. Service Inquiry into the Watchkeeper (WK006) Unmanned Air Vehicle (UAV) accident at Boscombe Down Aerodrome on 2 November 2015, Ministry of Defence and Defence Safety Authority, Dec. 15, 2016.

b. Service Inquiry into the Watchkeeper (WK031) Unmanned Air Vehicle (UAV) accident at West Wales Airport on 16 October 2014, Ministry of Defence and Defence Safety Authority, Aug. 12, 2016.

c. **PrivateFly:** What are the weather colour codes used by RAF pilots? https://www.privatefly.com/ask-the-pilot/15-weather-colour-codes-for-aviation.html Accessed Feb. 20, 2019.

Visit nsc.nasa.gov/SFCS to read this and other case studies.

NSC NASA SAFETY CENTER

Responsible NASA Official: Steve Lilley
Steve.K.Lilley@nasa.gov

This is an internal NASA safety awareness training document based on information available in the public domain. The findings, proximate causes, and contributing factors identified in this case study do not necessarily represent those of the Agency. Sections of this case study were derived from multiple sources listed under References. Any misrepresentation or improper use of source material is unintentional.

Thanks to Mr. Simon Whiteley for his insightful peer review.