The Agile Incident Response for Industrial Control Systems (AIR4ICS) Framework

Dr. Richard Smith [a], Prof. Helge Janicke [b], Dr. Ying He [c], Dr. Fenia Ferra [a], Mr Adham Albakri [a]

a. Cyber Technology Institute, School of Computer Science and Informatics, De Montfort University, UK
b. Cyber Security Cooperative Research Centre, Edith Cowan University, Australia
c. School of Computer Science, University of Nottingham, UK

Abstract

Cyber incident response within Industrial Control Systems (ICS) is characterised by high levels of uncertainty and unpredictability and requires a multi-disciplined team that encompasses personnel business operations, Operational Technology (OT), IT, security operations and media engagement to be effective. Such teams require a dynamic decision framework to allow ICS operators to maintain services during the recovery of full operating capability. There is empirical evidence that static incident response playbooks do not provide enough flexibility in their definition to support situations outside of the scope of their initial definition, and that they have been ignored when cyber incidents have occurred. A thematic analysis of semi-structured interviews with ICS incident response professional identified three main areas of concern: communication, information sharing between knowledge areas, and achieving external buy-in. The Agile Incident Response for Industrial Control Systems (AIR4ICS) framework has been developed to integrate Agile techniques into the Cyber Security domain of incident response. AIR4ICS provides a dynamic approach to improve situational awareness, information sharing, collective decision-making and response flexibility within the unique context of ICS. The techniques used in AIR4ICS were initially shaped by interviews with professionals with experience of protecting ICS, structured using the Scrum methodology, and refined through a series of Cyber Incident Response exercises with Incident Response professionals facing-off against specialist ICS Red Teams.
AIR4ICS has resulted in a framework that provides a modular approach that can be adapted to fit the working practices, skillsets and priorities of individual organisations. The framework improves communication, promotes information sharing between knowledge areas, and increases external buy-in.
Ultimately, AIR4ICS provides a dynamic decision framework that allows Incident Response Teams to manage uncertainty and unpredictability to reduce the time taken to restore normal operations.

Keywords

Incident Response, Agile, Industrial Control Systems, SCADA, threat hunting

1. Introduction

Contemporary Industrial Control Systems (ICS) have evolved from isolated systems to connected architectures, integrating operational data sources and the wider supply chain to improve business efficiencies. Because of this architectural shift, devices not designed to defend against malicious attack are exposed to Internet connections, and are therefore susceptible to cyber attacks (He & Janicke 2015).

Traditional ICS technologies are often unfamiliar to contemporary Information Technology (IT) security professionals and the methods and tools they typically utilise may not necessarily be effective in industrial environments. In order to determine whether existing incident response techniques and mechanisms are applicable to ICS it is necessary to consider the characteristics of such systems to determine where and how they deviate from the behaviour of IT systems. For ICS operators to adequately prepare for possible cyber incidents, methods and tools must be implemented that support the response process, cognisant of the nature of control system technologies. To truly address this challenge and establish incident response as part of 'business as usual' activities as usual the process must be owned by a cross-functional team that brings together business, IT security and operational technology (OT) expertise.

Incident response is an established concept (e.g. *NIST SP800-61)* of preparing for, and responding to, unplanned incidents that negatively affect a business or organisation (Eugene Schultz & Shumway 2001). The US Department of Homeland Security (2014) highlighted that incident response matured as a process long before modern IT, and historically focused on damage by storm, flood or vandalism, although more recently they have expanded the scope to include IT and OT systems (Cook et al. 2018).

Regardless of the cause of the situation, incident response planning produces contingency plans to manage the negative impacts on critical equipment and operations. ICS operators typically have plans in place for loss of essential power, supplies, and output, but it is only recently that these plans have started to consider cyber impact. However, many of the processes applied to incident response in ICS are driven by the approaches applied to IT business systems, which differ from ICS, and as a result may be ineffective or worse, amplify the impact of cyber attacks on such industrial infrastructure.

There is significant focus on improving Incident Response (IR) within critical national infrastructure with solutions ranging from the use of enhanced reconnaissance; autonomous defence operations to subversive machine learning (e.g. IAEA - SIREN project: Technologies for Ensuring Safe and Secure Incident Response Strategies for Nuclear Facilities). There is a clear difference in the response within the ICS context in comparison to IT; whilst many IR technologies can be applied, the considerations and defence strategies that apply in the safety critical context of ICS and their underpinning OT systems, in particular for essential services such as energy or communications, system down-times or loss of availability are unacceptable and can lead to loss of life or livelihood. Cyber management plans are mandated for operators of Critical National Infrastructure by the UK implementation of the NIS Directive, making cost-effective, efficient implementations important for business.

Security vulnerabilities have been reported in control systems with an observable increase in cyber threats (Nikishin 2015; Maglaras et al. 2018). Unlike IT systems, where patches to mitigate vulnerabilities can be installed within short timescales, patching is often only possible by halting activity on operational devices and therefore is further time constrained in many cases. These changes to an ICS must also be rigorously tested before deployment to ensure the risk of unintended consequences is contained (Larkin et al. 2014; Cook et al. 2017) as the impact can extend to physical damage (Nikishin 2015), denial of national infrastructure, environmental contamination (Nikishin 2015; Schultz & Shumway 2001) as well as financial loss (Cornelius et al. 2008). This is exacerbated by the need to certify the changes with the relevant regulatory body, adding cost and often significant delays.

Rigid, procedural incident response processes are increasing the predictability of the defence efforts and make it more difficult to protect the remaining infrastructure and business functions in the context of fast-pivoting and multi-pronged cyber-attacks. Playbooks often form the central tenet of most organisations' incident preparations. Unfortunately, these tend to be monolithic documents, overly prescriptive, slow to change and often suffer from a lack of responsible oversight. Playbooks very rarely

include any elements of ICS security, having been tailored to the IT estate under threat, and whilst they can be useful for dealing with small scale threats they are insufficient to deal with APTs that might target industrial systems. Naedele 2007 argues that the costs involved in ICS security are prohibitive, especially within critical systems, when the perceived risks to an organisation or infrastructure cannot be adequately quantified and a business case not satisfactorily articulated. This often leads to an underdeveloped incident response capability in the deployed operational ICS (Pauna 2013).

Key to a successful OT incident response is the amalgamation of knowledge and experience of individuals from various pillars of the organisation. The diversity of responsibilities and requirements in different pillars can lead to conflicting priorities and concerns. This separation of objectives, coupled with subject specific terminology (e.g. IT layer 3 device vs OT layer 3 device) reduces the performance of the team. This is compounded by the fact that it is rare that team membership remains fixed for the full duration of an incident, individuals will often have other duties or are only brought on board for specific tasks. This occurs reactively, once a gap in capability has been identified, which introduces a delay in the response. The constant flux of skillsets and personalities poses significant difficulties for those leading IR teams.
When IR crosses IT/OT boundaries communication between stakeholders, often from different disciplines and organisational hierarchies, is frequently problematic thus reducing situational awareness of the team. Agile approaches welcome changing requirements and are driven by value and understanding of the system by a cross-functional team able to manage conflicting stakeholder requirements. This approach is therefore geared to environments where change is constant and the environment and objectives are not clearly identified or defined. This framework advocates the integration and evaluation of agile methods and practices, used in e.g. Scrum and Kanban, to provide a security incident response team with the ability to respond quickly to changes whilst maintaining the focus on the business and its value-chains. By its very nature incident response needs to be adaptive to a highly dynamic nature of cyber-attacks and anticipate further exploitation paths of the adversaries and requires a cross-disciplinary team effort to respond effectively.

2. AIR4ICS Agile Approach

For many years project management methodologies followed a linear design, such as the waterfall method (Royce 1970), where one phase could not start until the previous phase was completed and once complete that phase would not be revisited without significant cost. The main example of this is the capture of requirements, any change to requirements proved costly and often led to delays, increased costs or project failure (Whittaker 1999). As software became more complex, and customer requirements for a quicker delivery and deployment cycle increased, it became obvious that in many cases a more flexible and adaptive approach was required. This eventually led to the publishing of the Agile Manifesto (agilemanifesto.org) which defines the 4 core values for Agile development as:

1) Individuals and interactions over processes and tools
2) Working software over comprehensive documentation
3) Customer collaboration over contract negotiation
4) Responding to change over following a plan

By adopting the 4 values, along with the 12 principles also presented in the Agile manifesto, software teams were able to reduce the time required to bring products to market and facilitated rapidly changing requirements throughout the project lifecycle (Lindvall 2004). The adoption of Agile methods has increased rapidly in the 18 years since the publication of the manifesto, with some surveys indicating that 97% of respondents now use some form of Agile practice (techbeacon.com). This innovative approach is geared towards environments where change is constant and the objectives and priorities change rapidly. By adapting Agile tools and techniques the proposed approach facilitates dynamic security incident response.

The AIR4ICS framework addresses the traditional activities of incident response outlined in Figure 1 with emphasis on *Pre-Incident Response*; *Initial Response*; *Formulate Response Strategy*; *Investigate the Incident*;

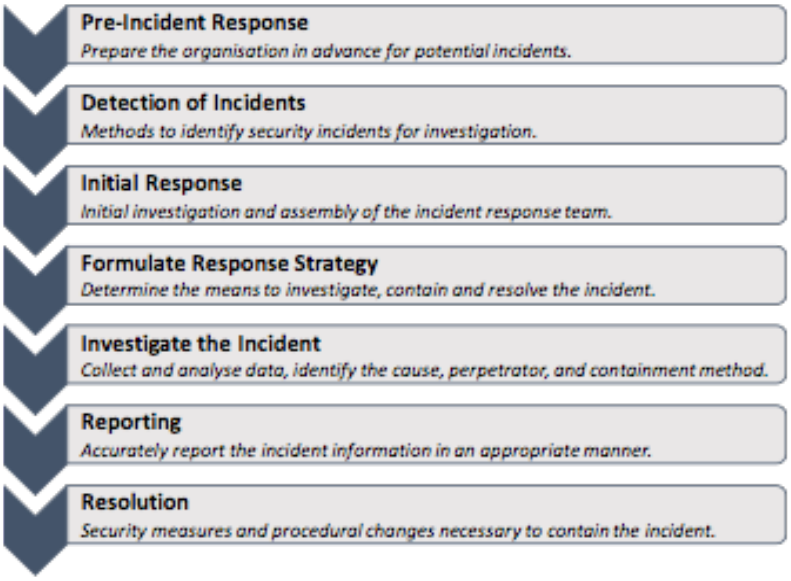

Figure 1 Traditional Incident Response activities

Reporting. This is linear approach matches the waterfall method, with each phase following on from the last providing centralised control for managers. Effort is allocated to each phase and once completed no further effort is expended on that phase.

However, in reality investigations are rarely linear. Effort will vary dependent upon the current state of the investigation and this is particularly the case when dealing with ICS and OT technology. As an example, an incident response team will develop an initial response when activity is detected on the enterprise network of an organisation. As the investigation progresses and activity is eventually found on the OT network they will need to spend effort developing a new initial response strategy to incorporate the OT systems. That is why the AIR4ICS framework integrates an iterative approach to this sequence that will emphasise the continuous improvement of the IR process. The dynamics of a complex cyber-attack may require several iterations and revisions to the response strategy, depending on the information gained during the attack.

The AIR4ICS framework structures the Incident Response process into short bursts of activity analogous to SCRUM's sprints during which the objectives of the traditional phases (Initial Response to Resolution) will be partially achieved and steps to the resolution being added in iterative steps. This process is indicatively depicted in Figure 2, showing how in AIR4ICS all activities from Detection onwards are undertaken by the team to some level. The decision to what level additional detection, or a revision of the initial response or strategy is required is driven by the cross-functional team and continuously planned and reviewed in every sprint. Unlike for development projects, these sprints are shorter in duration allowing the team to respond and adapt to adversary action or unanticipated changes in their operating environment as a consequence of physical effects on the ICS. The approach to identify the objective for the next sprint is driven by the value of the response and the risk

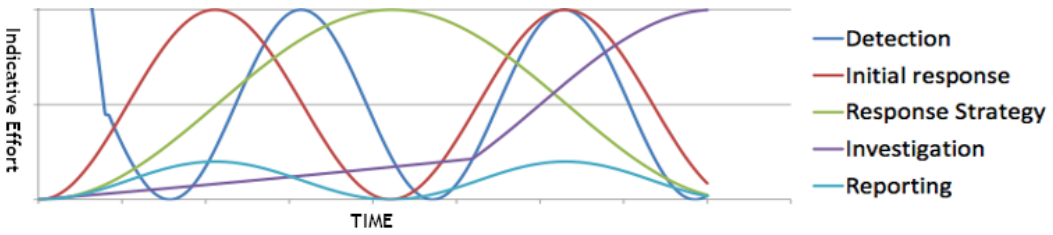

Figure 2 AIR4ICS Incident Response effort

associated with the attack in terms of probability of success and impact on the business. The cross-functional team is ideally placed to establish the best course of action and where necessary escalate this through the business, external organisations such as product Computer Emergency Response Teams (CERT) and National CERTs. This approach also lends itself to support the coordination of multiple IR activities for attacks that are overlapping in scope, similar to e.g. the BlackEnergy attack in the Ukraine where a number of attacks were coordinated to increase impact and reduce the organisation's ability to recover.

2.1. AIR4ICS novelty and contribution

Traditional incident response teams are very hierarchical, with individuals assigned to specific roles such as threat hunting, firewalls, networks and more. Whilst this approach has benefits it also leads to the creation of information silos. Staff members become focused upon their own individual tasks and do not have visibility or understanding of what others are doing. This is turn leads to the introduction of mistakes or inefficiencies as work is duplicated or responsibility for key information becomes unclear. Reducing the efficiency of the response increases risk and impact of malicious actions against an organisation.

The rising threat to Industrial Control Systems presents a further challenge for traditional incident response teams. ICS technology does not operate in the same manner at standard IT equipment, when a single IT machine is compromised the impact (barring network traversal) is often limited to the functionality of that machine and those machines with significant impact to the business process are placed on the critical asset list. In the OT domain devices rarely exist in isolation, compromising individual aspects will have knock on effects along the entire process. This extends to the operation of the incident response team, changes made during the course of an investigation may have significant impact for other team members further down the production line. This means that IR professionals are required to understand not just the implications of their own work but also that of all others involved when tasked with protecting ICS equipment.

AIR4ICS presents a novel approach to the management of incidents and the operational practices of incident response teams; placing an emphasis on adaptability by informed, confident professionals, rather than rigid procedures followed by rote by staff disconnected from their allotted tasks.

AIR4ICS delivers improvement in four key areas:

Situational awareness: All team members are informed and involved in the strategic planning and implementation of the response. Traditional responses rely upon existing risk assessments to identify critical devices and allocate resources accordingly. However, risks are not static; as evidence of malicious activity is identified the priority of potential targets will change. For example, if the only evidence of attacker activity is on the enterprise network effort might reasonably focus upon the domain controller or servers containing financial information would be recognised as being at the greatest risk. Once there is evidence of malicious activity on the operational technology network the overall risk picture would change, ICS devices would then become the focus of defensive actions and the strategy of the incident response team would need to shift accordingly.
AIR4ICS facilitates the rapid changing of priorities and dissemination of this information to all team members. By providing a greater understanding of the current investigation Team members report increased confidence in their decision making.

Discipline integration: Including disparate business elements, such as Engineers or Business Analysts, into the IR team facilitates knowledge exchange between these groups and the cyber security professionals. Traditional approaches often have personnel from other business departments acting as consultants, queried on specific questions but otherwise provided limited information about the response. By incorporating the different business elements into the IR team those individuals will be able to provide more contextual assistance and disseminate their expertise shifting towards a T shaped team, where individuals have a much greater understanding of all aspects of the business.
AIR4ICS methodologies aid the integration of new personnel into the IR team and facilitate information sharing between the entire group.

Communication: In a rapidly changing, high pressure environment it is difficult to ensure efficient information dissemination, be it new threat intelligence or changing a password. Information is often only shared within a team or to a manager if at all. Communication between teams is reliant upon mangers sharing pertinent information between themselves before informing their team. This approach leads to delays whilst the relevant information is transmitted or redundant effort as tasks are duplicated.
The tools presented in AIR4ICS ensure that information is transferred quickly and efficiently, not just to team leaders but to all those involved in the investigation. Ensuring that all relevant information is readily available minimises time delays in an already high-pressure environment, allowing actions to be completed sooner and reducing repetition.

Staff motivation: Tasks are usually assigned by the team manager (or above). Individuals often become focussed similar tasks regardless of the circumstances, with individuals rarely stepping outside their speciality. This limits the individual's ability to grow their knowledge base and often means that the tasks seen as most boring are left to the most junior staff.
The flat structure recommended by AIR4ICS facilitates greater ownership of tasks by team members. By providing individuals a say in the tasks that they complete and trusting them to get the job done they will be more motivated in the completion of these tasks. This allows them to control their own personal development and will lead to an increased sense of well-being.

3. Professional Interviews

Each organisation and industrial response team will have their own methods of operation, at both a technical and personal level. Whilst no two will ever be identical, it is important to identify common practices and issues faced by incident teams tasked with protecting ICSs to identify where agile techniques can prove beneficial.
Incident response teams operate in a multitude of ways; some are permanent teams split into differing service levels, others are groups of individuals brought together because of their skillsets and knowledge for the duration of an incident. To ensure that the study was representative of the differing team organisational types the sample was selected from a cross section of Incident Response professionals from industry and government.

3.1. Interviews

A semi-structured interview schedule was designed by the research team including specific questions that focussed upon aspects critical to the study. Questions were designed using the 12 Agile principles as a basis to probe for specific information on the topic, whilst focusing on the current issues and challenges faced when dealing with ICS, e.g. "What are the main factors impacting a responses' effectiveness". To ensure that areas of best practice were also identified questions were tailored to include both positive and negative experiences of the interviewee.

Prior to each interview, participants were provided with a detailed information sheet outlining details of the research, including aims and objectives, as well as information on taking part on the project, such as protection about anonymity and right to withdraw. Participants were asked to provide verbal consent and they were also provided with full details of the lead researcher.
Interviews took place between the 16th April and 2nd August 2019 and lasted between 1 hour 30 minutes and 3 hours.

3.2. Analysis

The sensitive nature of the contents and professional meant that note taking has been used as a means to record interviews. Thematic analysis, as described by Braun & Clarke (2006), has been used for the analysis of the data. The analysis consisted of the following stages:

a. familiarization with data
b. production of initial codes
c. searching for themes
d. reviewing the themes
e. defining and naming the themes
f. producing the report

The approach of the analysis was inductive, and thus

the themes emerged were data driven. Inductive thematic analysis is data-driven; hence theme development was not restricted by an existing coding framework or the researcher's interest in the area. All transcripts were reviewed by another researcher to check for validity in analysis. No differences were reported in relation to coding, however, several themes were expanded to include subthemes. The themes identified were:

1. How incidents may vary in volume and impact and how this influences IR and its effectiveness. Most professionals noted that they are mainly prepared to deal with common incidents, and when it comes to incidents of higher sophistication and scale they are often struggling to deal with. They mentioned that insider threats are common, and they result from inconsistencies and fallacies in policies, ie. access to certain systems, removing access to ex-employees etc. Moreover, they noted that investigations and IR are commonly economic driven, which is a factor that might influence or limit IR's effectiveness.

2. There is an overload and at the same time a lack of information available. More precisely, there is an extreme volume of information to be digested (information digestion), while it seems that quite often there is a lack of information about systems, and how systems work, which is commonly attributed to how old and complex OT systems might be, as well as the lack of people having the appropriate expertise being available.

3. The IR teams are focused on individual tasks and responsibilities, instead of team aims and goals, while there is often a lack of OT personnel in the operation rooms.

4. There is a lack of communication between departments and IT and OT experts. This was also the case when 3rd party companies were involved. 3rd party companies may be located in different countries, making communication even more challenging.

5. Playbooks, as well as certain tools and techniques are being used. Some of the tools and techniques involved were: antivirus, forensic software, network monitoring, log files etc. With regards to playbooks, while most professionals said that they do use it in actual practice, they noted that playbooks' effectiveness is questionable and mainly IT focused.

6. That their approach is commonly adaptive, but only when a need for adaptation was identified. Professionals noted that they follow a consistent approach with common cases, with adaptation only required in more sophisticated cases.

7. There is no consensus in the metrics and methods for evaluation of their work. However, it was noted that both metrics and defining success might be challenging.

8. That media and external communication is a great concern when dealing with an incident.

Common elements identified across these themes are communication, information sharing and situational awareness. AIR4ICS has therefore been designed to increase these elements within Incident Response Teams, by utilising an iterative experimental approach the team were able to incorporate feedback from professionals during evaluation exercises to help refine the framework.

4. AIR4ICS Roles

Traditional Incident Response teams often follow a rigid, hierarchical structure. Individuals are allocated to a specialised role, such as firewalls, threat hunting etc… This segregation of tasks often leads to the creation of information and knowledge silos, where attempts to pass information and skills to other relevant units can be suboptimal. This effect is magnified within the Operational Technology domain where dealing with an incident will require significant input from Engineers, Business Analysts, Communications, Legal, Management and more.
Agile principles aim to break down these silos by creating more integrated teams. To that end there are only three distinct roles within an Agile IR team:

1. **Incident Owner**

2. **SCRUM master**

3. Team Member

4.1. Incident Owner

- Owns the incident vision/strategy
- Acts as the point of contact with senior management
- Acts on behalf of the customer (where different from organisation)
- Controls and prioritises the Incident Backlog

This role is often taken by an experienced IR manager or Technical Lead.
The essential criteria for the role are an intimate knowledge of the dealing with an incident and an understanding of the value to the organisation of a successful response. They are responsible for handling interactions external to the team and ensuring that any information is disseminated to the team, thus protecting the team from multiple, potentially conflicting, sets of requirements.
The incident owner is also responsible for the incident backlog. Even though anyone can create new items for the incident backlog the incident owner will create many of them and is responsible for ensuring that all items are well formed, clear, properly sized and considered at some point during the incident.
They are constantly responsible for dissecting information from predictive attack sources such as attack trees and evil user stories into reasonably sized backlog items, clearly identifying acceptance criteria for each task. They are in a constant loop of ingesting information from stakeholders and feeding it into the backlog to ensure that the team is well placed for planning cycles. This approach allows for feedback and change whilst enabling strategic planning and expectation management.
The backlog is ranked by the highest value items and the Incident Owner is responsible for ensuring that the high value stories are delivered first. Value can be based upon customer value, business value, risk value or learning value. It is the Incident Owner that accepts an investigation strand as completed, using their knowledge of the overall incident to redeploy freed up resources. It is up to the Incident Owner what to report and when to external clients (such as the board or customers) but the choice of high value items at the earliest possible opportunity ensures that results are more likely to demonstrate reasonable measures taken in the face of regulatory requirements. Additionally, they are responsible for ensuring that all required tasks are allocated during a sprint, including those that no team member has taken voluntary ownership.
The Incident Owner best serves the team by being available to answer questions, assess results and provide feedback in real time.

4.2. Scrum Master

- The Scrum Master is responsible for ensuring Scrum is understood and enacted.
- Is a servant-leader for the Incident Response Team
- Removes obstacles and improves the Incident Response Team's performance to maximise value.

The Scrum Master role is often taken by an experienced team member with excellent communication skills. It is highly beneficial if the person has experience of using Agile techniques previously but it is not a requirement.
It is essential that the Scrum Master has the ability to multi-task whilst retaining an overall situational awareness of the incident. Their role is that of a Servant-Leader for the Scrum team. As such they are responsible for ensuring the Scrum is understood and enacted, taking a facilitators role during regular meetings. During normal operation they will act as a focal point for information exchange, ensuring that critical information is disseminated to all Team Members and the Incident Owner. This will enable them to ensure that the information provided through the Incident board is kept up-to-date whilst ensuring that Team Members have all of the information necessary to make informed decisions.
A key element of the role is to remove obstacles that impede the progress of the team during the incident. This can take many forms from requesting additional resources through to facilitating break out meetings for technical discussion. By ensuring that the team is able to perform to the best of their abilities the Scrum Master maximises the value of the response.
The Scrum master also has a coaching role, enabling Team Members to enhance their learning, make decisions and achieve their goals. By empowering

team members to have an increased confidence in their capability to make informed decisions and achieve ownership of their own development the mental load placed upon Team Members will be reduced and lead to a reduced burn-out rate.

4.2.1. Scrum Master and Incident Owner

The Scrum Master will work closely with the Incident Owner in overseeing the response. By ensuring that the flow of information remains high, with any developments reported through the Incident board, the Scrum Master supports the Incident Owner in effective Incident Backlog management. They will also ensure that the Incident Owner knows how to arrange the Incident Backlog to maximise value.

4.2.2. Scrum Master and Incident Team

As part of the coaching element of the role the Scrum Master will be responsible for supporting the team in self-organisation and cross-functionality. Often Team Members will select tasks that align to their current knowledge base, introducing the risk of information silos occurring. The Scrum Master ensures that individuals are involved with at least one task that is not within their area of expertise per Sprint. This will develop a broader skill base and reduce the potential for single points of failure within the team.

The Scrum Master is responsible for facilitating Scrum events as requested or needed. It is their responsibility to ensure that the daily Scrum meetings do not overrun and become long technical discussions. If situations arise requiring the discussion of significant technical information the Scrum Master will convene a Technical Discussion Meeting and where possible act as Coordinator to ensure that discussion progress and do not become stalled by opposing viewpoints.

Acting as a constant point of contact for Team Members the Scrum Master will analyse the performance of the team, identifying examples of excellence that can be shared amongst the team along with any elements that need to be modified to optimise team performance.

4.2.3. Scrum Master and Incident Backlog Items

Depending upon team size and incident complexity the Scrum Master need not be a full-time role. Where possible they can assist Team Members with regular tasks from the Incident Backlog. Where this happens care must be taken to ensure that the Scrum Master does not spend too much time on the Backlog tasks to the detriment of the Scrum aspects of the role.

4.3. Team Members

- Self-organising
- Cross functional
- No titles
- Accountable as a whole

Professionals who do the work of providing the response to minimise and mitigate the impact of an incident. They are structured and empowered by the organisation to organise and manage their own work. Where possible team members should be encouraged to self-select ownership of at least one Incident Backlog Item every sprint. By allowing greater autonomy in task selection team members are more confident in their actions and display an increased level of satisfaction within their role. This can be implemented on an incremental basis, with the number of self-selected tasks per sprint increased as the team becomes more familiar with the workstyle.

4.3.1. Sub Teams

When a number of people are working on related tasks it is natural that they will form a sub-team. Wherever possible sub-teams should not be pre-defined and instead allow dynamic membership as the situation demands. These sub-teams are expected to have a lifecycle of no more than a single sprint, as they should be defined by the Backlog tasks rather than the Team Members present.

4.3.2. Cross-functionality

Team members will develop their skillsets to increase their capability within other elements of an Incident Response Team. They will still retain a specialisation but this will be supplemented by additional knowledge within other domains. The idea is to create T shaped teams, with in-depth knowledge in some areas but with working knowledge within the other areas required for the team. It is vital that at the least each Team Member develops their knowledge of Operational Technology

systems to allow them to operate effectively within the environment.

4.4. Capability Maps

Due to the varied nature of Industrial Control Systems a core element of any response is an understanding of existing system requirements. Even where existing information, such as safety assessments, are provided it is not guaranteed that there will be the expertise within the team to adequately assess the likely impact of changes made to the system, leading to security teams potentially expediting the attack. Therefore, it is vital to ensure that personnel are assigned to tasks most suited to their skillset.

To facilitate the creation of well-rounded teams AIR4ICS recommends adapting the Agile concept of a Capability Map. A capability map is used to visualise the current capability of the team to respond to an incident. The skills required to respond to an ICS incident outlined in Figure 3 have been thematically identified through consultation with OT cyber response professionals. For each skill an assessment must be made as to the current capabilities and skillsets within the team to quantify any performance gap that exists. The performance gap is then rated within a five-point scale from Low to High. Similarly, the value to the response of each skill is assessed and assigned to the five-point scale as before. Finally, the risk to the system associated with each skill is designated as either Low, Medium or High risk.

Any areas where serious disjoint between the performance gap, value and risk occur is considered significant and can be identified and remediated through either training or bringing in additional Team Members with the knowledge required.

The Capability Map is the three-vector image representing the details identified below. By presenting the information in a graphical rather than tabular format key information, such as areas with high value, risk and performance gap, is more easily identified and remediated by introducing new team members.

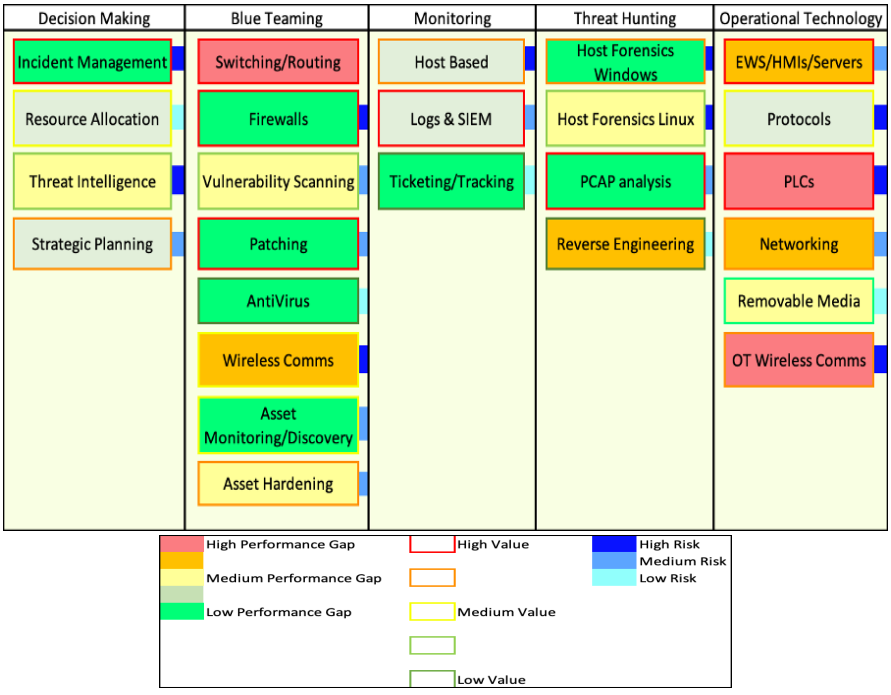

Figure 3 Example Capability Map

Individuals will self-assess their competence in each area to allow incident managers to make more informed decisions about task allocation. Areas with a deficiency in available resources can be identified allowing mitigation strategies to be developed. These will often be skills that are not easily transferable and cannot be “learnt on the job”. In these situations, additional team members will be required to integrate into the team.

Please note that the themes presented in Figure 3 (a larger version is available in Appendix A) have been identified through the AIR4ICS training events. They are presented as an example rather than a definitive list and it is expected that organisations will identify the themes that best fit their operational procedures.

The best method to create a capability map is through a discussion forum involving all Team Members as this allows group consensus of each element to be achieved. However, it is recognised that there may not be time at the beginning of an incident to spend time creating a capability map. For semi-permanent teams it is recommended that this takes place in the pre-incident planning phases. Any personnel changes can then be reflected in the existing map. For completely new teams if it is not possible to allocate the time/effort for a discussion forum then a questionnaire such as Appendix B can be used as a starting point by the Incident Owner.

5. AIR4ICS Methodologies

5.1. The Sprint

The Sprint is a time-boxed iteration during which prescribed Scrum events take place as detailed in Figure 4. Each sprint should last no more than one fifth of the allotted time for the investigation or one month (whichever is smaller) and each sprint begins immediately after the previous sprint.

Sprints consist of:

- Sprint Planning
- Daily Scrums
- Workstreams
- Sprint Review
- Sprint Retrospective

During the Sprint:

- No changes are made that would endanger the Sprint Goal
- Quality goals do not decrease
- Scope may be clarified and re-negotiated

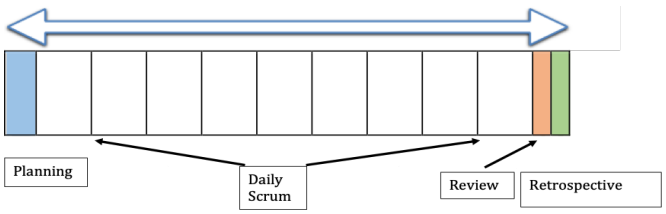

Figure 4 Sprint Lifecycle

Sprints are cyclical processes which start with the Incident Backlog which is then dissected to create a Sprint Backlog. This is then used as the input to the Daily Scrums until the end of the Sprint when reviews and reflection takes place, any lessons learnt are then fed forwards to create actions in the next Sprint (Figure 5).

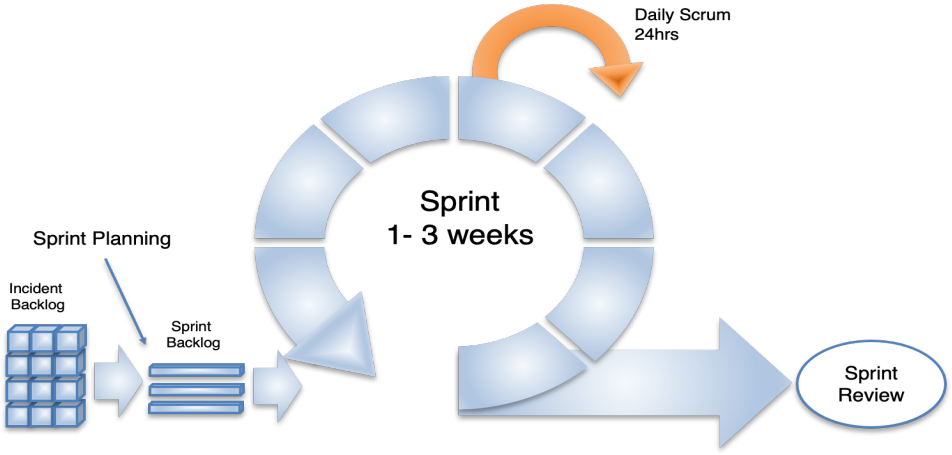

Figure 5 SCRUM process

5.1.1. Sprint Planning Meeting

Bring together relevant stakeholders and team members to efficiently and effectively define the work to be performed in the current iteration. Limited to 5% of total Sprint time.

The meeting has two objectives:

1. What can be delivered in the update resulting from the upcoming Sprint?

2. How will the work needed to deliver the Increment be achieved?

Incident Backlog Items to be worked on during the sprint will be identified creating a Sprint Backlog, with Team Members assuming ownership of tasks.
It is the responsibility of the Incident Owner to decide upon the Items to be worked on during the forthcoming sprint. This decision should be informed by discussions with the Team and using tools such as Risk Poker to identify the current threat status and plan remedial actions accordingly, creating a Sprint Goal that should realistically be achievable. Once chosen for the Sprint Items should be self-selected by Team Members. Where items are not claimed by any Team member the Incident Owner will be responsible for assigning the items to appropriate Team Members.
Particular focus of the meeting will be on providing a strategic overview of the entire response and identifying any foreseen roadblocks for the sprint. It is important to ensure that all Team Members understand the priority of their tasks and the Sprint goal by the end of the meeting.

5.1.2.(Daily) Scrum Meeting

A 15-minute time-boxed event for the Development Team to synchronise activities and create a plan until the next Scrum meeting. The optimal frequency for Scrum meetings is highly context dependant, requiring a balance between updating the team's knowledge and interrupting work mid-task. It is recommended that Scrums take place either once or twice daily with the Scrum master deciding on the most appropriate cadence. As Agile encourages adaptability and responding to the situation, meetings can take place more regularly during times where the incident is changing rapidly.

The meeting centres around Three questions:
- What did I do yesterday?
- What will I do today?
- Do I see any impediment?

The purpose of the meeting is to inspect progress toward the Sprint Goal. The meeting is attended by all members of the Incident Team with the Scrum Master acting as meeting facilitator. All team members should have the opportunity to present an update on their progress. These updates should be short summaries and not technical discussions, where more in-depth information is required a Spin-off Technical Discussion Meeting should be arranged. Progress reports should not include slides or a presentation but should reference the Incident Board.
Where available new Threat Intelligence will be presented to ensure all Team Members are aware of relevant information.

Updating the Incident Board
The Incident Board should be updated dynamically as issues arise. However, Team Members inexperienced with the tool can become focussed on completing their tasks/investigating new information and therefore delay updating the Board. The SCRUM meeting provides a natural break point to ensure that all Items have been placed into the correct phase on the Board.
The Incident Owner can also use the opportunity to alter the tasks in the Sprint Backlog. Depending upon the findings of the investigation this may mean adding or removing Items to be completed in this Sprint. Any chances should not reduce the quality of the Sprint Goal.

Inexperienced Teams Overunning SCRUMs
The purpose of the Daily Scrum meeting is to highlight which tasks are being worked upon/have been completed. They are not intended to be a technical discussion. If your team is new to the Agile approach or the Scrum meetings often overrun their 15-minute timeslot then it is recommended that if during the meeting a task is taking longer than 3 minutes to discuss that the Scrum Master recommend a Technical Discussion Meeting instead. These Technical Discussion Meetings will commence after the end of

the Scrum meeting and should include all relevant Team Members (including the Incident Owner and Scrum Master).

5.1.3. Sprint Review

The Sprint Review is an opportunity to inspect the progress made during the current Sprint and adapt the Incident Backlog if necessary. The meeting should be time-boxed, lasting no more than 5% of the time of the sprint (e.g. a 1 month Sprint would have a 8-hour review) and allows for a more in-depth understanding of what has happened during the sprint. The outcomes of the meeting will include:

- Identification of what went well and best practice to carry forward into subsequent Sprints.
- Identification of any blockages to the investigation and potential mitigation strategies.
- Strategic information required for the subsequent Sprint planning session.

It is important that representation from across the business is present at the Sprint Review meeting if they are not already integrated into the team. This will enable a much greater understanding of the progress made to date and provide a more holistic organisational response.

A typical review will include:

- The Incident Owner explains which Incident Backlog items have been "Done" and what has not been "Done"
- The Incident Team discusses what went well during the Sprint, what problems it ran into, and how those problems were solved;
- The Incident Team highlights the work that it has "Done"
- and answers questions about the progress;
- The Incident Owner discusses the Incident Backlog as it stands. Projects likely completion dates based on progress to date
- The entire group collaborates on what to do next, (input to subsequent Sprint Planning)
- Review of how the landscape or potential impact of the incident might have changed, based upon current risk assessments

A key part of the review is the retrospective element looking at the human factors of the response. To that end all participants provide input to a Learning Matrix to help identify lessons that can be learnt and taken forward for both the next and future Sprints.

Human Factors Objectives:

- Inspect how the previous Sprint went with regards to people, relationships, process, and tools;
- Identify and order the major items that went well and potential improvements; and,
- Create a plan for implementing improvements to the Scrum team operational processes.

5.1.4. Learning Matrix

The Learning Matrix is a tool to aid teams in reflecting upon how the previous sprint went. All team members participate by spending five minutes to "Brainstorm" items for the learning matrix, recording each idea on separate post-it notes. The following quadrants should considered:

1. Things you liked
2. Things you disliked
3. Appreciations
4. Ideas

A suitable area (such as a flip chart) should be separated into the four Quadrants (Figure 6) and the post it notes placed in the appropriate area. It is then the responsibility of the SCRUM Master to group all of the similar items together to identify consistent themes by looking for connections between items. Once the thematic analysis has been completed all team members use sticky dots to vote by placing dots on those post-its they feel most strongly about. Each team member should be given between 5 and 10 sticky dots for the voting, although it is important to ensure that all team members receive the same number of dots.

After the voting has been completed the team then discuss those themes identified as the most important and produce actionable items for the next sprint.

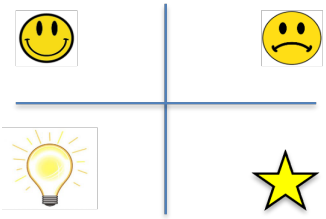

Figure 6 Learning Matrix Quad Chart

5.1.5. Technical Discussion Meetings (TDMs)

Any team member can initiate a TDM when they feel that they have identified a significant event or events representing a change in the overall understanding of the incident. The first TDM must include the Incident Owner and SCRUM master and at least one team member. These meetings are technically focused and more in-depth than SCRUM meetings, allowing key points to be identified and addressed by the group more effectively. From a strategic perspective the Incident Owner and SCRUM master are better able to identify when key findings have been identified in a timely manner, allowing the Incident Backlog to be updated accordingly. Where two or more TDMs are occurring the Incident Owner and SCRUM master split membership accordingly.

5.2. Scrum Artefacts

5.2.1. Incident Backlog (IB)

The Incident Backlog is an ordered list of every task needed for the engagement including all aspects of identify, protect, detect, respond and recover. It provides the single source of requirements, any changes required must be reflected in the IB.
The Incident Owner is responsible for the Incident Backlog's

- content
- availability
- ordering

The IB is never complete and exists as long as the investigation is live and provides through-Life Management (Cradle-to-Grave). Initially, the only known and best-understood requirements are included, as the situation progresses these initial items will be expanded and new items created as and when necessary.

5.2.2. Incident Backlog Items (IBI)

Incident Backlog items should facilitate the prioritisation of tasks during the incident. To ensure that the backlog can be managed effectively each item should be DEEP:

- Detailed appropriately
- Evolving over time
- Estimated Effort (Optional)
- Prioritised

Detailed Appropriately:
To ensure the smooth flow of information in high pressured situations each IBI is required to include the "3 Ws" as shown below in Figure 7:

Who: Person responsible for the item

What: Description of the item

Which: Implications of this item with respect to other devices and items

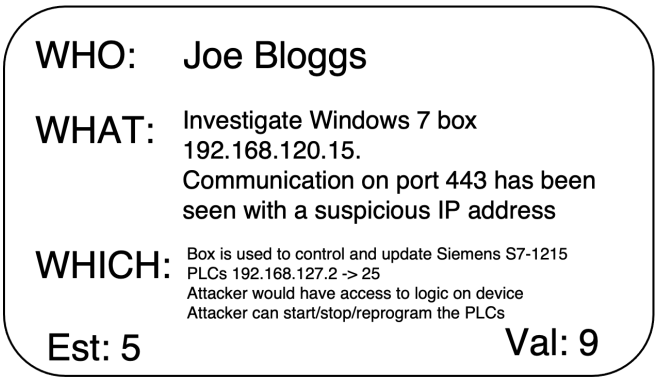

Figure 7 Example Incident Backlog Item

This information allows personnel to quickly and easily ascertain who is responsible for and possesses all relevant information required for that task. By ensuring that the responsible person is identified, when information pertinent to that task is discovered or required the delay in sharing that information is minimised, ensuring informed decisions can be made by the team.
As much information as possible should be included about each task, where space is an issue (e.g. using physical post-it notes) key points should be listed and the named task owner is responsible for ensuring that they have more detailed information available.
Devices do not exist in perfect isolation; issues with a single device can have implications for many others. This may be a direct impact (e.g. a faulty valve may reduce the quantity of an ingredient and therefore the entire batch must be destroyed) or indirect (e.g. the adversary has demonstrated that they have the ability to deployed targeted PLC attacks, therefore all PLCs of

the same type are at greater risk). During an incident the situation can change rapidly and an element of "firefighting" is often seen. When this occurs participants focus on the immediate implications of what is happening, rather than divert resources to investigate potential future avenues of impact. Therefore, all Incident Backlog items will include a list of all other devices that could be impacted by that item (Which). Identifying dependencies/knock on effects will aid the strategic planning process for the group and allow Team Members to make a more informed choice, encouraging more confidence in their own decisions and decreasing their response time.

Evolving over time:
As part of pre-incident planning a baseline set of high-level IBIs will be created. As more information on the network or systems under investigation becomes clearer and malicious activity is identified available these tasks will spawn child tasks, focussed on more specific instances. e.g.
Starting Item: Compare hosts in IDS network traffic with Network Diagram
Child Item: Investigate host not present on network diagram 192.168.170.45
Child Item: Investigate host 192.168.170.22 showing no incoming or outgoing connections
Links to child items should be clearly denoted on the original item card.

Estimated Effort:
This is highly subjective and therefore used as a proxy-indicator for the amount of effort actually required. Some tasks will require more effort than originally envisaged, as the amount of effort required changes the item should be updated accordingly.
If there are issues agreeing an estimation of effort related to time then effort can be estimated relatively. Identify the smallest task and assign that an effort value of 1, each subsequent task is then assessed relative to this point.

Prioritised:
This is an organic document, representing the current risk situation of the incident and so prioritisation of tasks is an ongoing requirement of the Incident Manager. The prioritisation of tasks takes into account factors such as the impact of the task, the likelihood of the relevance, threat intelligence and personal experience. Due to these factors the prioritisation of tasks is envisaged to alter significantly as the incident investigation progresses.
At the end of an incident the IB can be used to provide feedback on team performance and be used to update the starting set of items included within an IB.

5.2.3. Incident Board

The Incident board provides a focal point for the Scrum meetings and is used extensively throughout the process. To allow the easy identification of the current situation as regards to IBIs the task board is split into different phases.
When using a physical Incident Board each IBI should be written on a separate post-it note and then placed in the relevant phase. This is a living document and Team Members should add new IBIs into the To Do section as they arise. The To Do section can be all of the remaining items in the Incident Backlog, however to improve clarity it is often either a subset of the most currently relevant tasks or just the tasks in the current Sprint Backlog. To ensure that the Incident Board provides an up-to-date picture of the situation Team Members should update individual Items to the appropriate phase as soon as they are progressed.
The Incident Owner and Scrum Master are the principal users of the board, utilising it to maintain situational awareness of the team's progress. If Team Members are unable or unwilling to update the Incident Board it is the responsibility of the Incident Owner and Scrum Master to ensure that all IBIs are located in the correct phase.
The Incident Board is particularly beneficial during fast-paced actions, when the situation is changing rapidly. It allows the team to improve their efficiency by removing the potential bottleneck of identifying new tasks for completion without having to consult a single person (the Incident Owner), who might be otherwise engaged. The Board also provides information on who is responsible for each task, providing a named point of contact if Team Members require information related to a specific task.

Incident boards can be further subdivided into thematic areas (Figure 8), allowing areas of concern to be identified and highlight currently under-represented areas. The use of themes allows a shifting of focus for

the team from the tactical to the strategic, providing a greater situational awareness of the response as a whole.

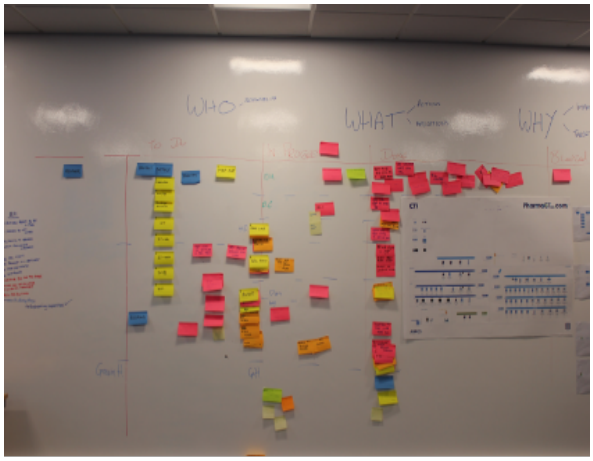

Figure 8 Example Incident Board with themes identified by different coloured post-it notes

Electronic Boards

Due to the often geographically distributed nature of Incident Teams it may not be possible to have a physical Incident Board and instead an Electronic version should be used (Figure 9). The change to an electronic Incident board provides both positives and negatives for the team. Increased information can be provided in the description for each Item in the Incident Backlog as the space available is not limited by the size of the post-it note. Additional resources, such as relevant files, can be linked to specific IBIs to form a widely available knowledge base for the Team. The user interface also provides a more structured appearance with regards to IBI cards compared to the sticky note approach on physical whiteboards, this coupled with search capabilities greatly reduces the time required to find the correct IBI. By providing more information on all aspects of the response Team Members can make more informed decisions, increasing their confidence in those decisions and removing the issue of information silos.

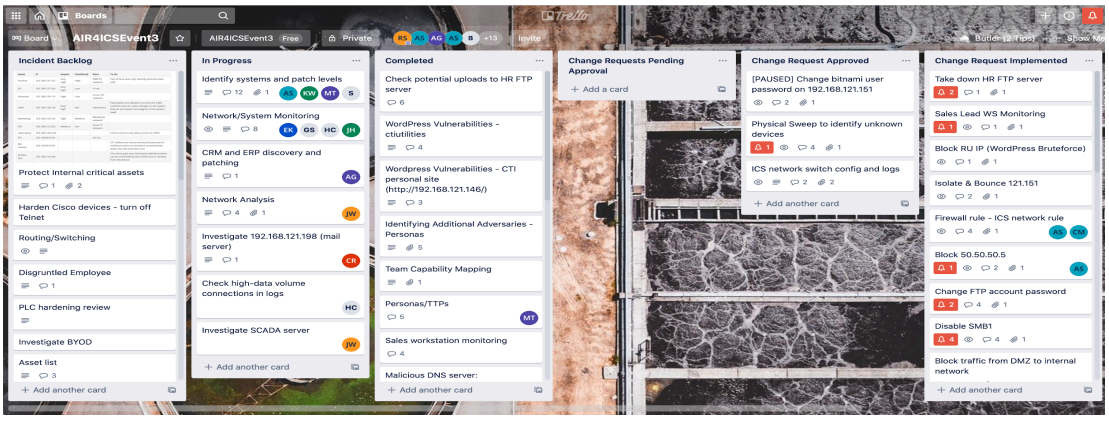

Figure 9 Example Electronic Incident Board

Due to the perceived requirement for increased information content in each IBI Team Members may be less likely to create new Items as they do not feel that they have enough information available. Team Members should be encouraged to create new IBIs even if no other information is available than the title, the Board is designed to constantly evolve and more information can be added as it becomes available. Another potential issue is that Team Members can get into the routine of adding Items to the Backlog just prior to a Sprint meeting, rather than as they arise. This is partly attributed to the lack of a central focal point for the Board, another application window is less prominent than a large whiteboard with people visibly interacting with it. The lack of interaction can also be a potential reason for not adding tasks immediately, as there could be a perception that most Team Members would only be checking on the Board periodically. One potential strategy to combat this is to ask all participants to keep the Incident board window open and visible in the top right-hand corner of their screens at all times. This approach works well for systems with a large viewing area (large or multiple monitors) but is more limited where visible area is limited as participants are more likely to maximise working windows.

5.2.4. Personas

Personas are fictional characters or archetypes that exemplify the way that a typical Threat Actor interacts with a system. It is described as a real person providing estimates for:

- Capabilities
- Objectives
- Motivations
- Commitment
- Resources

Personas add to our understanding of potential threats to the system by estimating the level of sophistication that might be faced and the likely effort required to halt an attack. Human factors play an important part of any incident. A malicious insider might well be more interested in stealing information that could be used to publicly embarrass the company than a professional crime syndicate looking to steal industrial secrets for a competitor. By identifying and incorporating the concept of different agendas the defensive effort can be managed accordingly and more actively targeted.
Where possible Personas can be linked to Threat Intelligence information, in particular indicators of compromise. Threat Intelligence can greatly enrich the information available from the persona, allowing a much more in-depth analysis of the Actor. Utilising the information provided by a persona aids in the strategic management of the incident, if actions can be attributed to a persona likely end targets can be identified, therefore allowing the responders to become more pro-active by focussing their efforts on potential pathways from identified compromised devices to those targets. During the pre-incident planning personas can be used to allow the team to put themselves into the mindset of the attackers and generate Evil User stories.

5.2.5. Evil User Stories

Often used to capture tasks for the IB and identify risks to the system, allowing the Incident Owner to

- Scope
- coordinate
- prioritise

Stories should be kept short and simple to invite explorations of requirements through

- Conversations
- supplementary documentation
- can exist at various levels (Epics, Stories)
- are detailed into tasks during Sprint Planning 2.

A template to generate user stories is provided in Figure 10 an.
The differing aspects of each Threat Actor will determine their actions within the network during the incident. This ranges from which devices they may attack to the methods they will use to achieve their objectives. Addressing the problem from the viewpoint of each Threat Actor yields new stories that are unique requirements related to that actor; Backlog items can then be created from these stories. As part of the process an estimation as to the risk posed to the system is made, aiding the prioritisation of tasks during sprint planning meetings.

ID No.	Title of Story
As a ...	
I want ...	
So that	
I can use ...	
Risk Estimate	

Figure 10 Evil User Template

These stories provide a starting point that can then be expanded upon to derive and enrich Evil Storyboards.

5.2.6. Evil Storyboards

Evil storyboards are similar to attack trees and can be used in the same way to extract Backlog Items. Storyboarding is used in conjunction with other techniques such as Evil user stories, and the baseline backlog to detail visually and textually the key events summing up different interactions of threat actors with the system or business.

- to elicit, elaborate, organise and validate requirements
- to identify what needs to be investigated
- show attack variants

Storyboards are an anchor point for discussion of requirements (Figure 11). The actual requirements live in the conversation and shared understanding developed through additional IBIs.

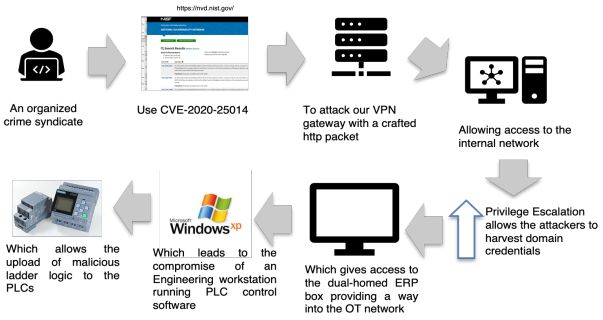

Figure 11 Example Evil Storyboard

5.2.7. Themes

Themes are cross-cutting categorisations that can be used to group tasks together into a context familiar to cyber security professionals. The creation of these themes is up to the individual teams, an example is provided below.

During an attack on a Water Treatment facility Backlog Items were labelled with a combination of the appropriate NIST Framework functions:

- Identify
- Detect
- Protect
- Respond
- Recover

These labels were then assigned a unique colour for visual identification (**Error! Reference source not found.**).

Items belonging to different themes may require different skillsets and efforts. Themes can be used to aid scheduling and progression, the Incident Owner will ensure that some items from each theme are being acted on to ensure progress in all areas, thus reducing planning risk.

5.2.8. Parking Lot Diagrams

Grouping IBIs thematically provides a useful tool for strategic management of the incident. This principle can be taken further by using parking lot diagrams to plot progress within individual themes (**Error! R eference source not found.**). Themes are further sub-divided into smaller thematic areas. All IBIs for a thematic area are consolidated and compared against the number of completed IBIs for that area. This is then combined with the due date to determine a progress rating which when plotted is colour coded for easy visual identification as per Table 1. This provides a visually striking resource for both the Incident Owner and Team Members, allowing them to identify areas where work is not progressing and redeploy resources as necessary.

Table 1 Parking Lot colour schema

Progress	Colour Code
Completed	Green
In progress AND within time limit	Yellow
Overdue OR not yet started	Red

5.2.9. Risk Poker

This takes place during every Sprint Retrospective, allowing the Team to gain an understanding and input into the current risk strategy through the creation of the current critical risk register. The Incident Owner then incorporates the register into their strategic planning and the identification of IBIs for the following sprint.

At least three participants are required to participate in a round of risk poker outlined in the steps below.

1. Every member of the team has a set of poker cards, these are not typical poker cards but follow a sequence (e.g. fibonacci) to allow greater variation on the range of available values (**Error! Reference source not found.**).

2. All participants blindly submit (cards face down if using physical cards) their estimate as to the risk for a specific device or system as relates to the overall incident.

3. After all participants have submitted their bid, the cards are revealed.

4. If there is a consensus then this is noted down and the team move onto the next risk to assess.

5. If there is no consensus, the highest and lowest bidders must explain their reasoning and if no agreement can be reached bidding takes place again.

6. This will continue until a consensus is reached or three rounds have been completed.

7. If there is no consensus the Incident Owner will assign risks and create a ranked critical risk register.

6. AIR4ICS Evaluation Events

A series of three three-day Red vs Blue exercises took place for the analysis and refinement of the AIR4ICS framework. Each event was based around a different ICS scenario chosen to represent different sectors of Critical National Infrastructure, each with unique elements and requirements and used DMU's CYRAN hybrid Cyber Range to provide a realistic cyber sandbox environment. To increase the realism and better represent the pressures faced by an Incident Response Team the scenarios incorporated both physical and virtualised elements. ICS security demonstrators were integrated into the scenarios and collocated with the Blue team to provide additional stimulus when a successful attack occurred. Support for these scenarios was kindly provided in the form of specialised equipment and expertise by Rolls Royce (ship networking equipment) and Airbus (manufacturing line and robotic arm). The chosen scenarios were:

Event 1: Port

Event 2: Pharmaceutical Manufacturing plant

Event 3: Water Treatment Facility

All scenarios incorporated two main elements:

- an Enterprise estate comprising both Windows and Linux boxes representing the standard IT estate of an appropriately sized company
- an Operational Technology estate representing the manufacturing process for a given product.

Both elements contained numerous systems found within a real-world organisations including but not limited to:

- Enterprise Resource Planning
- Human Resource Management
- Customer Relationship Management
- SCADA systems
- OT Historians

To increase the realism of the scenario and ensure that the actions of the Red team were not immediately apparent noise generators producing standard network traffic were included. These noise generators produced traffic including but not limited to:

- https
- DHCP
- DNS
- SFTP
- Version Control
- Modbus
- DNP3
- Profinet

The Blue Team was composed of 62 Incident Response professionals across the events from both the public and private sector. The level of experience within the team varied to better represent that spread of experience within a real-world Incident Team. Teams self-selected AIR4ICS roles and applied the AIR4ICS methodologies whilst defending the network. Participants varied throughout each event due to personnel availability, some attended the whole event, others were only present for parts. This mimics team changes that would take place when dealing with a sophisticated attack taking place over a long timescale in the real world. Training in the AIR4ICS methodology was provided to the Blue team at the beginning of the event, with time provided to allow familiarisation with the network and the creation of the initial Incident Backlog. The Blue team were then responsible for continuously applying the AIR4ICS methodologies, with exact implementations evolving based on feedback during the Sprints.

A selection of defensive tools were provided to the defending Blue team including:

- Intrusion Detection Systems
- Log management Systems

- End-point protection

To protect the network the Blue team were able to implement security measures such as firewall rules, devices hardening, forensic investigation and network segmentation provided a suitable business case, incorporating potential impacts to the business process, was presented.

The Red Team was composed of Red Team professionals from organisations such as Limes Security with experience Penetration Testing Industrial Control Systems. The Red Team actions followed attack lifecycles, such as the Lockheed Martin Cyber Kill Chain (Hutchins 2010), with each stage time constrained to facilitate the analysis the use of AIR4ICS methodologies by the Blue Team. As the attack progresses specific Red Team objectives were introduced with actions that would be identified by the Blue Team, allowing the research team to assess the situational awareness and adaptability of approach provided by AIR4ICS.

Both Red and Blue Teams were provided context specific objectives to complete over the three days of each event. The ultimate goal for the Red Team in each event was to cause a physical impact by acting upon the Operational Technology devices within the network. Observers from the research team were embedded in both Red and Blue teams to monitor team interactions and analyse the evolution of the implementation of AIR4ICS techniques as the team became more familiar with them and tailored their approach. During each Sprint Review meeting participants were provided with a questionnaire designed by Cyber Psychologists to assess the areas of situational awareness and mental load. Finally, an open discussion forum at the end of the event allowed participants to provide specific feedback on their likes/dislikes with the AIR4ICS approach.

6.1. Event Results

Results were collated from both observers reports and participant feedback to refine the AIR4ICS methodologies. Only those elements that proved a tangible benefit to the teamworking and effectiveness of response were included.

Regular SCRUM meetings were identified a providing the greatest impact on team communication and overall situational awareness, allowing Team Members to understand what was happening and facilitating the dynamic shift of tasks when new information was obtained.

The Incident Board provided an invaluable tool for both the management and implementation of the response. As participants became more familiar with the tools the use of the board became more efficient, with participants updating more frequently and increasing the amount of relevant information provided for each task. It should be noted that IBI that contained the “3 Ws” were considered significantly more useful than those containing just a description of the item.

The majority of the effort for Capability Maps, Personas, Evil User stories and storyboards came at the beginning of the events, with each element being updated as new information arises. As the exercise progressed these tools were deemed valuable for providing areas of investigation and possible explanations for behaviour that had been identified. This allowed participants to identify potential pathways to end targets and either stop or considerably slow the attackers.

Sprint review meetings were seen as useful periods of reflection with the whole team assessing the current situation, identifying any issues and how to how to ensure that they did not occur again. It is important that these sessions are also used to highlight the positives from the previous Sprint, this not only increased team morale but provided useful advice for less experienced Team Members.

Participants felt that by including as many people as possible in risk poker a more robust representation of the current risk landscape was produced. It was also appreciated that there was a limit to the number of iterations for any single risk as this removed the possibility of meetings overrunning due to an inability to form a consensus.

Throughout each event questionnaires were completed by each participant as part of every sprint retrospective and more frequently where possible. These questionnaires were designed to assess the mental load, trust and situational awareness of each participant. The key findings are summarised below:

a. The study’s earlier findings (interviews with practitioners) have been supported by the initial findings from the questionnaire designed by the research team looking at the current practises and challenges in IR for industrial control systems.

b. Decision making style: there was an increased thoroughness, control, hesitancy, idealism after agile training and practise.

c. Team decision making: an increase in the scores after agile training and practise.

d. Positive and negative affect: there was an increase of positive after the training.

e. Team interpersonal trust: There was an increase of propensity to trust, perceived trustworthiness, cooperative behaviours and a decrease in monitoring behaviours.

7. Conclusions

The Agile Incident Response for Industrial Control Systems (AIR4ICS) framework has been developed as a modular framework integrating Agile techniques into the Cyber Security domain of incident response. AIR4ICS provides a dynamic approach to improve situational awareness, information sharing, collective decision-making and response flexibility within the unique context of ICS. The techniques used in AIR4ICS were initially shaped by interviews with professionals with experience of protecting ICS, structured using the Scrum methodology, and refined through a series of Cyber Incident Response exercises with Incident Response professionals facing-off against specialist ICS Red Teams.

AIR4ICS ensures that relevant information is available in a clear and concise manner, providing resources and techniques to attribute and present information to the whole group. By ensuring that all team members have a greater understanding of the overall response strategy they are better able to make informed decisions in their own work.

Through regular, short stand-up meetings the team members are encouraged to discuss their work in informal settings, reducing the possibility of information silos developing and increases the buy-in to the overall strategy as team members and stakeholders contribute to the response strategy. As a result, incident response teams are better able to identify and adapt to new information that may alter the current approach as it arises, allowing resources to be rapidly redeployed to mee changing circumstances.

The tools and methodologies presented by the framework have been analysed and refined through a series of three cyber incident response exercises simulating real-world environments. Participants implemented the techniques and provided feedback regarding their applicability within Incident Response Teams. The techniques were then adapted based upon this feedback to create tailored approaches suitable for use within the Cyber domain.

The modular design of the framework means that it can be adapted to fit the working practices, skillsets and priorities of individual organisations. The framework improves communication, promotes information sharing between knowledge areas, and increases external buy-in, Ultimately, AIR4ICS provides a dynamic decision framework that allows Incident Response Teams to manage uncertainty and unpredictability to reduce the time taken to restore normal operations.

Acknowledgements: The authors wish to thank the Research Institute for Trustworthy Inter-Connected Systems (RITICS) for funding this project.

8. References

- Cook, A., Janicke, H., Maglaras, L., Smith, R., 2017. An assessment of the application of IT security mechanisms to industrial control systems. *International Journal of Internet Technology and Secured Transactions*, 7(2), p.144.

- Cook, A. et al., 2018. Managing incident response in the industrial internet of things. *International Journal of Internet Technology and Secured Transactions*, 8(2), p.251.

- Cook, A., Smith, R., et al., 2016a. Measuring the Risk of Cyber Attack in Industrial Control

Systems. Available at: http://dx.doi.org/10.14236/ewic/ics2016.12.

- Cook, A., Janicke, H., Smith, R., et al., 2017. The industrial control system cyber defence triage process. *Computers & Security*, 70, pp.467–481. (*)
- Department of Department of Homeland Security, 2014. *Control Systems Cyber Security: Defense in Depth Strategies*, CreateSpace.
- Cornelius, E., and Fabro, M.. 2008, *Recommended Practice: Creating Cyber Forensics Plans for Control Systems*. United States: N. p., 2008. Web. doi:10.2172/944209.
- Schultz, E. & Shumway, R., 2001. *Incident Response: A Strategic Guide to Handling System and Network Security Breaches*, New Riders.
- Larkin, R.D. et al., 2014. Evaluation of security solutions in the SCADA environment. *ACM SIGMIS Database*, 45(1), pp.38–53.
- Maglaras, L.A. et al., 2017. A security architectural pattern for risk management of industry control systems within critical national infrastructure. *International Journal of Critical Infrastructures*, 13(2/3), p.113. (*)
- Maglaras, L.A. et al., 2018. Cyber security of critical infrastructures. *ICT Express*, 4(1), pp.42–45. (*)
- Nicholson, A. et al., 2012. SCADA security in the light of Cyber-Warfare. *Computers & Security*, 31(4), pp.418–436. (*)
- Nikishin, A., 2015. ICS Threats. A Kaspersky Lab view, predictions and reality. In *Cyber Security for Industrial Control Systems*. Available at: http://dx.doi.org/10.1049/ic.2015.0003.
- Royce. W., 1970, Managing the development of large software systems: Concepts and techniques. In: Proc. IEEE WESCOM. IEEE Computer Society Press, Los Alamitos (1970)
- Whittaker, B., 1999, What went wrong? Unsuccessful information technology projects, Information Management & Computer Security, Vol. 7 No. 1, pp. 23-30. https://doi.org/10.1108/09685229910255160
- The Agile Manifesto weblink https://agilemanifesto.org/ last accessed 15th December 2020
- M. Lindvall et al., "Agile software development in large organizations," in *Computer*, vol. 37, no. 12, pp. 26-34, doi: 10.1109/MC.2004.231, 2004
- https://techbeacon.com/app-dev-testing/survey-agile-new-norm last accessed 15th December 2020
- Braun, V., & Clarke, V., 2006, Using thematic analysis in psychology, Qualitative Research in Psychology, 3:2, 77-101, doi: 10.1191/1478088706qp063oa
- Naedele, M., 2007, Addressing it security for critical control systems, 40th Annual Hawaii International Conference on System Sciences (HICSS'07), pages 115–115. IEEE, 2007.
- Pauna, A. et al., 2013, Can We Learn from SCADA Security Incidents. White Paper, European Union Agency for Network and Information Security, Heraklion, Crete, Greece
- Hutchins, E., Cloppert, M., Amin, R., 2010, Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains, Proceedings 6th International Conference Information Warfare and Security (ICIW 11), pp. 113–125