Principles for Increased Resilience in Critical Networked Infrastructures

Kyle J. S. White, Dimitrios P. Pezaros, Christopher W. Johnson
School of Computing Science
University of Glasgow
Glasgow, Scotland
mail@kylewhite.com, dimitrios.pezaros@glasgow.ac.uk, christopher.johnson@glasgow.ac.uk

***Abstract*—We propose a framework for deploying stronger, intelligent resilience mechanisms in mission-critical ATM networks over and above that offered by physical n-fold redundancy. We compare the challenges facing power and data network resilience and discuss disruptive threats to real-world operations. Using recorded live data from an ATM data network we argue our proposed architecture with deployable, distributed on-demand anomaly detection and monitoring modules provides enhanced fail-secure versus current fail-safe resilience.**

Resilience; Critical Infrastructure; Automated Network Management; Network Monitoring

I. INTRODUCTION

Critical infrastructures worldwide are increasing their already heavy reliance on the underlying data networks which transfer their mission-critical information. At the same time, society is escalating its dependency on these infrastructures and in particular, there is swelling demand and reliance on Air Traffic Management (ATM) systems. The International Air Transport Association (IATA) predict 3.6 billion passengers in 2016, a 28.5% increase on passengers carried by airlines in 2011 [10]. Increasing passengers will translate to an increase in the volume of critical information, therefore raising the impact and consequent disruption of data network threats. In this paper, we propose that ATM data networks can and should be more resilient through automation, highlighting relevant evidence, and we present our proposal on how this can be achieved. We recognise automation in this context raises safety concerns among domain experts and we address these issues. In Section 2, we discuss the resilience of an existing ATM infrastructure, comparing power and data network architectures using our domain knowledge. This comparison is framed within our depicted pyramid of criticality, detailing the various layers of systematic reliance required in order to provide a functionally operative environment for an ATM service. We review recent disruptive incidents which highlight serious challenges facing daily ATM operations in Section 3. Our next significant contribution is our proposal for an architecture which exploits state-of-the-art networking mechanisms to allow configurable, intelligent network security and monitoring modules to be deployed on-demand throughout the network in the face of emerging challenges in Section 4. Providing evidenced-based understanding of the status-quo, we examine the secondary radar systems within the ATM service on a live national Air Navigation Service Provider's (ANSP) network and showing the strong correlation between the air traffic and the bytes on the wire in Section 5. Section 6 concludes the paper.

II. RESILIENCE ARCHITECTURES

Critical infrastructures rely on power and communications in order to maintain mission-critical services. This holds true for the ATM industry which requires a multitude of systems, in a system of systems nearly all of which require both power and some form of communications to function adequately, to provide safety and service management. In Figure 1, we present a functional hierarchy of crucial aspects required to operate a critical infrastructure effectively. The diagram details the various layers of systematic dependency required in order to provide a functionally operational environment. Each row of the pyramid builds on the per-requisite layers beneath, forming the overall system requirements necessary for today's operational standards. In this respect, power and communications can be categorised together as basic needs, forming an inter-dependency. Often data networks manage the power networks which supply the energy to run them. Physical communication channels in this field include radio signals, satellite transmissions and computer network cables. Power and network cables are both prone to similar outages through physical damage. While potentially incapacitating, this threat can be statically mitigated through physical n-fold redundancy. As a general rule throughout the network of a major EU ANSP, each 2-fold redundant link carries 40% utilisation. If one link fails the other can take 80% utilisation and still have the capacity available for some peaks in the data traffic. The air traffic control centres of this ANSP are linked redundantly with a data network which has an overall reliability requirement of 1 x 10^{-6}, meaning there may be one complete failure every 100 years. This is primarily achieved through the magnitude of redundancy, individual components are no longer critical to the operation as a whole and that even if multiple services fail there is still a way to deliver services. This holistic approach to safety is the key concept behind resilience engineering [9]. However, this means individual failures are more often (since there are more components), and therefore it is more challenging to detect these failures without automated systems.

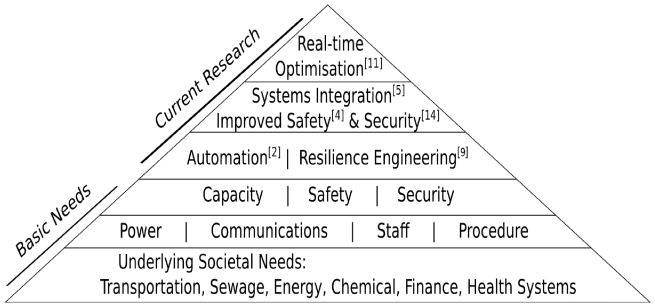

Figure 1: Depiction of the layers of dependency in critical infrastructure annotated with the direction of future research.

However, considering the payload on power cables and computer networks the similarities diminish. While power can fluctuate, e.g., with voltage spikes, this can be mitigated through a voltage regulator. The importance being the consistent flow of enough of the common power payload. Communication payloads however, are a complex, non-Poisson process of traffic load and arrivals. This implies high variability and unpredictable dynamics over long timescales, and the traffic behavior cannot be smoothed out. Traffic peaks can also be significant in terms of utilisation, even with substantial over-provisioning. Data packets are also susceptible to corruption, loss and delay. This makes the communication resilience problem much harder and the integrity and availability of network data therefore requires a more sophisticated solution than power.

A. ATM Power Resilience

It is a complex task to ensure continuous power to Area Control Centres (ACC)s. One ACC in Europe has primary and secondary power supplies which come from two independent electrical supplies, from separate parts of the national power grid. These supplies run four Diesel Rotary Uninterruptible Power Supplies (DRUPS) which convert the power to a steady, clean stream in terms of phase, harmonic distortion and without voltage spikes. The generators also each power a large (approximately 12 foot diameter) fly wheel which spins constantly. Should the primary power supply fail, the process to switch to the secondary refinery takes approximately six seconds. These fly wheels have enough stored energy to power the systems for approximately eleven seconds, well in excess of the time required to switch. This sizeable margin of error, within an already highly redundant system, highlights the importance and care engineered into maintaining the perpetual operation. In the rare instance of both these supplies failing, there is enough back-up fuel to run these generators for a week and a half. For further details on air traffic control power resistance see [13]. In the worst case scenario, there are 110 tonnes of batteries which have the capacity to keep systems online for the couple of hours necessary to implement fail-safe procedures, clearing the skies and keeping air traffic safe. This is also the length of time the controllers area is rated to be resistant to fire. Contingency plans are also in place to transfer control to another location should the facility no longer be functional. The building designs and physical layout for critical infrastructures are often highly symmetrical, with redundant systems mirroring each other numerous times. This holds true for ATM control centres in the EU and US. If a system has 2-fold redundancy through a single back-up system issues can still arise. For example, if a component fails, then human error in maintenance could take the functional component offline instead of the failed piece, rendering the service completely unavailable. Data networks, are also physically mirrored, with independent cabling, servers and connections acting as back-up systems. Often, the partition between two replicated systems is a physical firewall to further separate the primary systems from their fall-back system(s). Generally, there is a risk in having completely identical, duplicated redundant systems as they are exposed to Common-Cause Failures [9]. If conditions arise which raise a dormant, underlying flaw, or software bug then the primary system will fail. When the failure conditions are applied to the duplicated system, the failure will occur again. As a result, some differences between primary and back-up systems increase the overall resilience.

B. ATM Secondary Radar Resilience

To protect the mission-critical secondary radar surveillance system, a national EU ANSP has two full network topologies. These architectures are fully redundant and transfer the radar information to distributed processing locations. Servers at these locations take the feeds from both network cables and examine the difference. Independently from the data cables, there are also two redundant physical connections used explicitly for command and control communications and network monitoring. The biggest loss of data observed in their systems is through long distance cables. Therefore this redundancy is exploited, comparing the information from each source and merging the feeds where applicable to get the best data on air traffic. Further still, each radar site is located to overlap the portion of sky it can monitor. The resultant Venn diagram style architecture is used to further merge the combined data flow from each radar to select the most representative and accurate picture of the sky at any given moment. Once the air traffic positioning has been defined, this data is available for all ATM operators to pull from the national network in a publish/subscribe manner. Each Air Traffic Control Operator (ATCO) terminal has two independent network cables ensuring full resilience against physical disruption across the system. Recent work by Borener and Guzhva [4] highlights the importance of resilient communication and surveillance systems on air traffic separation. Their research shows that when these services experience outages, where there is no access to the system or redundant systems, the number of Traffic Collision Avoidance System Resolution Advisory (TCAS) (RA) events increase considerably. These events are the airborne safety system warnings, designed to avoid aircraft coming in closer proximity to one another than the safe limits. In the study, they found that in the 30 minutes after a service outage there are 1.31 more events as compared to the 30 minutes preceding the outage. There is therefore a strong relation between the resilience of the network communications, as part the complete communication and surveillance systems, and the safety of air traffic.

C. The Risk of Change

Like most critical infrastructures, air travel for passengers is currently very safe with worldwide fatal accident rates from 1997 to 2006 at 0.79 fatal accidents per million flights flown or 0.49 per million hours flown [16]. More recently, metrics show significant improvements in fatal accident rates worldwide [1]. Changes to the system are often perceived as a risk, yet in order to maintain these high safety standards, changes are often necessary. Safety calculations are made in numerous ways with risk probabilities, likelihood matrices and fault trees [12]. Such models are based on a strong understanding of the physics and engineering involved in flying, weather, etc. Each of these areas is well understood. Innovation, however, can cause unknown safety issues such as the use of lithium ion batteries in aircraft [6]. Data networks and software services which run are open to a multitude of issues which can be hard to define, from hardware malfunctions to software misconfiguration and, when components are updated, the new interactions amongst the virtual data systems can be challenging to comprehend and predict. The safety modelling for such aspects is very complex, time consuming and expensive. ANSPs have multiple systems and testbeds. Some software or networking updates can be tested for months prior to deployment on an active system. Errors will always occur and therefore the different back-up system configurations are in use. However, sometimes making a change can be necessary due to a known flaw in a piece of software. Often the software patch or upgrade can be considered a greater risk for fear that the patch itself is not safe. If changes to the software or network infrastructure are made on the secondary systems, this leaves the primary systems unprotected from the original flaw or error [3]. Hence, whilst the physical aspects of data networks redundancy are similar to power supply, maintaining the data and information flow aspects is significantly more complex.

III. Recent Disruptive Incidents

Despite the physical redundancies in ATM, vulnerabilities still exist and can lead to serious incidents if they are not suitably mitigated. In November 2009, the FAA Telecommunications Infrastructure (FTI) experienced a four-hour outage causing system-wide delays and disruption for over 800 flights. The incident was managed safely with contingency plans in effect allowing ATCOs to manually manage flight plan data. The FTI services are designed to meet the NAS service telecommunication performance goals (independent of site-specific architecture). These give maximum restoration times for service classifications: Critical: 6 sec; Essential: $6x10^2$ sec; Routine: $6x10^3$sec. This outage was nearly 2.5 times longer than the acceptable Routine service outage. The incident report [7] states this outage was the product of a cascading series of events which resulted from errors introduced into the external provider's network maintenance and network monitoring processes. During earlier scheduled maintenance, an incorrect routing table was programmed into the infrastructure. This remained dormant until the Los Angeles router was restarted in

November 2009. Monitoring systems checked FTI routers and sent an alert if any router exceeded 60% utilisation for longer than 10 minutes. A legacy, low-capacity router in Atlantic City, due for replacement, regularly exceeded the alert threshold. The monitoring system was then programmed to ignore alerts from the Atlantic City router. This action unintentionally instructed the monitoring system to ignore all alerts from all routers. This monitoring system was not routinely observed if no alerts were sent, and the operator was unaware of the alert functionality being lost throughout the networked system. The lack of monitoring at the time of the incident compounded the impact of the routing table misconfiguration. The majority of the outage time was spent probing the system for routers with high utilisation and, on detection of the misconfigured router with excessive utilisation, the remediation action was immediate. An interim solution to continuously remotely restart the router allowed the majority of systems to function while a technician was dispatched to the location. Among many recommendations and observations, our work is most applicable to the following key points: There was no model of the network to simulate change or to understand normal behaviour; Information on network status was available but there was no process to regularly review and log situational awareness; There was no way for the operator to check the network link saturation with the telecommunication providers; There was no standard for reporting network outages with current processes focussing on the outages but not sufficiently identifying specific operational impacts; There was no test capability that mirrors the network backbone and can simulate the application traffic mix. By creating a model of normal behaviour and understanding typical correlating trends in traffic patterns, when faults occur the symptoms deviating from the norm can be identified rapidly. With the architectural mechanisms of distributed, deployable, on-demand monitoring and security modules we propose, should disruption occur, operators can implement the automated processes to begin diagnosing and reacting to emerging incidents far more quickly than current architectures allow. For example, should an outage require network components to be polled for diagnostics, standard tested modules, which comply with safety regulations, can be deployed. Continuously running network monitoring at a granularity sufficient for diagnosing complex emerging threats is impractical and an enormous challenge due to the high demands on processing and storage required to perform and analyse such data. Incidents such as these and others[17], highlight the importance of good resilience engineering with a holistic perspective. Examining the improvements that are necessary in current implementations to meet existing service requirements in the face of evolving challenges provides strong motivation for our proposed resilient architecture.

IV. Improved Architectural Resilience Mechanisms

We propose a framework for deploying stronger, intelligent resilience mechanisms in mission-critical ATM networks over and above that offered by physical n-fold redundancy. By distributing anomaly detection components and understanding the traffic matrix with respect to a taxonomy of critical functionality, the architecture provides better fail-secure versus current fail-safe resilience. We believe ATM data network operators are seeking the functionality and flexibility to deploy on-demand network monitoring and security modules to distributed locations within their network. The state-of-the-art in Internet-wide networking is transitioning towards Network Functions Virtualisation (NFV), including Software Defined Networking (SDN), for many reasons including increased flexibility, reduced operating costs and improved functionality. ATM data networks differ from general Internet networks with respect to traffic composition, relative isolation, more legacy components and a dedicated authoritative stakeholder typically operates them. These differences are important to consider when planning for the challenges specifically facing ATM data

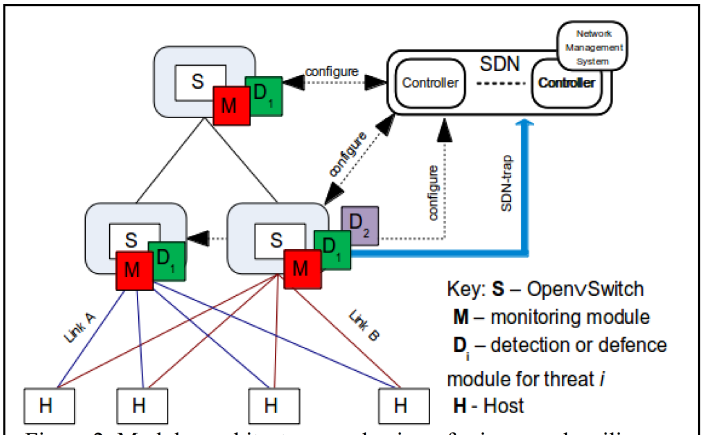

Figure 2: Modular architecture mechanisms for increased resilience.

networks, however, the underlying design of a switched, routed, TCP/IP based infrastructure is akin to most Internet-wide networks. Due to this fundamental similarity, the state-of-the-art in networking can be applied and exploited to service the needs of mission-critical data networks. In Figure 2, we show an abstracted design of the mechanisms we propose. As stated earlier, physical n-fold redundancy does improve resilience and we retain this aspect with switches connected to hosts using *alpha and beta links*. Maintaining this status-quo allows our architecture to be applied to implemented ATM data network infrastructures. At the switching level of the network, we add modular intelligence. As switches perform packet forwarding within the network, they examine the characteristics of these messages and can ascertain aggregated information such as emerging trends and anomalies. We classify our modules into two types: *Monitoring* modules and *Detection* modules. Monitoring modules are generic but can include varying quantities of variables to observe depending on what an operator desires. For example, one monitoring module may poll CPU utilisation for routers every minute, while a different module could provide an overview of CPU utilisation, queue length and traffic volumes every five minutes. Detection modules are threat dependent. Following many years of anomaly detection research it has become clear that different techniques can identify different forms of anomalous behaviour. This has lead to combining algorithms to get optimal overall detection results. For example, the ASTUTE algorithm compliments the Kalman algorithm[15] since the former examines groups of flows which simultaneously increase or decrease their traffic, while the latter can better detect anomalies involving a few large flows, which ASTUTE cannot detect. Since there is demand for a high level of situational awareness in ATM data network operations, a Hough-transform anomaly detection technique[8] would be an applicable choice for a deployable threat detection module. Threats it can accurately detect through visualisations include port scans, network scans and certain worms. It is clear that with such a wide array of possible variables to measure and threats to detect that resources are insufficient to achieve everything simultaneously. As the network behaviour evolves different aspects will be desired. Traditional architectures require hardware reconfiguration and take a long time. By deploying on-demand modules the operators have far greater flexibility, understanding and control over their network. A centralised SDN controller and network management system manages the configuration, deployment and notifications from modules. *Asynchronous messages* we call *SDN-traps* will notify the controller when, for example, a threat has been detected. The operator can also use the controller to enforce fail-secure procedures limiting non-mission-critical traffic in the network by instructing switches not to forward certain data. The algorithms and knowledge to achieve these holistic architectural aims must be based on an understanding of typical traffic and the correlations and inter-dependencies which exist.

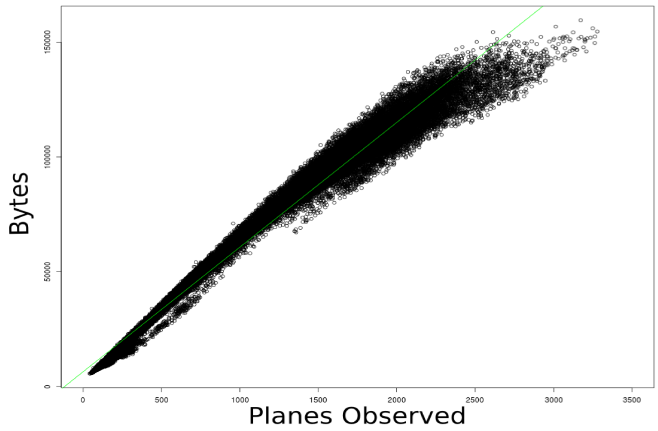

Figure 3: Correlation between numbers of planes observed by radar and bytes transferred, aggregated over 60 sec intervals over 1 month.

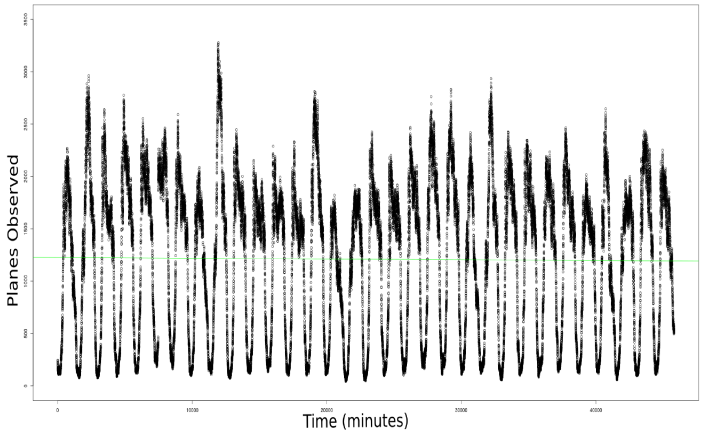

Figure 4: The distribution of numbers of planes observed by radar, aggregated over 60sec intervals over 1 month.

V. ATM Secondary Radar Data Network Analysis

Examining live data recorded from a large EU ANSPs secondary radar data network, we were able to analyse data traffic correlations and dependencies necessary to feed back into the design of our architecture. The data primarily consists of User Datagram Protocol (UDP) with some regular Internet Group Management Protocol (IGMP) packets of negligible size interspersed. UDP is used instead of Transmission Control Protocol (TCP), since TCP introduces timing variability. The issue arises when data packets arrive out of order. For a time-critical service, such as surveillance, the effect is the same as data loss. The maximum delay from the radar site to processing is 20ms for this national ANSP. Each link has approximately 40% utilisation allowing a redundant cable to hold 80% should the primary link fail. Traffic is unidirectional from radar site to the processing server, with any command and control or monitoring polling data using separate network links. Packet lengths are reasonably consistent with all packet sizes within 40-1279 bytes, the majority of which lie between 40-79 bytes (40%). The secondary radar surveillance data was recorded from a radar dish which makes one full revolution approximately every 7.5 sec. Therefore, as an aircraft passes this radar site, it is observed numerous times as it progresses on its flight. The total number of distinct aircraft identifications observed was 21,455. In the graphs in Figures 3 and 4 there are a far greater number of planes represented since this is observations of aircraft, not distinct aircraft. Therefore, the proportionality between network traffic and air traffic is dependent on the constant factor of the rotation of the radar dish. By understanding this relationship and the breakdown of typical traffic structures we can tailor our architecture to this implementation and design optimal modules for use. Future ATM systems will use satellite transmissions for positioning, instead of radar dishes, which are likely to update at a different regularity and therefore it is important to understand the current correlation in the data. Due to our modular approach, adapting to such changes will be more time and cost efficient.

VI. Conclusion and Future Work

In this paper, we have shown our unique architecture for improved ATM data network resilience mechanisms exploiting state-of-the-art Internet techniques. We discussed disruptive incidents which have occurred in ATM systems, their impact and how serious threats such as these, from emerging challenges must be mitigated by network operators on a daily basis. We argue that our proposed mechanisms, with deployable network modules for security and monitoring, allow mission-critical network operators the ability to better understand and mitigate threats, increasing overall resilience.

We base our proposal on domain knowledge and our analysis of recorded live data from a major EU ANSP. Another significant contribution of this paper is a detailed discussion of current critical infrastructure resilience techniques implemented for power grid and data network communications. Our future work will focus on developing an experimental proof of concept through scaled simulations of our architecture. We intend to develop a framework of deployable modules, with different monitoring and automated anomaly detection algorithms and test these against a range of known and emerging, domain-specific challenges.

References

[1] Air Transport News, “Safety Report 2013: An Exceptional Year in Global Aviation Safety”, 2013.

[2] Bainbridge, L., “Ironies of automation”, Automatica, pp 775-779, 1983

[3] Bigio R., Veoni J., Miller J., “Enterprise Information Systems Security for NextGEN”, ATCA Aviation Cyber Proceedings 2012.

[4] Borener S., Guzhva V., “Aviation Infrastructure Risk Assessment: Effect of Communication and Surveillance Facility Service Outages on Traffic Separations”, ENRI International Workshop on ATM/CNS. 2013

[5] Eurocontrol, “Heathrow becomes 5th CDM Airport”. Accessed: 02/2014 http://www.eurocontrol.int/news/heathrow-becomes-5th-cdm-airport

[6] FAA Press Release, January 2013. Accessed: 02/2014 http://www.faa.gov/news/press_releases/news_story.cfm?newsId=14233

[7] FAA FTI Review Panel, “Report on November 19, 2009 Outage”, 2010

[8] Fontugne, R., Fukuda, K. “A Hough-transform-based anomaly detector with an adaptive time interval”, SIGAPP, pp 41-51, 2011, ACM

[9] Hollnagel E.; Woods D.D., Leveson N., “Resilience Engineering: Concepts and Precepts”, Ashgate Publishing, 2006

[10] International Air Transport Association (IATA) Press Release. “Airlines to Welcome 3.6 Billion Passengers in 2016”, 2012

[11] Marnerides, A., Pezaros, D., and Hutchison, D. “Autonomic diagnosis of anomalous network traffic”, IEEE World of Wireless, Mobile and Multimedia Networks, 2010.

[12] Netjasov F. and Janic, M., “A review of research on risk and safety modelling in civil aviation”, Journal of Air Transport Management, pp 213-220, 2008. Elsevier

[13] Platts, J.R. and Aubyn, J.D.S. and Institution of Electrical Engineers: “Uninterruptible power supplies”. IEE Power Engineering Series, 1992.

[14] Signore T.L., Daum J., “Quo Vadis: National Airspace System Cyber-Security Incident Detection and Response?”, ATCA Aviation Cyber Proceedings 2012.

[15] Silveira, F., Diot, C., Taft, N., & Govindan, R. “ASTUTE: Detecting a different class of traffic anomalies”, SIGCOMM pp267-278, 2010 ACM

[16] UK CAA: Global Fatal Accident Review 19972006, July 2008

[17] White, K., Pezaros, D., Johnson, C., “Increasing Resilience of ATM Networks using Traffic Monitoring and Automated Anomaly Analysis”, ATACCS 2012