

# Forensic-by-Design Framework for Cyber-Physical Cloud Systems

**Nurul Hidayah Ab Rahman**, University of South Australia  
**William Bradley Glisson**, University of South Alabama  
**Yanjiang Yang**, Huawei Singapore Research Centre  
**Kim-Kwang Raymond Choo**, University of South Australia

*A forensic-by-design framework allows the integration of forensics tools into the development of a cyber-physical cloud system that can help organizations recover from a cyber-physical attack.*

**T**he continued amalgamation of cloud technology into all aspects of our daily lives creates business opportunities, operational risks, and investigative challenges. But as businesses continue to offer customers and employees increased access, improved software functionality, and new supply chain management opportunities, the risk of cyber-physical attacks on cyber-physical cloud systems (CPCSs) grows. Increasing digital interconnectivity between devices at the physical (such as sensors and actuators) and cyber (such as intelligent decision systems) levels has transformed cyber-physical systems (such as the electric power grid) into large ecosystems requiring a scalable and flexible infrastructure.

Integrating cyber-physical systems into a cloud computing infrastructure forms a CPCS that not

only, potentially, improves interaction between cyber-physical devices but also enables large-scale data storage and analysis.<sup>1</sup> News organizations increasingly highlight the risks of integrating these technologies. For example, a recent article reported on a Polish airline that was grounded when hackers accessed the system handling flight plans ([www.wired.com/2015/06/airlines-security-hole-grounded-polish-planes](http://www.wired.com/2015/06/airlines-security-hole-grounded-polish-planes)); another reported a cyber-physical attack that damaged a blast furnace in a German steel mill ([www.wired.com/2015/01/german-steel-mill-hack-destruction](http://www.wired.com/2015/01/german-steel-mill-hack-destruction)). A high-profile example of an attack on a cyber-physical system is the Stuxnet virus that targeted Iran's nuclear power plant, resulting in the system's malfunction.<sup>2</sup>

In reality, moving from an internal cyber-physical network to the cloud can lead to various security issues. There are only a few known cyberattack in-

cidents on cyber-physical systems, but a successful attack can have real-world and catastrophic consequences. A recent survey suggested that the role of digital forensics in CPCS incident handling isn't widely understood.<sup>3</sup> Although existing digital forensics tools and techniques are unlikely to stop an attack in real time, a forensic-by-design approach can help in several ways. For example, it can help identify an incident by its source and determine its type, preserve and analyze critical evidential data, reconstruct fragments of evidential data and draw conclusions, and accelerate information asset restoration.

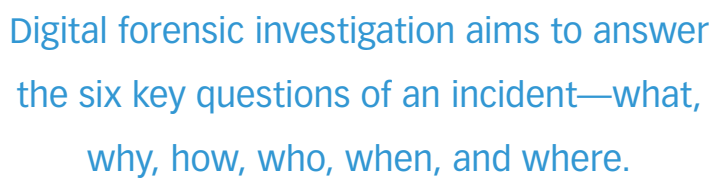
### Security Breach: A Matter of “When,” Not “If”

As technology dependency and cloud integration continue to escalate, ensuring CPCS security becomes a critical factor in delivering trustworthy and robust services. The nature of cyber-physical and cloud computing infrastructures, however, presents inherent challenges to ensuring data confidentiality, integrity, and availability.

In a cyber-physical system, for example, sensitive data from sensors in the physical environment will likely need to travel through different networks to user devices, and the communication path, if unsecured, will be vulnerable or exposed. An attacker could also use cyber-physical components (such as a remote terminal unit) as an attack vector to undertake network attacks (such as timing, data integrity, or replay attacks) against the connected cyber-physical infrastructure. Such attacks could result in power system blackouts, damaged user devices, and smart grid infrastructure failures. They could also result in leaked user data, which infringes on individual privacy. Expanding the preliminary research concept, demonstrated by George Grispos and his colleagues,<sup>4</sup> that “residual artefacts generated by cloud-based synchronized applications can be used to identify broad user behaviour patterns” to interconnected transportation systems creates opportunities for profiling, theft, and physical attack. An attacker could realistically use the interconnected transportation system's data to profile daily life activities (such as identifying specific locations, common travel times, and most visited places), making the abuse of this data itself very risky. Couple this information with mobile devices, cloud storage data, social website interactions, and data from favorite restaurants, fuel stations, and stores, and the profile becomes a detailed roadmap for a host of illegal activities.

An attacker could also exploit vulnerabilities in the cloud infrastructure to launch an attack against a CPCS. Vulnerabilities and threats in cloud computing, which have been widely discussed in the literature, can be broadly classified into two primary types: generic security threats, such as man-in-the-middle attacks and malware, and cloud-specific security threats, such as attacks exploiting vulnerabilities in cloud software or hardware.

In addition, different cloud architectures might have different vulnerabilities that could be exploited. For example, service injection attacks typically affect platform-as-a-service (PaaS) cloud services, and hypervisor attacks affect infrastructure-as-a-service (IaaS) cloud services. Therefore, as explained elsewhere, “[t]here will most certainly be variation in the way criminal investigation is carried out in each



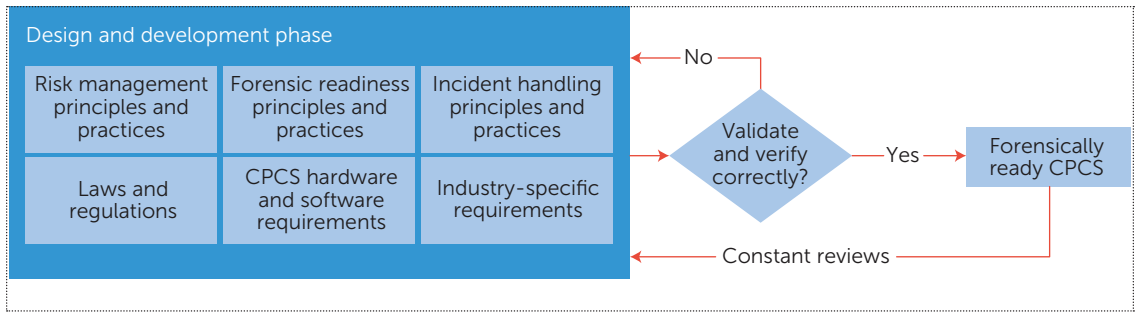
Digital forensic investigation aims to answer the six key questions of an incident—what, why, how, who, when, and where.

type of cloud platform and deployment model,”<sup>5</sup> and potential evidence could be present in places such as the system infrastructure (for example, network logs or camera footage) and user applications (for example, cached or accessed files).

Microsoft suggests an “assume breach” approach for cloud security—an innovative approach to design, engineering, and operations that assumes an attack has already happened.<sup>6</sup> Securing the perimeter like a castle is no longer adequate because of cyberspace's asymmetric nature. To secure an information asset, for example, a cyberdefender would have to ensure that various security technologies are in place, all systems are patched in a timely manner, and so on. However, a cyberattacker only needs to successfully locate and exploit one or more vulnerabilities to carry out an attack.

### Why We Need Forensic by Design

In a security incident, attribution plays a key role in the investigation, such as in tracing and identifying the attack source. This could be facilitated by a digital forensic investigation that aims to answer the six key questions—what, why, how, who, when, and where—of an incident occurrence. Researchers have highlighted potential issues in conducting digital



**FIGURE 1.** Conceptual forensic-by-design framework for a cyber-physical cloud system (CPCS), which ensures that a CPCS (and any other IT system) is designed to facilitate forensic investigations. The framework consists of six factors: risk management principles and practices, forensic readiness principles and practices, incident-handling principles and practices, laws and regulations, CPCS hardware and software requirements, and industry-specific requirements.

forensic investigations in cloud environments, such as the appropriateness of existing data capture methods, tools, multiple evidence sources, and jurisdiction issues. Cloud-specific forensic challenges (for example, multilocation and multiversions of datasets), along with specific cyber-physical system data capture and extraction issues, can complicate these issues. Furthermore, digital forensic investigations typically occur after the event (that is, they’re triggered by a detected security incident); however, systems generally aren’t designed to be digital forensic friendly (or forensic ready). Therefore, collecting critical evidential data might not be practical or even possible.

Further complicating CPCS investigations is the fact that, in many cases, shutting down a cyber-physical system (for example, a power grid, 911 call center, water treatment plant, or hospital network) to conduct forensic investigations isn’t a viable option. Therefore, a digital forensic investigation involving a CPCS requires a different strategy. In this situation, proactive forensic data collection would help reduce the complexity of a forensic investigation and minimize investigation time. A recent study highlighted the need for systems to continuously collect and preserve information prior to a security incident.<sup>7</sup> This work, coupled with recent practitioner insights into security incident response criteria and previous work investigating the integration of security into large-scale application development processes, motivated this article.<sup>8,9</sup> We propose integrating forensic requirements into the CPCS design and development phases (that is, *forensic by design*). Conceptually, forensic by design is similar to security by design, which integrates information security requirements into every relevant phase of software development during the design phase.<sup>10</sup> (See the sidebar for related work in this area.)

### Conceptual Forensic-by-Design Framework

Our conceptual forensic-by-design framework comprises six factors, as Figure 1 illustrates. These six factors, presented as a black box, seek to ensure that a CPCS (and any other IT system) is designed to facilitate forensic investigations.

#### Risk Management Principles and Practices

It would be unrealistic to expect any organization to have infinite resources to identify and act on all potential threats and risks. Therefore, based on the “assumed breach” approach,<sup>6</sup> to achieve CPCS systemic resilience the system developer and forensic expert need to adopt risk management principles and practices to identify and prioritize current and emerging threats (for example, potential vulnerabilities in both cloud computing and cyber-physical systems and how these vulnerabilities can be exploited), risk areas (including risks arising from unexpected and highly unpredictable causes, also known as the “black swan” problem), and potential evidence source and type (see the forensic readiness principles).

#### Forensic Readiness Principles and Practices

Our framework adopts the following activities from the ISO/IEC 27043:2015 processes groups<sup>11</sup> (see the sidebar):

- *Identify potential evidence sources.* The identified evidence sources within the cloud-based cyber-physical system could include a virtual machine snapshot, human–machine interface (HMI) application logs, and events derived from physical system sensors.
- *Plan pre-incident collection.* Strategies for collecting raw evidence data in advance include

using built-in modules on remote telemetry unit (RTU) systems to automatically send event metadata to a forensic database.

- *Define storage and evidence handling.* A centralized and securely configured forensic database can store collected evidential data. Evidence-handling procedures must be documented to adhere to the digital forensic principles and maintain the chain of custody.
- *Plan pre-incident analysis.* The framework should define strategies to detect incidents by analyzing data using suitable tools, such as intrusion detection systems, log monitoring, and security information and event management systems. This activity also involves identifying responsibility boundaries—for instance, a cloud service provider is unlikely to be responsible for the system's physical layer.
- *Plan incident detection.* This activity, typically part of the digital investigation procedure, involves identifying actions to be undertaken after the incident has occurred or has been detected. The forensic responsibility boundary is also a factor here. For example, cloud service users might not need to be involved if a cyberattack occurs at the cloud provider's datacenter.

### Incident-Handling Principles and Practices

Guiding principles and practical strategies can minimize the impact of loss after a security incident and help prevent and mitigate future incidents. As earlier work noted, incident handling and digital forensic practices overlap, and both practices should be integrated into an incident-handling strategy.<sup>3</sup> For example, intrusion detection systems can help determine attack sources. In addition, having a forensic database (for pre-incident collection) would benefit incident responders during a preliminary incident response. In earlier work, Grispos and his colleagues note that organizations have opportunities to strengthen policies, standards, and procedures prior to migrating to cloud environments.<sup>12</sup> Organizations need to investigate these opportunities from a CPCS perspective. Additional work by Grispos and his colleagues in the area of security incident response criteria demonstrate the type of industry practices that need to be identified and verified for CPCS incident handling.<sup>9</sup> However, we need to ensure that activities undertaken during incident handling (for example, evidence collection) don't result in service disruption, and therefore system backup and redundancy must be carefully planned in incident handling.

### Laws and Regulations

When designing forensic strategies, it's important to consider international and local legal and regulatory requirements, because different national laws and regulations might have different evidence requirements. A law designated for data protection might only be applicable to the country in which the data resides, for example. In some scenarios, cloud providers might be required to comply with a court order and surrender user data without notifying the data owner. Relevant standards and industry best practices should also be considered in the design and development phases. The Payment Card Industry-Data Security Standard (PCI-DSS), for instance, mandates regular monitoring of access to network resources, which would require the system to include an efficient logging capability for compliance purposes as well as the digital evidence source.

### CPCS Hardware and Software Requirements

The interdependencies between hardware and software within a CPCS complicate the identification and collection of evidential data. Potential evidence artefacts would exist across several CPCS layers (for example, from field devices to cloud aggregators); thus, providing an embedded forensic agent is a potential solution to remotely collecting the evidential data. Furthermore, specific communication protocols used in cyber-physical systems, such as ModBUS, to control field devices would require a customized forensic approach as compared to the common network protocol (for example, TCP/IP). Understanding hardware and software requirements are, therefore, critical in supporting the collection of forensically sound evidence.

### Industry-Specific Requirements

Because of the diversity of cyber-physical components (for example, sensor, controller, and networked systems) and data types (for example, sensor data from in-vehicle systems are quite different from sensor data from power grid systems), we must also consider industry-specific (for example, energy, automotive, and transportation) requirements. Therefore, identifying and collecting evidence data sources requires careful planning. Moreover, each industry has a different security risk profile, which would affect the choice of forensic strategies.

### Validation and Verification

Once a prototype of the system has been designed and developed, it's important to validate and verify to ensure that the evidence collected is adequate and reliable, and that the forensic processes and

## RELATED WORK IN DIGITAL FORENSICS

Digital forensic readiness and system security engineering are both closely related to forensic by design.

### Digital Forensic Readiness

Digital forensic readiness (DFR) refers to planning digital forensic strategies (for example, what evidence is required) before an incident occurs to facilitate a cost-effective and efficient investigation,<sup>1</sup> and to achieve corporate security hygiene. To implement DFR in an organization, system designers need to incorporate a range of operational and infrastructural readiness strategies, such as risk assessment, staff training, tool deployment, and evaluation metrics.

George Grispos and his colleagues used semistructured interviews to investigate incident response procedures and practices in a Fortune 500 organization.<sup>2</sup> The results of their case study, integrated with industry survey findings and relevant literature, identified six incident response criteria that are relevant to security incidents. The criteria that directly impact digital forensic readiness are “access to security data” and “protecting digital evidence.” Having appropriate access to data is critical to any security investigation and can, realistically, be problematic within large organizations as well as across organizational situations. The protection of digital evidence criteria highlights the need to “ensure the timely identification and preservation of all digital evidence which could be used in subsequent legal cases or internal hearings.”<sup>3</sup> The criteria identified in the study that indirectly impact digital forensic readiness are “incident learning through the incident lifecycle” and “short investigation lifecycles.” These criteria focus on identifying root causes and disseminating lessons learned from previous incidents along with minimizing asset downtime.

Cornelia Petronella Grobler and her colleagues proposed a theoretical framework that comprises dimensions such as legal and judiciary matters, governance, policy, process, people, and technology to provide organizations with a state of readiness.<sup>4</sup> Similarly, Mohamed Elyas and his colleagues proposed a framework comprising forensic factors, forensic readiness capabilities, and forensic strategy,<sup>5</sup> which they subsequently refined to include two major components<sup>6</sup>:

- forensic readiness capability, whose subcomponents include organizational factors and forensic strategy; and
- forensic readiness objectives, whose subcomponents include regulatory compliance, legal evidence management, forensic response, and business objectives.

Kamil Reddy and Hein Venter presented a DFR management system with three key modules: event analysis capability, DFR information (for example, policies, procedures, and training requirements), and costing (for example, staff cost, infrastructure, and training).<sup>7</sup> Aleksandar Valjarevic and Hein Venter proposed a harmonized process model for digital forensic investigation readiness,<sup>8</sup> which was subsequently incorporated into ISO/IEC 27043:2015 ([www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=44407](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44407)).

The ISO/IEC 27043:2015 states that a DFR strategy encompasses three processes groups:

- *Planning* includes defining scenarios, storage and evidence handling, and system architecture; identifying potential evidence sources; and planning pre-incident collection, pre-incident analysis, and incident detection.
- *Implementation* involves the implementation of the system architecture; pre-incident collection, storage, and handling; pre-incident analysis; and incident detection.
- *Assessment* involves evaluation of the implementation processes and the subsequent results.

Several researchers have investigated DFR's use in IT systems, including cloud systems. For example, applying information retrieval techniques to file system forensics, Clay Shields and his colleagues presented a prototype that proactively collects evidence data based on digital signatures that contain a digital object's information event that was created, edited, or deleted on an organization's network.<sup>9</sup> The events are then stored on a centralized database. Brian Cusack and Ar Kar Kyaw applied drones to track, trap, and forward packets to the forensic server to enable DFR in wireless infrastructure.<sup>10</sup> They then mapped events onto defined behaviors in the forensic server.



Philip Trenwith and Hein Venter outlined several requirements for implementing a DFR strategy in cloud systems, such as the need for a secure communication channel for data transfer between client and server (that is, using encryption), compression of backup log files, authentication of log data and proof of integrity, and client and server authentication.<sup>11</sup> Using a risk analysis approach, Mpho Percy Makutsoane and Awie Leonard incorporated DFR as a criteria for evaluating a cloud service provider's ability to manage cyberbreaches, as well as to increase users' trust.<sup>12</sup> As with introducing security into existing systems, retrofitting an existing cloud system architecture with a DFR strategy could be difficult and costly.

### System Security Engineering

System security engineering draws on systems engineering, software security engineering, and risk management to identify threats and vulnerabilities and minimize the associated risks.<sup>13</sup> Logan Mailloux and his colleagues outlined five phases of system security engineering: developing system security criteria, analyzing and validating the system security baseline, designing and integrating the security system, implementing the security system design, and continually addressing operational support security concerns. Such an approach allows organizations to determine and incorporate security budget expenditures into the product's cost while avoiding compatibility issues should security features be introduced into an existing system.<sup>14,15</sup>

In other words, software security engineering (also referred to as security by design) incorporates security requirements into the software development lifecycle.<sup>14</sup> In their systematic review, Daniel Mellado and his colleagues show that security requirements are often studied in requirements modelling (for example, SecureUML and misuse cases), model development (for example, threat modeling, risk-based, and ontologies), and standards integration.<sup>16</sup>

Several conceptual security-by-design frameworks have been proposed in the literature,<sup>14,17</sup> and by organizations such as the National Institute of Standards and Technology<sup>18</sup> and IBM.<sup>19</sup> In 2014, the European Network and Information Security Agency (ENISA) suggested using a security-by-design approach to ensure user privacy and data protection.<sup>20</sup> An example of a real-world application is Citrix's

desktop virtualization, which is built on a secure architecture.<sup>21</sup> Himanshu Khurana and his colleagues presented an architecture-based requirements for smart grids by focusing on authentication and encryption.<sup>22</sup>

### References

1. R. Rowlingson, "A Ten Step Process for Forensic Readiness," *Int'l J. Digital Evidence*, vol. 2, no. 3, 2004, pp. 1–28.
2. G. Grispos, W.B. Glisson, and T. Storer, "Cloud Security Challenges: Investigating Policies, Standards and Guidelines in a Fortune 500 Organization," *Proc. 21st European Conf. Information Systems (ECIS)*, 2013.
3. G. Grispos, W.B. Glisson, and T. Storer, "Security Incident Response Criteria: A Practitioner's Perspective," *Proc. 21st Americas Conf. Information Systems (AMCIS)*, 2015, in press.
4. C.P. Grobler, C.P. Louwrens, and S.H. von Solms, "A Framework to Guide the Implementation of Proactive Digital Forensics in Organisations," *Proc. Int'l Conf. Availability, Reliability and Security*, 2010, pp. 677–682.
5. M. Elyas et al., "Towards A Systematic Framework for Digital Forensic Readiness," *J. Computer Information Systems*, vol. 54, no. 3, 2014, pp. 97–106.
6. M. Elyas et al., "Digital Forensic Readiness: Expert Perspectives on a Theoretical Framework," *Computer Security*, vol. 52, July 2015, pp. 70–89.
7. K. Reddy and H.S. Venter, "The Architecture of a Digital Forensic Readiness Management System," *Computer Security*, vol. 32, Feb. 2013, pp. 73–89.
8. A. Valjarevic and H. Venter, "A Harmonized Process Model for Digital Forensic Investigation Readiness," *Advances in Digital Forensic IX*, G. Peterson and S. Shenoj, eds., Springer, 2013, pp. 67–82.
9. C. Shields, O. Frieder, and M. Maloof, "A System for the Proactive, Continuous, and Efficient Collection of Digital Forensic Evidence," *Digital Investigations*, vol. 8, no. 2011, 2011, pp. 3–13.
10. B. Cusack and A.K. Kyaw, "Forensic Readiness for Wireless Medical Systems," *Proc. Australian Digital Forensics Conf.*, 2012, pp. 21–32.
11. P.M. Trenwith and H.S. Venter, "Digital Forensic Readiness in the Cloud," *Proc. Information Security for South Africa*, 2013, pp. 1–5.
12. M.P. Makutsoane and A. Leonard, "A Conceptual

Cont. on page 56

Cont. from page 55

- Framework to Determine the Digital Forensic Readiness of a Cloud Service Provider," 2014, pp. 3313–3321.
13. L.O. Mailloux et al., "System Security Engineering for Information Systems," *Emerging Trends in ICT Security*, Elsevier, 2014, pp. 3–24.
  14. G. McGraw, "Software Security," *IEEE Security & Privacy*, vol. 2, no. 2, 2004, pp. 80–83.
  15. L. Fitcher and R. von Solms, "Guidelines for Secure Software Development," *Proc. Ann. Research Conf. South African Inst. of Computer Scientists and Information Technologists on IT Research in Developing Countries Riding the Wave of Technology (SAICSIT)*, 2008, pp. 56–65.
  16. D. Mellado et al., "A Systematic Review of Security Requirements Engineering," *Computer Standards and Interfaces*, vol. 32, no. 4, 2010, pp. 153–165.
  17. D.E. Denning, "Toward More Secure Software," *Comm. ACM*, vol. 58, no. 4, 2015, pp. 24–26.
  18. R. Kissel et al., *Security Considerations in the System Development Life Cycle*, tech. report, Nat'l Inst. of Standards and Technology, Gaithersburg, 2008.
  19. D. Allan et al., *Security in Development: The IBM Secure Engineering Framework*, IBM Redbooks, 2010; [www.redbooks.ibm.com/abstracts/redp4641.html](http://www.redbooks.ibm.com/abstracts/redp4641.html).
  20. G. Danezis et al., *Privacy and Data Protection by Design—From Policy to Engineering*, tech. report, EU Agency for Network and Information Security (ENISA), 2014; [www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design](http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design).
  21. *Secure by Design: How XenAPP Dramatically Simplifies Data Protection, Access Control and Other Critical Security Tasks*, white paper, Citrix, 2015; [www.citrix.com/content/dam/citrix/en\\_us/documents/products-solutions/secure-by-design.pdf](http://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/secure-by-design.pdf).
  22. H. Khurana et al., "Smart-Grid Security Issues," *IEEE Security & Privacy*, vol. 8, no. 1, 2010, pp. 81–85.

functions used are sound (for example, there's no contamination of evidence). As Yinghua Guo and his colleagues discuss, "validation refers to the confirmation by examination and the provision of objective evidence that a tool, technique or procedure functions correctly and as intended" and "verification is the confirmation of a validation with laboratories tools, techniques and procedures."<sup>13</sup>

Ensuring reliable evidence data is an important

aspect of producing digital evidence that's admissible in a court of law (that is, forensically sound). We can use Rodney McKemmish's criteria as guidelines to establish forensic soundness<sup>14</sup>:

- *Meaning*. Design digital forensic processes that won't change the data's meaning.
- *Error*. Design digital forensic processes that can avoid undetectable error. If an error is encountered when undertaking forensic processes, it must be identified and explained as evidence.
- *Transparency*. Verify evidence by documenting the chain of custody, including identifying the forensic software and hardware used, detailing the analysis environment, and specifying any problems, errors, and inconsistencies throughout the forensic processes.
- *Experience*. Be sure to task an individual with sufficient and relevant expertise with finding digital evidence.

Assurance refers to the measurement of forensic processes and functions using relevant metrics, such as those involving security incidents, maturity level, and IT performance, and can include incident simulation or testing (for example, penetration testing) as input. The system designer can refine the CPCS based on the validation and verification results before finalizing. As part of the final check, the designer defines a set of actions that constitutes a strategy for incident handling and creates (or updates) digital forensic practices to manage incident occurrence in the product's postrelease phase.

Any problems resulting from the validation and verification will involve refining the related factors. The completed CPCS should be forensically ready in the aforementioned key areas. To sum up, defining and planning what evidence will be required ensures that better security mechanisms and architecture are in place, and that they can provide the evidence when it's required.

## A Hypothetical Case Study

A vehicular ad hoc network (vanet), a key component of an intelligent transportation system, facilitates vehicle-to-vehicle and vehicle-to-infrastructure (V2I) communications. A vanet generally consists of an on-board unit (OBU)—a set of communication units in the vehicles—and a road-side unit (RSU)—a set of infrastructure communication units on roads.<sup>15</sup> Increasingly, vanets are deployed over the cloud to leverage the benefits offered by the cloud environment (for example, increased processing and storage of a larger amount of data on demand).

**Table 1. Designing a vanet using the conceptual forensic-by-design framework.**

Design factors	Possible actions
Risk management principles and practices	An ongoing process to identify, assess, evaluate, and prioritize various security and privacy risks. <sup>15</sup> For example, a GPS spoofing risk might be classified as high priority because such attacks could result in real-world fatalities in a traffic accident.
Forensic readiness principles and practices	Information from risk profiling activities would assist in identifying specific sources of evidential artefacts, such as GPS data, car sensor data, event data, and vehicular cloud data. This is important in the system's planning and design to enable evidence collection.  Appropriate forensic best practices must be identified and implemented according to the deployed environment.
Incident-handling principles and practices	Typical incident-handling phases are prepare, detect, analyze, respond, and evaluate. Integrating a forensic plan into incident handling (such as integrating forensic readiness into the prepare phase) would enable more effective execution. <sup>3</sup>
Laws and regulations	Evidence must be collected in a manner that can be admitted in a court of law.
CPCS hardware and software requirements	Interoperability between CPCS hardware and software maximizes evidence collection efforts—for example, a better understanding of the on-board unit (OBU), road-side unit (RSU), and the underlying operating systems will allow designers to integrate evidence collection capabilities in the system.
Industry-specific requirements	Transportation and related requirements (such as a car's route information storage policy) must be considered in the system's design to maximize evidence collection efforts.

Table 1 outlines the importance of our conceptual framework in the design of such systems.

The same idea could be applied to other practical and relevant scenarios, such as on-board aviation systems that facilitate aircraft operations. A US Government Accountability Office (GAO) report highlights the need for a more comprehensive cybersecurity solution for the Next Generation Air Transportation System (NextGen).<sup>16</sup> The report recommends moving from non-IP-based communications to IP-based communications along with changing from air-gapped systems to non-air-gapped systems. This creates a great opportunity to implement a forensic-by-design framework.

In this framework, risk management needs to identify and quantify risks associated with all the components involved in IP communications on board an airplane, including both hardware, such as routers and network hardware, and software, such as firewalls. Known liabilities and attacks need to be identified and quantified from a plausibility and fatality perspective. Forensic readiness in this case includes identifying potentially relevant residual data produced by the network and by potential attacks.

At this point, appropriate incident-handling procedures need to be defined and integrated into aircraft investigation procedures. Realistically, the examination of a black box might not provide a complete investigative picture. The legal perspective in this scenario is particularly tricky. It shares the root problem haunting cloud computing investigations.

What country, district, or state has priority when investigating an incident on an airplane? Is it the location where the plane lands or where the flight began? Regardless, protocols and procedures for ensuring evidence admissibility need to be developed and integrated into the investigative process to ensure admissibility in the appropriate legal jurisdictions.

As long as the plane isn't in flight, the CPCS isn't an immediate issue. However, integration of digital forensic capabilities into CPCSs on an airplane can be problematic. For example, planes are weight sensitive, so the collection and storage of network data could become an issue. If the data is transmitted to the ground, what protocols are being implemented to ensure that the data hasn't been modified? When it comes to industry-specific requirements, the airline industry is in no short supply. Forensic frameworks will need to be compatible with all relevant Federal Aviation Administration regulations for normal running, redundancy, and investigation requirements.

There will never be sufficient resources to investigate all cybersecurity incidents. As CPCSs become increasingly integrated into critical infrastructures, criminals, terrorists, and actors with malicious intent could potentially exploit vulnerabilities in a particular environment or system (for example, a cloud system). This could lead to rapid escalation and detrimental impact of seemingly modest disruptions within the CPCS.



Arguably, it's important to ensure that when a cybersecurity incident occurs, the collection of evidential data is relevant, timely, and forensically sound enough to be used in subsequent criminal investigations or civil litigations. However, because of the number of field devices and machines that need to be examined, and the lack of forensic readiness in existing systems, it's challenging, and at times impossible, to extract and analyze data in a timely and efficient fashion (for example, evidential data collected from different devices and machines in the CPCS might be in different formats).

Our conceptual forensic-by-design framework for CPCSs would allow systems that are robust in the sense that their legitimate use is minimally constrained, but their illegitimate use is prevented or discouraged (for example, it significantly increases the risk of detection and successful prosecution because it collects evidence from the CPCS in a timely and cost-effective manner).

Future work includes collaborating with real-world system developers and forensic experts to develop the practical aspect (criteria/practice) of the respective factors in the design and development phase, as well as validating and refining the forensic-by-design framework. The long-term goal is to implement the refined forensic-by-design framework in a range of companies and industries to identify and investigate specific industry needs and nuances. In other words, what are the specific needs of organizations in the safety-critical industry as opposed to the financial or education industries from a CPCS forensic-by-design perspective? Do these needs and nuances differ based on international locations?

### Acknowledgments

The views and opinions expressed in this article are ours and not the organizations with whom we are or have been associated. We'd like to thank editor-in-chief Mazin Yousif and the three anonymous reviewers for providing constructive and generous feedback. Despite their invaluable assistance, any errors remaining in this article are solely ours.

### References

1. S. Karnouskos, A.W. Colombo, and T. Bange-mann, "Trends and Challenges for Cloud-Based Industrial Cyber-Physical System," *Industrial Cloud-Based Cyber-Physical Systems*, A.W. Colombo et al., eds. Springer Int'l Publishing, 2014, pp. 231–240.
2. R. Langner, "Dissecting a Cyberwarfare Weapon," *IEEE Security & Privacy*, vol. 9, no. 3, 2011, pp. 49–51.
3. N.H. Ab Rahman and K.-K.R. Choo, "A Survey of Information Security Incident Handling in the Cloud," *Computer Security*, vol. 49, Mar. 2015, pp. 45–69.
4. G. Grispos et al., "Identifying User Behavior from Residual Data in Cloud-based Synchronized Apps," *J. Information Systems Applied Research*, vol. 8, no. 2, 2014, pp. 4–14.
5. B. Martini and K.-K.R. Choo, "An Integrated Conceptual Digital Forensic Framework for Cloud Computing," *Digital Investigation*, vol. 9, no. 2, 2012, pp. 71–80.
6. Microsoft, "Microsoft Enterprise Cloud Red Teaming," 2014; [http://download.microsoft.com/download/C/1/9/C1990DBA-502F-4C2A-848D-392B93D9B9C3/Microsoft\\_Enterprise\\_Cloud\\_Red\\_Teaming.pdf](http://download.microsoft.com/download/C/1/9/C1990DBA-502F-4C2A-848D-392B93D9B9C3/Microsoft_Enterprise_Cloud_Red_Teaming.pdf).
7. M. Elyas et al., "Digital Forensic Readiness: Expert Perspectives on a Theoretical Framework," *Computer Security*, vol. 52, July 2015, pp. 70–89.
8. W.B. Glisson and R. Welland, "Web Engineering Security (WES) Methodology," *Comm. Assoc. Information Systems*, vol. 34, no. 1, 2014, pp. 1359–1396.
9. G. Grispos, W.B. Glisson, and T. Storer, "Security Incident Response Criteria: A Practitioner's Perspective," *Proc. 21st Americas Conf. Information Systems (AMCIS)*, 2015, in press.
10. G. McGraw, "Software Security," *IEEE Security & Privacy*, vol. 2, no. 2, 2004, pp. 80–83.
11. *Information Technology—Security Techniques—Incident Investigation Principles and Processes*, ISO/IEC 27043:2015, Int'l Organization for Standardization (ISO), 2015; [www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=44407](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44407).
12. G. Grispos, W.B. Glisson, and T. Storer, "Cloud Security Challenges: Investigating Policies, Standards and Guidelines in a Fortune 500 Organization," *Proc. 21st European Conf. Information Systems (ECIS)*, 2013.
13. Y. Guo, J. Slay, and J. Beckett, "Validation and Verification of Computer Forensic Software Tools—Searching Function," *Digital Investigations*, vol. 6, 2009, pp. 12–22.
14. R. Mckemmish, "When Is Digital Evidence Forensically Sound?" *Advances in Digital Forensics IV*, I. Ray and S. Shenoi, eds., Springer, 2008, pp. 3–15.
15. M.N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET Security Challenges and Possible Cryptographic Solutions," *Vehicular Comm.*, vol. 1, no. 2, 2014, pp. 53–66.
16. *Air Traffic Control: FAA Needs a More Com-*

*prehensive Approach to Address Cybersecurity as Agency Transitions to NextGen, tech. report GAO15-370, US Government Accountability Office, 2015; [www.gao.gov/products/GAO-15-370](http://www.gao.gov/products/GAO-15-370).*

**NURUL HIDAYAH AB RAHMAN** is a PhD scholar at the University of South Australia, and an academician in the Faculty of Computer Science and Information Technology at the University of Tun Hussein Onn Malaysia. Her research interests include information security management, incident management, and cloud computing security. She has an MSc in information security from the Universiti Teknologi Malaysia. Contact her at [nurul\\_hidayah.ab\\_rahman@mymail.unisa.edu.au](mailto:nurul_hidayah.ab_rahman@mymail.unisa.edu.au).

**WILLIAM BRADLEY GLISSON** is an associate professor at the University of South Alabama. His research interests include digital forensics, information assurance, software engineering, and applied computing science with specific interest in the security, business, and healthcare implications associated with residual data. Glisson has a PhD in computing sci-

*ence from the University of Glasgow. Contact him at [hgllisson@southalabama.edu](mailto:hgllisson@southalabama.edu).*

**YANG YANJIANG** is a senior researcher in information security at the Huawei Singapore Research Centre. His research interests include information security, with specific focus on wireless sensor networks, trusted computing, cloud security, multimedia security, cyber-physical security, and the Internet of Things. Yanjiang has a PhD from the National University of Singapore. Contact him at [yang.yanjiang@huawei.com](mailto:yang.yanjiang@huawei.com).

**KIM-KWANG RAYMOND CHOO** is an associate professor at the University of South Australia and a visiting expert at the Interpol Global Complex for Innovation. His research interests include cybersecurity and digital forensics. Choo has a PhD in information security from Queensland University of Technology, Australia. Contact him at [raymond.choo@fulbrightmail.org](mailto:raymond.choo@fulbrightmail.org).



Selected CS articles and columns are also available for free at <http://ComputingNow.computer.org>.

## ADVERTISER INFORMATION

### Advertising Personnel

Marian Anderson: Sr. Advertising Coordinator  
Email: [manderson@computer.org](mailto:manderson@computer.org)  
Phone: +1 714 816 2139 | Fax: +1 714 821 4010

Sandy Brown: Sr. Business Development Mgr.  
Email: [sbrown@computer.org](mailto:sbrown@computer.org)  
Phone: +1 714 816 2144 | Fax: +1 714 821 4010

### Advertising Sales Representatives (display)

Central, Northwest, Far East:  
Eric Kincaid  
Email: [e.kincaid@computer.org](mailto:e.kincaid@computer.org)  
Phone: +1 214 673 3742  
Fax: +1 888 886 8599

Northeast, Midwest, Europe, Middle East:  
Ann & David Schissler  
Email: [a.schissler@computer.org](mailto:a.schissler@computer.org), [d.schissler@computer.org](mailto:d.schissler@computer.org)  
Phone: +1 508 394 4026  
Fax: +1 508 394 1707

Southwest, California:  
Mike Hughes  
Email: [mikehughes@computer.org](mailto:mikehughes@computer.org)  
Phone: +1 805 529 6790

Southeast:  
Heather Buonadies  
Email: [h.buonadies@computer.org](mailto:h.buonadies@computer.org)  
Phone: +1 973 304 4123  
Fax: +1 973 585 7071

### Advertising Sales Representatives (Classified Line)

Heather Buonadies  
Email: [h.buonadies@computer.org](mailto:h.buonadies@computer.org)  
Phone: +1 973 304 4123  
Fax: +1 973 585 7071

### Advertising Sales Representatives (Jobs Board)

Heather Buonadies  
Email: [h.buonadies@computer.org](mailto:h.buonadies@computer.org)  
Phone: +1 973 304 4123  
Fax: +1 973 585 7071