A Case for Dynamic Risk Assessment in NEC Systems of Systems

Jonathan M. Aitken, Rob Alexander, Tim Kelly
Department of Computer Science
University of York
York, UK
jonathan.aitken, robert.alexander, tim.kelly @cs.york.ac.uk

Abstract – *The level of complexity in Systems of Systems is increasing as more complex functionality emerges from the interaction of individual components. As networks become more complex it becomes more difficult for an individual to identify potential safety risks. We know, from previous accidents, that poor understanding of networks can be dangerous. In this paper, we demonstrate the potential value of incorporating a process to identify risks in a deployed network, focusing on factors concerned with the interaction of this process with a user, and the potential for new hazards.*

Keywords: Systems of Systems, Safety, Risk Assessment

1 Introduction

In this paper we will advance the case for a dynamic risk assessment process based on a dynamic safety case concept. Drawing on research from a variety of disciplines, we will show where there is potential for new processes that integrate well with current operational practice, allowing them to succeed where other decision support systems have failed before.

In part, this builds upon the work of Gary Klein [1] on how "*decisions*" are actually made – specifically how they generally *aren't*. It also builds on an understanding of how a range of Systems of Systems (SoS) accidents occurred and on prior work at the University of York on using a "dynamic minimum equipment list" for an aircraft [2].

It is our view that a dynamic risk assessment process is an essential part of achieving safety in complex SoS, and therefore will be an essential part of SoS engineering in the future.

2 The Challenge of Risk Awareness and Understanding in SoS

In the UK there is a strong drive to move forwards with Network Enabled Capability (NEC) concepts (as proposed in JSP 777 [3]). This move will both increase the complexity of battlefield networks, the availability of live data, information and the responsibility on personnel in the battlefield situation. Paradoxically, these two changes both reduce the commander's ability to understand the state of his force in the field whilst providing him with vastly greater flows of information about exactly what is happening right now – information he cannot integrate and use because of its sheer volume.

In an NEC world there are new sources of risk from network-related issues such as data corruption, data looping, source/sender ambiguity and unpredictable bandwidth or latency constraints. JSP 777 promises that NEC will provide greater risk awareness, but if this does not hold true then there is a danger that NEC will actually increase safety and operational risk.

This situation has serious implications for the management of safety risk, and several attempts have been made to tackle it. The DARP (Defence and Aerospace Research) project at York proposed Systems-of-Systems analysis techniques to tackle this complexity, and these can potentially be used to produce SoS safety cases for networked forces (See Alexander [4], Despotou [5] and Hall-May [6]). Safety cases, however, are static representations – they help analysts and planners, but do not help the commander in the field. They have been criticised for being too absolute – they do not support dynamic operational tradeoffs of safety against performance that may be made in the field.

The NECTISE (NEC Through Innovative Systems Engineering) project explored a range of NEC safety issues, focusing on four areas: Through-Life Systems Management, Decision Support, Systems Architectures and Control and Monitoring [7]. Report TIN005 of the JERNEC (Joint Enablers for the Realisation of NEC) project explored ways to support safety-related decisions, but given its time and resource limits it was only able scratch the surface. One output was a general set of safety risks focused around the deployment of NEC SoS [8].

In particular, the JERNEC project identified that at present *"Mitigation responsibility defaults to deployed users without a means to: evaluate the balance of operational risks; determine the most appropriate mitigation; determine when risk is acceptable or indeed what is considered acceptable"*. This will be exacerbated by another problem that JERNEC identified: *"NEC SoS safety requires vastly increased awareness of the entire human-technical SoS. Risk cannot be mitigated entirely by improved safety-related SoS engineering"* [8]

In order to use NEC systems to their full benefit the operators of such networks need to be able to understand the risks and safety applications of what they command. As

978-1-4244-8196-5/10/$26.00 ©2010 IEEE
DOI 10.1109/SOSE.2010.319

part of this picture the risks that are present in the network must be expressed in a clear and concise way. Once they have a clear understanding of the risks present in the network the operator can make justifiable decisions based around environmental conditions.

It follows that the modern commander needs processes to cope with increasing force complexity, tools that let him do something useful with the volumes of data NEC gives him, and some way to leverage the investment in platform and SoS safety cases. It is critical that he be able to understand the "risk picture" at any point in time.

Our aim is to develop techniques capable of automating risk assessment processes so that they become more accessible and informative to personnel. Informing personnel correctly ahead of operation can provide wide ranging benefits by analysing the networks properly then the operator is presented with a full picture on which to base their decisions. By performing this analysis upfront complex issues that are commonly found in subsequent enquires can be brought to light and positively influence the decision making at a time when it is most critical, as it is needed.

Many current approaches to military system safety are concerned purely with accidents; they do not take adequate account of the risks caused by hostile or even with friendly (blue on blue) action. The process we aim to produce will be a step towards resolving all these issues, by providing commanders with insight into their total safety margin, and letting them project the effect of any degradation of their network. This will allow them to make trade-offs between these two sources of risk. This, in turn, will allow the MOD to meet the obligations identified by Mr Justice Collins in April 2008: *"[Article 2 of the European Convention on Human Rights] imposes a positive obligation to protect life. Thus where there is a known risk to life which the State can take steps to avoid or to minimise, such steps should be taken"*.

2.1 A Practical Example – Überlingen

We can illustrate the difficulties of risk comprehension in SoS using a classic SoS accident. The Überlingen midair collision occurred on 1st July 2002. A Boeing 757 operated by the freight carrier DHL collided at right-angles with a Bashkirian Airlines Tupolev- Tu-154 jet resulting in 71 fatalities. Both aircraft were fitted with the Traffic Alert and Collision and Avoidance System (TCAS), which monitors the airspace around an aircraft giving warning about any potential collision between aircraft. This is achieved independently of air traffic control, and achieved by instructing one aircraft to increase and one aircraft to decrease altitude.

At the time of the accident both aircraft were under the authority of the Zurich Area Control Centre. The air traffic controller (ATC) first cleared the Boeing 757 to climb to FL320, then to climb onto FL360 (the same level as the Tu-154).

The TCAS on board the Tu-154 advised the pilot to climb, whilst the system on board the Boeing 757 advised a descent. The situation was then confused when the ATC contacted the Tu-154 pilot and instructed a descent. The Boeing 757 pilot followed TCAS advice to descend to FL350; the Tu-154 pilot followed the ATC's advice and descended to FL350 where the collision occurred.

The primary cause would seem to be confusion between the TCAS and the ATC. However, Nunes and Laursen [9] outline six contributing factors that indicate a strong lack of awareness in the operating procedure, and conditions on the evening of the accident.

Single man operation - one controller was responsible for the airspace during the shift rotation. A second controller was taking a break. During daytime operation a number of controllers operated the airspace allowing for a greater number of eyes to be on the lookout for problems. When Single Man Operating Procedures (SMOP) were in place the collision detection equipment should have been active – the Short Term Conflict Alert (STCA) system that provides a two minute warning to a collision.

Downgraded radar – maintenance work was being carried out on the main radar system leaving only the backup in operation. In theory this increased the required minimum separation of aircraft mitigating for the fact that the STCA was not operational. However, this directly contravened the rules dictating the running of the SMOP.

Dual frequency responsibility – during busier shifts the each controller is responsible for monitoring one assigned frequency using one display. At night an ATC is often responsible for more than one frequency. The ATC had a second monitor set up for arrivals traffic at a local airport – this pair of monitors was separated by over a metre. At the time of the incident the ATC was dealing with two aircraft on approach which required use of the local phone system.

Phone system errors – The ATC in Zurich needed to contact the local facilities at the airport to arrange for the approaches of the aircraft. The main telephone system was under maintenance. An unnoticed software failure had occurred in the backup system, so the local ATC could not be contacted at all. Other sectors noticed the developing problem (as their STCA system was operating correctly), but due to the telephony issues they could not contact the Zurich controller.

TCAS – TCAS operated correctly, notifying each aircraft of impending collision and giving safe avoidance instructions seven seconds before the ATC. The TCAS only provided information to the pilots onboard each aircraft; no information was relayed to the controller. However, TCAS did not take into account that an aircraft may not follow instructions; by descending, the Tu-154 caused an increase in demand for the descent of the Boeing 757. This failure to keep the ATC abreast of the situation is thought to be a key factor in the accident [9].

Corporate Culture – European pilots are advised to follow the advice of the TCAS in the case of contradicting information. Russian pilots are given the freedom to decide which information source to follow.

By viewing the situation as a whole many different factors appear to contribute to the accident. Most of these revolve around drawing an accurate picture of the situation on the evening of the accident. Information relating to factors 1-5 would have been available prior to the accident and played a direct role in the escalation of the situation.

Knowledge of the risks could have enabled mitigating action to have been taken. For example abandoning the SMOP so that the separate radar sets could be independently manned and workload shifted to maintain awareness of the situation between the Boeing 757 and Tu-154. This would have been especially prudent due to the inoperability of the STCA and phones due to maintenance.

3 Operational Risk Assessment and Safety

This section intends to briefly introduce similar process and highlight their limitations in order to provide a baseline for this work. There is no intention to go through the process of generating a live safety case, but instead to bring information through from the safety cases for individual components to the operational scenario.

The Minimum Equipment List (MEL) is a simpler relative of the safety case, and is widely used. MELs capture the results of risk assessment into a simple decision process for an aircraft. The flight conditions that are permissible, given safety requirements, can be determined given a list of the operable equipment on board. By knowing failures present on board the aircraft, and cross-checking against the MEL, then safety-based decisions can be made. Whilst the information is captured, a word of caution must be used in using it operationally, there is no direct method for tracing the instructions given by the MEL back to risks in the system; the MEL does not give reasons for its instructions. Additionally, no information is given about multiple failures [2].

Henery [2] created a prototype for a dynamic MEL which used an electronic representation of the Typhoon safety case to make decisions about when it was safe to fly. This took the safety case off the shelf and made the information it contained available to users.

The US army has attempted to adopt a process of in-the-field risk analysis known as Composite Risk Management (CRM). Johnson [10] questions whether it is possible for leaders in the field to adequately carry out this process. He lists a series of paradoxes that exist in the implementation of risk and hazard mitigation procedures. Andree [11] presents an apparently compelling case for the incorporation of CRM procedures, but says that the benefits of the process are challenged by complexity and the time critical nature of military operations. In addition the simple breakdown into score metrics does not reveal underlying complexity in the tasks undertaken; again the reasoning behind the risk is taken away from the user, they cannot question the reasons why the risk has reached the level claimed by the CRM. These come into direct conflict with the time taken to perform thorough risk analysis and can be at odds with the bias towards risk [10].

In our current work, we propose to create a lightweight assessment of risk based around the equipment safety cases that is regularly updated. This can then be continually checked via real-time monitoring to ensure claims, relied on by the network, are still delivered. Building on prior work at York on simulation-based hazard analysis, this will enable rapid risk assessment of military SoS. These processes will support hazard identification, hazard analysis and quantitative risk assessment during operation. This will provide a live risk analysis that shows, not the estimated safety of the SoS as projected a long time in advance, but the current level achieved by the force in the field.

4 Could this Have Helped in the Past?

The principal example previously stated in this paper centres around the midair collision over Überlingen in 2002. Analysis of the accident reveals the collection of causal factors outlined in Section 2.1. Cursory inspection of the information reveals that alternative action by the Russian pilot could have averted the accident. It is tempting to treat this as the factor that matters, and apportion the blame.

However, further inspection performed by Nunes and Laursen [9] paints a very different picture. A chain of decisions taken in the setup of the system on the evening in question lead to a particular series of events; the final one of which was human error. It was this network setup that provided the catalyst.

The air traffic controller took decisions based on the information that he was presented with at that time. This contained little actual information about the risks in the network – risk contained within the operating conditions. Given a greater awareness of the instantaneous risk the controller would have had the opportunity to make a better decision, based on the knowledge of the criticality of broken communication paths.

A process of this nature provides an opportunity to positively influence decision making, wherein a user can actively search out good solutions and practically view the risks being traded against operating conditions.

Coupling amongst the components of an NEC SoS is typically quite tight, producing complex interactions [12]. These structures provide a high level of flexibility in their connectivity. However, the nature of this flexibility is often hidden from the operator of such a network, buried within the complex interactions that dominate the response. This can result in a series of accident precursors that may not be

pulled up as serious concerns within the network – this flexibility allows reconfiguration that provides the properties that the system operator seeks; the system sits within an environment not unlike the flight envelope of an aircraft, however, the parameters of such an environment are not simple to quantify. As the system reconfigures it moves through this envelope, without information about the boundaries the operator does not have a clear picture about the risk that is present in the network at a given moment.

The Haddon-Cave report [13] highlights the importance of capturing precursors to major accidents in aircraft and argues the criticality of carrying the potential implications forward. As systems grow more complex these precursors become harder to spot and a more joined up thinking process is required to capture and track risks in the system to provide adequate notice.

In the case of the Überlingen accident it would be a fallacy not to state that had the Russian pilot obeyed the TCAS instruction the accident would have been avoided. However, this does not arrest the fundamental problem centred on the network being placed in an unsafe initial condition that went unrecognised. There were many ways in which the accident could have been prevented.

5 Bringing Analysis to the Users – Practical Issues

Our concept of dynamic risk assessment faces a number of challenges, mostly related to getting the right relationship between the process and the user. Any automation of the process will rob the user of natural intuition about the system; this section considers how to give it back.

5.1 Understanding Automation

By adding the automation the nature of how the system operates is fundamentally changed. This change of relationship can bring about problems when a user relies on the data that they are supplied with as part of the process.

By automating a system the user is removed from the direct process of information routing. This issue is one that is especially relevant in the accident of Aeroperu Flight 603, a Boeing 757, on 2nd October 1996. Whilst the accident had a wide range of contributing factors [14] the key cause was the blocking of a pitot-static tube (used to derive information such as airspeed, altitude and vertical speed) during a routine maintenance procedure.

Blocking the port caused contradictory warnings on the flight deck. One crucial factor in the accident was the information supplied by the air traffic controller based on the ground in Lima. The crew of the aircraft asked the air traffic controller to confirm their speed and altitude, because their cockpit instruments were giving confusing readings. He used the information on his monitor to confirm their altitude and speed. He was unaware of the sources of data that it used; his system used information from the aircraft's onboard transponder which sourced information from the flight deck, the commonality being the pitot-static tube.

5.2 User Accountability

The process of dynamic risk assessment introduces a new source of information into the decision-making process. The information sources brought online are likely to bring into question the accountability of decisions taken.

Accountability can impact on the usage of such a process, especially in an area such as safety or risk management. When decisions of an individual can affect the safety of others, there is a reluctance to rely on an automated aid. The process intends to provide information to aid decision making rather than replace the operator.

If problems then develop it is possible that the individual may face a subsequent enquiry into their actions. This situation becomes especially pertinent if information from the process is then used to show the situation at the time, demonstrating that the operator had the information available to take different action. Such a process could have the effect of "*[i]ncreasing accountability for decisions*" which "*creates pressure for decision-makers to become more cognitively complex*" [15] – it might force them to think harder about problems. Further to these issues Tetlock and Boettger found that an increase in accountability lead to buck-passing and postponement of decisions that could have had positive impact on safety [16].

This accountability can lead the user in one of two directions. On one hand it can promote thoughts of "*self-justification*" which lead the user to take decision that are not solely based around the broader alternatives and present situation. Alternatively, and beneficially, it can press the user into taking a more "*self-critical*" decision "*taking into account a broader range of alternatives*" [15] – as users became made more socially accountable they probed the network deeper to understand problems that were flagged.

5.3 Bias and Overreliance – Trust

When automation is used in the decision-making process the user must trust information they are given, especially if this information related to a decision on risk. Such a system must be designed with appropriate user trust [17] – if the user over-trusts, performance may degrade in cases where tasks are better performed manually. The counter is also true; if the user ignores the automation then potential benefits will be missed.

This level of trust is important in determining the use of the information provide, advice from an automated system will be ignored if it is believed less reliable than manual operation [18]. Dzindolet et al [19] have conducted a study in which users were presented with a series of images of camouflaged human figures. An automated tool

advised on the presence of a human. The tool had various parameters so that it was capable of performing either substantially better or worse than the user. When the tool outperformed the user, their confidence and trust increased.

In a further study users were given information to possible reasons about errors made by the tool. When they understood the processes undertaken by the tool and likely factors that could cause errors their awareness was increased. Through understanding possible causes of errors they could identify problems yet still maintain trust [20].

5.4 Bias and Overreliance – Self-Confidence

Lee and Moray [21] investigate issues around the confidence of users in themselves and the links with use of automation. This is shown by the preference of a user to trust their judgement over any advice presented by an aid. This work is extended by Kantowitz et al [22] where harmful information damaged trust in the automation. If self-confidence were seen to exceed trust, information from the automated system would be ignored; this is especially true in the case where the environment is familiar.

5.5 Operation in Practice

The addition of new features can prove problematic as users often find methods for using them in ways that the designer never intended. Walker et al highlight these problems in two different sets of applications; the creation of the short-messaging service for mobile phones [23] and the use of the ComBAT software on the Bowman radio system when undergoing trial [24].

The ComBAT software suite operates on the Bowman network. It provides a *"highly prescribed method of working"* through a set of pro-forma, however, as part of the design process a Free Text facility was provided.

During a trial of the system it was found that a disproportionate amount of communication took place via Free Text: 9% of the total communication representing 73% of that started by users [24]. The communication protocol was never anticipated to be as widely used. Users of the system had found a niche in the specification and adapted it to their benefit.

Any natural scepticism about automated technology can lead them to abandonment of its use as was observed in research conducted by Dzindolet et al [19]. In field trials observed by Salmon et al [25] problems caused abandonment of technology in favour of paper and pen.

These problems were primarily caused by unfamiliarity with the technology and uncertainties over its capabilities. This required personnel to make more decisions about the system itself, and coupled with poor feedback, added to the complexity of the situation. This lead to users asking questions more focused on system performance rather than operational requirement [25].

This has lead to Salmon et al [25] concluding that there have been three specific factors that caused these problems with the realisation of automated devices:

1. *"Lack of understanding on behalf of the system designers on the decision making process undertaken*
2. *Poorly designed graphical user interfaces and associated tools rendered the aids difficult to utilise*
3. *Technological limitations on the systems in place limited the performance of the system"*

6 Conclusions

This paper has investigated the need for dynamic risk assessment in NEC SoS, provided a rationale for developing dynamic risk assessment, and identified problems caused by the introduction of such a process.

The mid-air collision at Überlingen provides an example where the air traffic controller lacked a clear picture of the conditions operating within the network. If the specific risks posed by the network configuration made apparent to the controller, then he might have made different decisions.

Later analysis pointed to these different network operating criteria as distinct steps leading to the accident. The information from this analysis has then fed into future working practice. Dynamic risk assessment can provide an early indication of network factors that are often only observed in an after-the-fact accident investigation. The benefits of gathering and efficiently presenting this information upfront will be to provide new information sources to facilitators of network enabled systems, thereby enabling better decision making in real-time.

Whilst the introduction of such a process has the ability to allow a user to develop a deeper understanding of the network with which they interact, its presence introduces its own hazards into the network. These hazards are primarily concerned with the interaction between user and process; the nature of this interaction is critical in determining use and in limiting any hazard. Information must be efficiently presented to the user in order to limit any ambiguity that can arise through the complexity in the system. It is important to inform the user of the conditions within the network so they can take good decisions.

This interaction is not solely driven by the user interface (when realised as a tool), although this is a very important component of such a process in its own right, but by a much more complex process of user feedback. The introduction of such a process places new pressures on the user, just through its presence – there is accountability on the user on which they can be judged.

The trust a user places on the process becomes a critical factor in its usage. Trust is important in a user using any process to its full potential. Too little trust will result in

the potential benefits being lost through under-utilisation. Equally too much trust can result in over-reliance and failure of the user to intervene when necessary. Therefore a focus must be placed on developing a process that presents useful information to the user; moreover the process use to obtain this information must be as clear as possible in order to foster better user understanding.

Acknowledgement

The authors would like to thank the Ministry of Defence Software Systems Engineering Initiative (SSEI) which is funding this project.

References

[1] G. Klein, *Sources of Power: How People Make Decisions*. Cambridge, Massachusetts: MIT Press, 1999.

[2] L. Henery, "The Eurofighter 'Operational' Safety Case," MSc Thesis, University of York, (2001).

[3] "Joint Service Publication 777 - Network Enabled Capability," Ministry of Defence, 2005.

[4] R. Alexander, "Using Simulation for Systems of Systems Hazard Analysis," PhD Thesis, University of York, (2007).

[5] G. Despotou, "Managing the Evolution of Dependability Cases for Systems of Systems," PhD Thesis, University of York, (2007).

[6] M. Hall-May, "Ensuring Safety of Systems of Systems - A Policy-Based Approach," PhD Thesis, University of York, (2007).

[7] M. J. D. Henshaw, D. J. Gunton, and E. N. Urwin, "Collaborative, Academic-Industry Research Approach for Advancing Systems Engineering," in *Proceedings of the 7th Annual Conference on Systems Engineering Research* Loughborough, UK, 2009.

[8] A. Matthews, S. Williams, and A. Campbell, "JERNEC TIN005 NEC Systems of Systems Safety/Risk/Liability Final Report," UK Ministry of Defence, 2009.

[9] A. Nunes and T. Laursen, "Identifying the Factors that Contributed to the Überlingen Mid-Air Collision," in *Proceedings of the 48th Annual Chapter Meeting of the Human Factors and Ergonomics Society* New Orleans, Louisiana, USA, 2004.

[10] C. W. Johnson, "The Paradoxes of Military Risk Assessment," in *Proceedings of the 25th International Systems Safety Conference*, Baltimore, USA, 2007.

[11] R. Andree, "Personnel Injury: Great Flying Stoves!," in *US Army Countermeasures*. vol. 27: Centre for Combat Readiness, 2006, pp. 10-11.

[12] Z. H. Qureshi, "A Review of Accident Modelling Approaches for Complex Critical Sociotechnical Systems," Australian Government Department of Defence - Defence Science and Technology Organisation, 2008.

[13] C. Haddon-Cave, "The Nimrod Review - An Independent Review into the Broader Issues Surrounding the Loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006," 2009.

[14] P. B. Ladkin, "News and Comment on the Aeroperu B757 Accident; AeroPeru Flight 603, 2 October 1996," 2002.

[15] L. J. Skitka, K. Mosier, and M. D. Burdick, "Accountability and Automation Bias," *International Journal of Human-Computer Studies,* vol. 2000, pp. 701-717, 2000.

[16] P. E. Tetlock and R. Boettger, "Accountability Amplifies the Status Quo Effect When Change Creates Victims," *Journal of Behavioural Decision Making,* vol. 7, pp. 1-23, 1994.

[17] B. M. Muir, "Trust Between Humans and Machines," *International Journal of Man-Machine Studies,* vol. 27, pp. 327-339, 1987.

[18] M. T. Dzindolet, S. A. Peterson, R. A. Pomranky, L. G. Pierce, and H. P. Beck, "The Role of Trust in Automation Reliance," *International Journal of Human-Computer Studies,* vol. 58, pp. 697-718, 2003.

[19] M. T. Dzindolet, L. G. Pierce, H. P. Beck, L. A. Dawe, and B. W. Anderson, "Predicting Misuse and Disuse of Combat Identification Systems," *Military Psychology,* vol. 13, pp. 147-164, 2001.

[20] T. B. Sheridan, *Telerobotics, Automation and Human Supervisory Control*. Cambridge, Massachusetts: MIT Press, 1992.

[21] J. D. Lee and N. Moray, "Trust, Self-Confidence and the Operators' Adaptation to Automation," *International Journal of Human-Computer Studies,* vol. 40, pp. 153-184, 1994.

[22] B. H. Kantowitz, R. J. Hanowski, and A. C. Kanotwitz, "Driver Reliability Requirements for Traffic Advisory Information," in *Ergonomics and Safety of Intelligent Driver Interfaces*, Y. I. Noy, Ed. Mahwah, New Jersey: Lawrence Erlbaum Associates, 1997, pp. 1-22.

[23] G. H. Walker, N. A. Stanton, D. P. Jenkins, and P. M. Salmon, "From Telephones to iPhones: Applying Systems Thinking to Networked, Interoperable Products," *Applied Ergonomics,* vol. 40, pp. 206-215, 2009.

[24] G. Walker, N. Stanton, P. Salmon, and D. Jenkins, "From Clansman to ComBAT: HFI Principles for NEC System Design," Brunel University, 2008.

[25] P. M. Salmon, N. A. Stanton, D. P. Jenkins, G. H. Walker, L. Rafferty, and K. Revell, "Decisions, Decisions... and Even More Decisions: The Impact of Digitisation in the Land Warfare Domain," in *Proceedings of the 9th International Conference on Naturalistic Decision Making*, London, UK, 2009.