C. Alcaraz, and J. Lopez, "Analysis of Requirements for Critical Control Systems", *International Journal of Critical Infrastructure Protection (IJCIP)*, vol. 5, pp. 137145, 2012.
http://doi.org/10.1016/j.ijcip.2012.08.003
NICS Lab. Publications: https://www.nics.uma.es/publications

Analysis of Requirements for Critical Control Systems

Cristina Alcaraz, and Javier Lopez

Computer Science Department, University of Malaga,
Campus de Teatinos s/n, 29071, Malaga, Spain
{alcaraz,jlm}@lcc.uma.es

October 27, 2015

Abstract

Technological convergence in control and acquisition tasks in critical control systems has become a cutting-edge topic in recent years. Modernization not only offers a way of increasing operational performance but it also infers greater security issues and associated risks. Although there currently is an important diversity of studies dealing with aspects related to the adaptation of new technologies in the control processes, it is also necessary to formally analyze problems and challenges when such technologies and information systems are being adopted. For this reason, in this paper we formally analyze how the different domains of a control system using new technologies could have an influence on each other, impacting sooner or later on the final performance of the system or critical systems. As a result, five requirements of control have been identified with the objective of proposing a new set of operational requirements that ensure a suitable trade-off between performance and security.

Keywords: Critical Control Systems, Requirements of Control, Critical Infrastructures.

1 Introduction

Industrial Control Systems (ICSs), such as for instance Supervisory Control and Data Acquisition (SCADA) systems, are complex systems with the mission of performing a set of specific control tasks, thus becoming an essential part of an industrial production process. They are considered the main framework for the supervision and monitoring of other Critical Infrastructures (CIs), such as: electric energy systems, nuclear energy systems, water and sewage treatment plants, gas/oil energy systems and transportation systems. In particular, they are able to remotely monitor and supervise engineering devices installed or deployed close to the critical infrastructure, manage automation and operational tasks, and store sensitive information. This type of information can be both data measurements, i.e., physical events related to real conditions of controlled infrastructures, and alarms, i.e., messages that explain the actual situation of the controlled infrastructure using different priority levels.

ICSs are also considered highly-critical systems because of the serious consequences that a failure or a threat could lead to the system or between systems, with a significant impact on business continuity, social well-being and economy [1]. This means that a disruption in the control process or an isolation of those essential parts of the system could hide evidence streams that could explain the actual situation or discard actions that should be performed at a given moment. In our critical control context, a disruption refers to degradation (or stoppage) of the control service that could become unacceptable for the good performance of other infrastructures.

One of the main causes of these security risks is the modernization of the subsystems with the adaptation of current resources, services and new Information and Communication Technologies (ICTs) for the management of sensitive information and control actions from anywhere and at any time. This technological adaptation also means that it is necessary to achieve a suitable balance between performance and security when unexpected faults or threats appear within the system.

For this reason, the main purpose and contribution of this paper is to reassess the control context and its requirements so as to evaluate whether current requirements (either operational or security) are really enough to accommodate current ICTs, or otherwise to identify new requirements. The paper is organized as follows. Section 2 identifies and analyzes those elements, denoted as control areas, that play a significant role in monitoring processes so as to study their dependency relationships and consequences. Based on this, Section 3 analyzes five specific requirements of control so as to locate and discuss in Section 3.6 the most critical and susceptible points to threats or faults. Finally, Section 4 concludes the paper and outlines future work.

2 Control Areas and Security Risks

We consider that four main control areas conform a control system: *delivered services, resources, managed information* and *operational control tasks*. Although all of them present a priori some differences from the functional point of view, they are closely related to each other due to the implicit relationships among them. This means that any significant change in a particular control area could have a serious impact on the normal functionality of other areas. For example, problems registered in an engineering component (e.g., a defect in a Remote Terminal Unit (RTU)) may create significant changes in operational control processes or a massive loss of information. In the following, the goals and functionalities of these four control areas are described in detail.

- Services: A service is made available by an infrastructure for use or consumption by end-users or other infrastructures. Within this category, it is possible to identify two types of services: *infrastructure services* (ser_i) and *control services* (ser_c). Infrastructure services are related to critical services provided by controlled infrastructures, such as electrical energy, whilst control services are related to all those supervision processes that monitor other CIs and their services (ser_i).
- Resources: It refers to those system elements (either physical or logical) that form part of the successful delivery of ser_c. In fact, within this category there are three further sub-areas:
  - Physical resources (r_{phys}): This type of resources represent the physical elements that form part of the facilities and protect the environment, conditions and safety (e.g., prevention, surveillance and access control mechanisms).
  - Control resources (r_{conts}): This type of resources form the set of engineering components in charge of managing and controlling the real status of the context. This means the management and storage of sensitive information as well as the execution of operational tasks. Basically, these engineering components can range from HW industrial devices (e.g., RTUs, relays, sensors, actuators ...), to software-based components (e.g., control applications, historical databases, alarm management systems ...). In addition, it is also possible to include within this category all those HW and SW security devices devoted to the logical protection of the information and its resources, such as firewalls, Intrusion Detection Systems (IDS), Early Warning Systems (EWS), Demilitarized Zones (DMZ), antivirus, etc.
  - Operational control resources (r_{opcs}). They are related to those elements that ensure a suitable operational management, interoperability and cooperation through a common regulatory framework, containing both technical and legal aspects. Also they are related to management activities such as risk assessment, schedule and management of training, maintenance and auditing, and verification and validation processes (known as safety-engineering) to check the (HW/SW) real status of the system.
- Operational control (opc): It refers to all those supervisory actions managed by an authorized entity (human operators, software processes or systems). Such actions are performed through control messages (i.e., commands) that specify the action to be executed (e.g., close/open pump).
- Sensitive information (inf): As has already been mentioned, inf represents a set of sensitive information such as measurements or alarms. However, inf also includes in its list, commands, since it contains sensitive information whose value is an action to execute. Hence, inf is composed of measurements, alarms and commands.

Nomenclature	Definition
I_x - ser_{ix}	Critical Infrastructure (CI) - Delivered Service by a CI
I_{SCADA} - ser_c	Control System - Control Service
I_E - ser_{ie}	Electrical Energy System - Electrical Energy
I_O - ser_{io}	Oil energy system - Oil Energy
I_G - ser_{ig}	Gas Energy System - Gas Energy
I_W - ser_{iw}	Water and Sewage Treatment Systems - Water
I_T - ser_{it}	Transportation System - Transportation
I_C - ser_{ic}	Communication System - Communication
inf	Sensitive Information
opc	Operational Control
r_{phy}	Physical Resources
r_{cont}	Control Resources
r_{opc}	Operational Control Resources
●	Affected Control Area
○	Origin of a Problem (either Threat or a Fault)
⟶	Dependency Relationship
⇢	Transitive Dependency Relationship

Table 1: Nomenclature

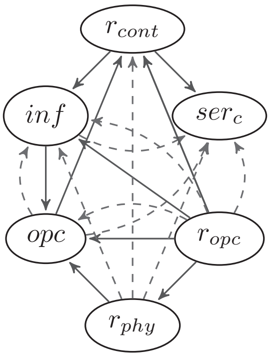

Figure 1: Dependence Graph $\mathcal{G}$ with the Control Areas

Taking into account the nomenclature of Table 1, the next step is to analyze the existing dependency relationships among control areas in order to study consequences and impact on the final control; i.e., ser_c. To this end, we firstly define the set of areas $\{ser_c, inf, opc, r_{phy}, r_{cont}, r_{opc}\}$ as $\mathcal{AC}$ so as to build a dependency graph denoted as $\mathcal{G}$. It should be noted that the construction of the graph is based on the experience and lessons Learnt from project SECRET [2], which is focused on the security of SCADA systems and their substations.

$\mathcal{G}$, depicted in Figure 1, represents, on the one hand, the control areas in each node, and on the other hand, the dependency relationships among areas through edges. This means that if $\{x,y\}$ $\in \mathcal{AC}$ and $x \rightarrow y$, then x *has an influence on* y or y *depends on* x *to work*. Said dependency relationship is symbolized as R and it is formally described as: $\forall\ x,y \in \mathcal{AC}$[1]: $(x,y) \in R$. Likewise, if $\forall\ x,y,z \in AC$: $((x,y) \in R \wedge (y,z) \in R)$, then a transitive relationship $(x,z) \in R$ could also happen.

Given the previous criteria, the following study focuses on analyzing how each area could have an influence on ser_c. Namely, let $(r_{cont}, ser_c) \in R$ be a relationship between a control component, r_{cont}, and a control service, ser_c. It is possible that such a relationship may directly affect the control as a HW/SW fault may cause a change in the normal state of the delivered service.

[1] It is important to comment that ser_i has not been included within this set, since the analyses mainly focus on those situations where an effect does not pass through the limits of a system. Nonetheless, ser_i will be analyzed later in Section 3.5, where an anomalous effect will be able to exceed the unallowable boundaries of the control system.

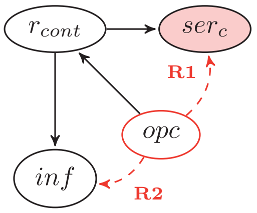

Figure 2: Relationships R1 and R2

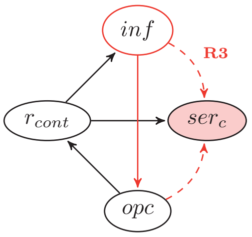

Figure 3: Relationship R3

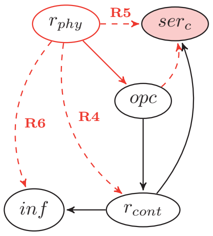

Figure 4: Relationships from R4 to R6

Given $(opc, r_{cont}) \in R$, any operational fault caused by an error provoked by an entity may sooner or later trigger a disruption on ser_c. This is due to the transitive dependency relationship described below (R1) and which is also depicted in Figure 2.

$$(opc, r_{cont}) \in R \wedge (r_{cont}, ser_c) \in R \Rightarrow (opc, ser_c) \in R \qquad <\text{R1}>$$

Moreover, as r_{cont} is in charge of containing and managing sensitive information, inf, any HW or SW fault in such a r_{cont} may affect the availability or integrity of inf. This can be formally represented as $(r_{cont}, inf) \in R$. Taking into account this relationship, an operational fault may also have an influence on availability/integrity of inf by taking out an existing transitive relationship between opc and inf (R2). Here, a malicious individual or an authorized operator may, for example, shut down a RTU at a given moment, hiding relevant information associated with supervision. Namely:

$$(opc, r_{cont}) \in R \wedge (r_{cont}, inf) \in R \Rightarrow (opc, inf) \in R \qquad <\text{R2}>$$

Given the dependency relationship $(inf, opc) \in R$, any data received from a r_{cont} can have an influence on the decision-making over the system (see Figure 3). For example, if an inf is altered, such as critical alarms, the human operator's decision will be unintentionally false through R1, putting at risk the continuity of ser_c. It can be formally described as follows:

$$(inf, opc) \in R \wedge \text{R1} \Rightarrow (inf, ser_c) \in R \qquad <\text{R3}>$$

Regarding physical resources of the system, r_{phy}, they also have a certain influence over control services. For example, problems with access control could impede an authorized operator from gaining access to the system to manage r_{conts}. Therefore, there exists a dependency relationship between r_{phy} and r_{cont} (R4), and even r_{phy} and ser_c (R5). Moreover, any authentication problem may even impact on inf (R6) since unattended r_{conts} also mean unattended inf. Formally,

$$(r_{phy}, opc) \in R \wedge (opc, r_{cont}) \in R \Rightarrow (r_{phy}, r_{cont}) \in R \qquad <\text{R4}>$$
$$(r_{phy}, opc) \in R \wedge \text{R1} \Rightarrow (r_{phy}, ser_c) \in R \qquad <\text{R5}>$$
$$(r_{phy}, opc) \in R \wedge \text{R2} \Rightarrow (r_{phy}, inf) \in R \qquad <\text{R6}>$$

With respect to r_{cont}, any compromised or defective control resource may suppose an inefficient operational control, opc, since inf is not managed properly. In addition, this situation may even leave inf unavailable, where critical alarms could be hidden/unattended or relevant measurements could be lost (R7). Likewise, any change in a r_{cont} may provoke an effect on ser_c due to the relationships $(r_{cont}, ser_c) \in R$ and R8. Figure 5 represents said links, the relationships of which are formally described as follows:

$$(r_{cont}, inf) \in R \wedge (inf, opc) \in R \Rightarrow (r_{cont}, opc) \in R \qquad <\text{R7}>$$
$$(r_{cont}, inf) \in R \wedge \text{R3} \Rightarrow (r_{cont}, ser_c) \in R \qquad <\text{R8}>$$

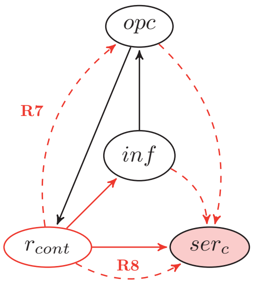

Figure 5: Relationships R7 and R8

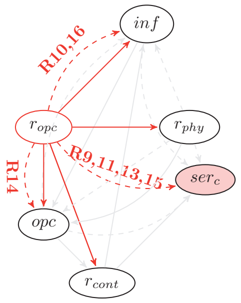

Figure 6: Relationships from R11 to R16

As r_{opc} is in charge of managing and coordinating any legal and technical activity within a system, it keeps a narrow relationship with the rest of the control areas. Namely, $(r_{opc}, r_{phy}) \in R$, $(r_{opc}, r_{cont}) \in R$, $(r_{opc}, opc) \in R$, $(r_{opc}, inf) \in R$. In spite of the fact that there is not a direct relationship between r_{opc} and ser_c, a negligent or an incorrect action in some part of r_{opc} may indirectly have an impact on ser_c (see Figure 6). Dependency relationships associated with r_{cont} are formally described below.

$$\begin{array}{cl}
(r_{opc}, opc) \in R \wedge \text{R1} \Rightarrow (r_{opc}, ser_c) \in R & \text{<R9>} \\
(r_{opc}, opc) \in R \wedge \text{R2} \Rightarrow (r_{opc}, inf) \in R & \text{<R10>} \\
(r_{opc}, inf) \in R \wedge \text{R3} \Rightarrow (r_{opc}, ser_c) \in R & \text{<R11>} \\
(r_{opc}, r_{phy}) \in R \wedge \text{R4} \Rightarrow (r_{opc}, r_{cont}) \in R & \text{<R12>} \\
(r_{opc}, r_{phy}) \in R \wedge \text{R5} \Rightarrow (r_{opc}, ser_c) \in R & \text{<R13>} \\
(r_{opc}, r_{cont}) \in R \wedge \text{R7} \Rightarrow (r_{opc}, opc) \in R & \text{<R14>} \\
(r_{opc}, r_{cont}) \in R \wedge \text{R8} \in R \Rightarrow (r_{opc}, ser_c) \in R & \text{<R15>} \\
(r_{opc}, r_{cont}) \in R \wedge (r_{cont}, inf) \in R \Rightarrow (r_{opc}, inf) \in R & \text{<R16>}
\end{array}$$

As a result, four control areas and sixteen dependency relationships have been analyzed. Based on this, the next step is to research what types of control requirements are necessary to accommodate ICTs in the four control areas. To achieve this, a trade-off between performance and security has to be considered throughout the following Section.

3 Requirements for Industrial Control Systems

Given that a trade-off between performance and security should be tolerated for guaranteeing a reliable and secure control, five requirements have been identified: *real-time performance, dependability, sustainability, survivability* and *safety-critical*. It should be stressed that the analyses described below are based on the studies shown in Section 2 and using the nomenclature described in Table 1.

3.1 Real-time Performance

Process execution is normally subject to certain deadlines and delays. These delays are very common in those r_{conts} in charge of concurrently processing different messages and algorithms for supervision. The execution time of an algorithm does not follow a static execution model. It varies according to the required time to run one or several control procedures, the computation of which could depend on the processing time and output streams from other processes or I/O interfaces. In addition, data integrity constraints may be violated due to the concurrent nature of processes, which may fall into the same execution point or request the same data registers or resources.

On the other hand, upgrade of the system not only involves important changes in the network architecture, but it may also add significant computational and communication delays. To be more precise, any agreement procedure and routing in TCP/IP-based communication systems may produce important delays in the control tasks [3]. If in addition, technological convergence allows supporting integration of different industrial devices using different communication protocols, then both interoperability and connectivity could also add significant delays in the control. Furthermore, incidents, faults, threats, or even their own (HW/SW) security measures, may also involve important operational delays or architectural complexities.

Therefore, computational or communication interruptions within a r_{cont} means delays of output streams either inf or opc due to the relationships $(r_{rcont}, inf) \in R$, $(inf, opc) \in R$ and R7, seriously affecting ser_c by $(r_{cont}, ser_c) \in R$, R3 or R8. The causes of the problem, its origin, impacted areas, security and protection measures, and its representation are summarized as follows:

- Problem: problems with scalability, extensibility, interoperability and intolerance to (HW/SW) failures.
- Origin of the problem: r_{cont}.
- Impacted areas: inf, opc and ser_c.
- Measures: fault-tolerance, fault-forecasting, fault-detection, fault-prevention, fault-removal, maintainability (r_{conts}), and coordination using self-stabilization techniques.

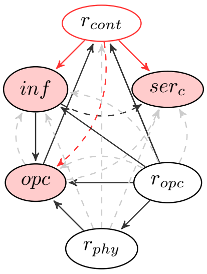

Figure 7: Real-time Performance

3.2 Dependability

Dependability was defined by Al-kuwaiti et al. as "*the ability of the system to properly offer their services on time, avoiding frequent and severe internal faults*[2]" [4]. Moreover, they also define it as the property that encompasses other five essential attributes, such as: *availability, reliability, maintainability, safety* and *security*. Given these five attributes, we will analyze how they can individually impact on the global dependability of the system, and more particularly on the individual performance of their operational resources; i.e., r_{conts}.

Both availability and reliability are two attributes that have a direct influence on the control components of the system (r_{conts}). If one r_{cont} does not properly offer the correct service at a given moment, then the r_{cont} will be unavailable, and it will hence be unreliable. This situation, normally caused by SW/HW faults within a r_{cont} or operational faults, may have a serious effect on inf by $(r_{cont}, inf) \in R$; on ser_c by $(r_{cont}, ser_c) \in R$, R3 and R8; and on opc by R7. If said effect is not controlled, it could take a progressive nature, since control components are narrowly linked each other, exponentially increasing the costs of maintainability.

Another aspect to consider is r_{phy} and r_{opc} on availability and reliability. For the former control area (i.e., r_{phy}), if a physical resource presents serious problems of configuration or HW failures, it can disrupt authorized human operators to gain access to the environment, affecting opc by $(r_{phy}, opc) \in R$. As a consequence, any r_{cont} may be unattended because of R4, as well as its critical information (e.g. critical alarms) by R6, later damaging ser_c through R5. Regarding r_{opc}, this one also has both a direct or indirect influence on r_{cont}, r_{phy}, inf and opc. For example, a r_{cont} may not be managed properly by the lack of knowledge or incapacity to access a technical documentation at a given moment. Therefore, the impact lies with r_{cont} through (r_{opc}, r_{cont}) or R12; opc through $(r_{opc}, opc) \in R$ or R14; inf through $(r_{opc}, inf) \in R$, R10 or R16; r_{phy} through $(r_{opc}, r_{phy}) \in R$; and ser_c through R9, R11, R13 and R15.

The maintainability of the system is another attribute to take into account within the dependability. A HW/SW fault in one r_{cont} involves an impact on inf through $(r_{cont}, inf) \in R$, causing a change in opc due to $(inf, opc) \in R$ or R7, on and ser_c through $(r_{cont}, ser_c) \in R$, R3 or R8. Similarly, an unintentional human-made error (i.e., opc) means incorrect management of a r_{cont} by $(opc, r_{cont}) \in R$, and consequently a change in the integrity of inf through R2 and in ser_c through R1. On the other hand, safety is also an associated attribute to physical conditions of the application context; i.e., r_{phy}. A context alteration may trigger a perturbation on opc due to $(r_{phy}, opc) \in R$, r_{cont} through R4, inf because of R6, and ser_c through R5.

[2] Internal fault refers to HW, SW or operational faults, which are originated within the system; whilst external faults are those that come from outside, such as natural occurrences, external malicious actions or accidents.

Lastly, security is an attribute that must be widely applied to r_{cont}, since it is in charge of managing sensitive data or operational tasks. Any unintentional internal fault may not only leave unavailable one r_{cont} and its inf, but also disrupt any operational task (opc), consequently affecting the ser_c. This is due to the relationships $(r_{cont}, ser_c) \in R$, $(r_{cont}, inf) \in R$, R7 or R8. If in addition, the opc has problems to operate a particular r_{cont}, then the stored inf and ser_c may be unattended by R2 and R1, respectively. In addition, in the case where inf is required, but is unavailable, then opc and ser_c can be affected through $(inf, opc) \in R$ and R3, respectively.

Summarizing:

- Problem: non-maintainability, intolerance to unintentional internal (HW, SW, operational) faults.
- Origin of the problem: r_{cont}, r_{phy}, r_{opc} and opc.
- Impacted areas: r_{cont}, inf, opc, r_{phy} and ser_c.
- Measures: fault-tolerance, fault-forecasting, fault-prevention, fault-detection, fault-removal, maintainability (r_{conts}, r_{opc}, training), safety-engineering.

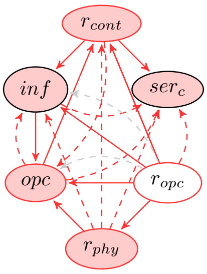

Figure 8: Dependability

3.3 Sustainability

Sustainability has been defined as "*that development that is able to meet the needs of the present without compromising the ability of future generations to meet their own needs*" [5]. In our context, this concept still makes sense, since the architecture of a critical control system has to endure over time, in terms of years and decades. This means that a critical control system has to guarantee that its (HW/SW) components are able to reuse their resources, services or mechanisms, support new and future versions, and ensure interoperability with existing (HW/SW) components.

We therefore highlight four additional attributes: *scalability, extensibility, interoperability* and *maintainability*. A non-scalable or non-extensible system is a system that is not able to support new control components r_{conts} such as current technologies, protocols, (HW/SW) components or new security services. In addition, these situations could become worse when one r_{cont} (e.g., an incompatible RTU) is not able to interact with other resources due to a lack of interoperability. As a consequence, parts of the system could remain isolated, causing an effect on inf, opc and ser_c. In other words, the system could degrade its functionalities because of $(r_{cont}, inf) \in R$, affecting operational tasks through $(inf, opc) \in R$ or R7. Likewise, if opc is affected, a human operator may not be able to manage either a r_{cont} or its inf due to the relationships $(opc, r_{cont}) \in R$ and R2, respectively. Obviously, the impact sooner or later falls on ser_c because of $(r_{cont}, ser_c) \in R$, R1, R3 or R8. On the other hand, a system with problems of extensibility could also take out the impact on the ser_c, since new or updated security services may not adapt to the existing design and resources, leaving control components totally isolated. Such isolation may even interrupt the continuity of operational tasks with an effect on the management and control of other control areas such as inf, r_{conts}, and ser_c. Given that extensibility and interoperability have the same effect as scalability, all of them present the same dependency relationships.

Regarding maintainability, human operators' skills to handle new resources or security services may also have an influence on managing the control components due to $(opc, r_{cont}) \in R$ with serious consequence on the ser_c through R1. Moreover, these skills could alter the integrity of inf given that there exists a relationship between opc and inf through R2. Hence, any human operator should be trained to learn how to use the new ICTs and their application in the field. Similarly, an unrevised r_{cont} may also reverberate on data acquisition and supervision, since inf, opc and ser_c may be affected by $(r_{cont}, inf) \in R$, R7, $(r_{cont}, ser_c) \in R$, R1, R3 or R8.

An uncontrolled risk management, a strategic plan or regulatory framework (i.e., r_{opc}) could also alter the business continuity and the interoperability due to the existing relationships of r_{opc} with r_{cont}, inf and opc, i.e., $(r_{opc}, r_{cont}) \in R$, $(r_{opc}, inf) \in R$ and $(r_{opc}, opc) \in R$, in addition to

R10, R14 and R16. As a result, ser_c can, thereby, be affected by R9, R11 or R15. Lastly, and as part of the maintainability, measures for validating facilities and their physical resources (i.e., r_{phys}) are also considered in order to protect working conditions. Such protection and control should follow established policies, since there exists a close relationship between $(r_{opc}, r_{phy}) \in R$ with an indirect repercussion towards opc, r_{cont}, inf and ser_c through $(r_{phy}, opc) \in R$, R4 and R6 and R5. Moreover, both r_{cont} and ser_c may also be indirectly damaged by R12 or R13 if one or several r_{phys} do not comply with the conditions defined in r_{opc} (e.g. access control policies).

Summarizing:

- Problem: problems with interoperability, extensibility, scalability and maintainability (r_{opcs}, r_{cont}, r_{phy} and opc through training).
- Origin of the problem: r_{cont}, r_{opc}, r_{phy} and opc.
- Impacted areas: r_{cont}, inf, opc, r_{phy} and ser_c.
- Measures: maintainability (r_{conts}, r_{opc}, r_{phy} and opc through training) and safety-engineering.

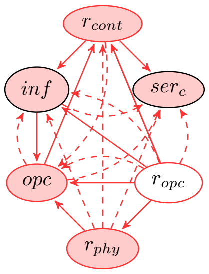

Figure 9: Sustainability

3.4 Survivability

Survivability can be defined as "*the capability of a system to fulfil its mission and thus to face malicious, deliberated or accidental faults in a timely manner*" [6]. This means that a survivable system also assumes the concept of *resilience* by allowing the system to continue its services when part of its security is compromised. Note that this fact is what distinguishes it from dependability. Dependability aims to provide services in the presence of internal faults, whereas survivability focuses on providing services in the presence of *external faults and/or malicious deliberate actions*. Moreover, Al-Kuwaiti et al. defined it as '*that attribute composed of a further five properties: reliability, availability, fault-tolerance, safety and security*" [4], which will be analyzed in detail below.

Considering a hostile environment, (deliberated or accidental) external faults could also leave r_{conts} in unavailable states. Such states could impede the management of sensitive information (i.e., inf and opc) because of $(r_{cont}, inf) \in R$, R2 and R7, or disrupt the execution of control operations due to the relationship $(opc, r_{cont}) \in R$. These facts could even affect reliability and availability of ser_c by $(r_{cont}, ser_c) \in R$, R1, R3 or R8. Similarly, there are other several ways of degrading the resilience of a system. One of them would be, for example, to compromise the safety or surroundings of the system (i.e., r_{phy}) in order to compromise opc due to $(r_{phy}, opc) \in R$. This means that if an operator cannot gain access to a part of the system, then r_{cont}, inf and ser_c could be left unattended due to R4, R5 and R6.

An intruder may also launch attacks on the availability, integrity or confidentiality of opc and inf by compromising r_{cont}. A threat on the availability means: (i) unattended inf if (r_{cont}, inf) $\in R$ or R2 are disabled; and (ii) unmanaged commands if $(opc, r_{cont}) \in R$, $(inf, opc) \in R$ or R7 are not feasible. Attacks on the integrity refers to manipulation of inf due to the relationship $(r_{cont}, inf) \in R$, creation of false/malicious actions through R2 or $(opc, r_{cont}) \in R$, or sending false information to an operator via R7. In either case, ser_c can be affected by the relationships $(r_{cont}, ser_c) \in R$, R1, R3 or R8. Lastly, attacks on the confidentiality means taking advantage of compromised r_{conts} (e.g., communication channels) to eavesdrop on inf. In spite of the fact that $(r_{cont}, inf) \in R$ can be compromised, this threat does not imply a greater risk in comparison to previous threats since ser_c is not really damaged.

In the same way, any authenticated malicious entity with enough permissions may pass through the constraint parts of the system to execute authorized malicious activities given the relationship $(opc, r_{cont}) \in R$. As a consequence, other control areas may be compromised, such as inf through R2 or ser_c through $(r_{cont}, ser_c) \in R$, R1, R3 or R8.

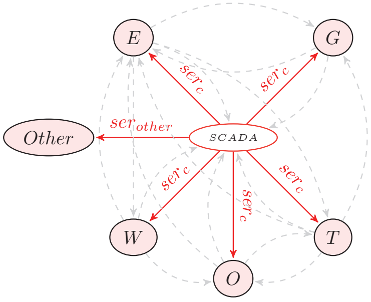

Figure 11: The effect of ser_c over ser_{ix}

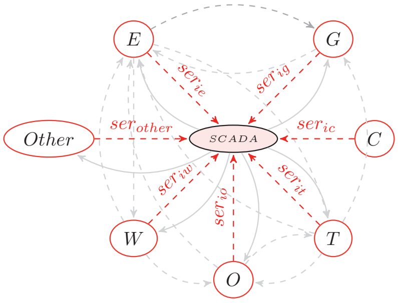

Figure 12: The effect of ser_{ix} over ser_c

Summarizing:

- Problem: intolerance to (HW, SW, operational) external faults or deliberated actions.
- Origin of the problem: r_{cont}, opc, r_{phy}.
- Impacted areas: r_{cont}, inf, opc and ser_c.
- Measures: security policies, accountability, authentication, authorization, non-repudiation, cryptographic services, isolation of affected areas, boundaries services (e.g. firewalls, IDSs, DMZs, etc.), fault-forecasting, fault-prevention, fault-detection, fault-location and redundancy (e.g., redundant systems, backup systems, etc.).

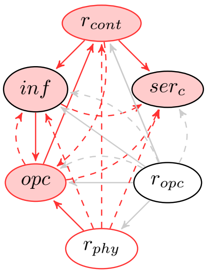

Figure 10: Survivability

3.5 Safety-critical

A variant of safety for critical environments is safety-critical. This property refers to "*those systems that can potentially lead to serious catastrophic consequences due to the existence of unplanned events, which could result in human deaths or injuries, or even significant physical damage*" [7]. When such an effect goes beyond that of the permissible boundaries of a critical system to other CIs, its effect could generate a cascading effect [1]. Taking into account this definition and the nomenclature found in Table 1, let $\mathcal{S}$ be the set of critical services $\{ser_c$, ser_{ie}, ser_{ig}, ser_{io}, ser_{iw}, ser_{it}, $ser_{ic}\}$ corresponding to the set of CIs $\{I_{SCADA}$, I_E, I_G, I_O, I_W, I_T, $I_C\}$, then three cases could take place within a critical control system:

- Case 1: ser_c *stops working*, leaving without protection the controlled infrastructures and their services, ser_{ix}. This situation is depicted in Figure 11 where it is possible to see how ser_c has an important influence over the rest of CIs and their services ser_{ix} (see direction of red arrow).
- Case 2: ser_{ix} *stops working*, leaving without service I_{SCADA} to provide ser_c, as Figure 12 depicts. This is due to the existing strong interdependence relationships between services. Additionally, a further two situations may occur:
  - Case 2-A: *An input stream, ser_{ix}, is required for the continuity of r_{conts}, where $ser_{ix} \in \{ser_{ie}$, ser_{ig}, ser_{io}, ser_{iw}, ser_{it}, $ser_{ic}\}$.* This means that a r_{cont} may stop its normal functions whether ser_{ix} (e.g., electricity for ICTs) is not properly provided given that $(ser_{ix}, r_{cont}) \in R$. This can even consequently affect on inf due to $(r_{cont}, inf) \in R$, opc through R7, and ser_c through $(r_{cont}, ser_c) \in R$, R3 or R8. To understand this situation by means of an example, we consider ser_{ix} as the TCP/IP communication service. If a remote r_{cont} (e.g. an RTU) is not able to access communication channels and send inf at a given moment, an essential part of the system could become unattended or isolated.

Requirements	Services	Resources			Infor.	Oper. Control
		r_{opc}	r_{cont}	r_{phy}		
	Real-Time Performance					
Real-Time Performance	→,R3,R8				→	→,R7
	Dependability					
Reliab. & Avail.	→,R1,R3,R5,R8,R9,R11,R13,R15		→,R4,R12	→	→,R6,R10,R16	→,R7,R14
Maintainability	→,R1,R3,R8		→		→,R2	→,R7
Safety	R5		R4		R6	→
Security	→,R1,R3,R8				→,R2	→,R7
	Sustainability					
Scalab. & Extens. & Int.	→,R1,R3,R8		→		→,R2	→,R7
Maintainability	→,R1,R3,R5,R8,R9,R11,R13,R15		→,R4,R12	→	→,R2,R6,R10,R16	→,R7,R14
	Survivability					
Reliab. & Avail. & Fault-tolerance	→,R1,R3,R8		→		→,R2	→,R7
Safety	R5		R4		R6	→
Sec-Availability	→,R1,R3,R8		→		→,R2	→,R7
Sec-Integrity	→,R1,R3,R8		→		→,R2	R7
Sec-Confidentiality					→	
Sec-Authen.&	→,R1,R3,R8		→		R2	
Sec-Author.						
	Safety-Critical					
Case 2-A	→,R3,R8				→	R7
Case 2-B	R1		→		R2	

Table 2: Requirements of control systems, vulnerable areas and impact on ser_c

  - Case 2-B: *An input stream, ser_{ix}, is required for operational control (i.e., opc), where* $ser_{ix} \in \{ser_{ic},\ ser_{it}\}$. Here, it is important to highlight the importance of communication systems and/or transportation systems (for human operators in the field) which are essential for supervision tasks. If *opc* is disrupted, then the control of one or several r_{conts} and their inf could be unattended due to $(opc, r_{cont}) \in R$ and R2, consequently interrupting ser_c by R1.

- Case 3: *The cascading effect.* It is possible that an effect can be widely extended towards other CIs when the first or second cases occur. This situation may not only impact on the business continuity, but it may also affect the welfare of a region or a country [1]. Here, the 'time' factor plays a fundamental role, since most of these events occur over time and their mitigation processes are also dependent on time.

Therefore, control of boundaries, the generated effect and its propagation throughout time must constitute an essential requirement to take into account in the life-cycle of a system. To this end, a set of protection solutions are required, such as for example: to verify the correctness of SW/HW components through safety-engineering approaches; define mitigation and preparedness plans, actuation policies and security policies using modeling and simulation approaches; implement proactive mechanisms, boundary and cryptographic services; and prepare all those emergency mechanisms that help the system to manage faults (i.e., fault-location, fault-removal, fault-isolation), as well as prioritization of services, isolation of areas, restoration and recovery.

3.6 Discussions

Table 2 summarizes the results obtained and presented throughout this paper. This does not only represent dependency relationships between areas, but it also provides us with much more information than we had expected. It shows us a clear representation of those areas that are most vulnerable to failures and those areas that could have a serious impact on ser_c. Observing Table 2, it is possible to see that r_{cont}, inf and *opc* are the most susceptible areas within a critical system. This fact can be also appreciated in Figure 7, Figure 8, Figure 9 and Figure 10. They show how a source node of a problem (or several) may have an impact on the rest.

Capacities of processing and storage of r_{conts} are the main causes of these facts, since said resources are in charge of managing information (inf) and control actions (*opc*), in addition to considering their narrow proximity to the control service. Skillful adversaries may take advantage of this situation to break the protection of the system and its performance. Their goal would be to compromise r_{conts} so as to alter its inf and *opc*, and consequently alter ser_c due to the relationships: $(r_{cont}, inf) \in R$, R7, $(r_{cont}, ser_c) \in R$ and R8. This can also be noted in Figure 13. In such a Figure, it is possible to see how a human operator is not able to interact with the system when a control resource is, for example, compromised, leaving unprotected both the control services and the services of the infrastructure itself.

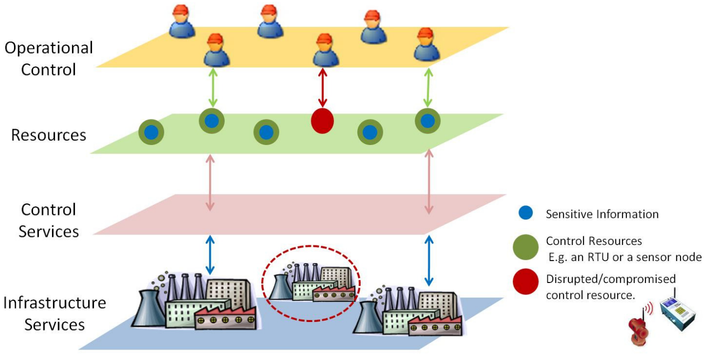

Figure 13: Dependences between Control Areas

4 Conclusions

While technological convergence offers interesting benefits for control, new operational complexities and security risks start to arise at the same time. This situation has encouraged us to reassess the context of control, its four control areas (services, resources, operational control and sensitive information) and their relationships. As a result, five requirements of control have been identified so as to study the possibility of accommodating new ICTs achieving a suitable trade-off between performance and security. Furthermore, this study has also helped us to formally show that the most targeted and most vulnerable control areas to incidents, faults and threats are the control resources, since they could put the operational activities and sensitive information at risk, seriously affecting the control service and on the services of other critical systems.

It should be noted that although there are several studies in the literature dealing with similar aspects to this topic, the work presented here differs from the rest by formally describing and analyzing the current control areas, their relationships and problems in the control service. Nonetheless, as all of these analyses follow a static model, where individual threatening cases have been considered, it would be useful, in the future, to extend the work done here to study the level of degradation of the system when several control areas are being affected at the same time.

5 Acknowledgements

We want to thank Prof. Stephen Wolthusen for his valuable comments and ideas. This work has been partially supported by the Spanish Ministry of Industry through the project SECRET [2], as well as by the Spanish Ministry of Science and Innovation through the projects ARES (CSD2007-00004) and SPRINT (TIN2009-09237), being the last one also co-financed with FEDER funds.

References

[1] J. Peerenboom and R. Fisher. Analyzing Cross-Sector Interdependencies. *IEEE Hawaii International Conference on System Sciences*, pages 112–119, 2007.

[2] SECRET Project. Security of Critical Elements of Energy Control Systems, Spanish Ministry of Industry, TSI-020100-2011-152. `https://www.nics.uma.es/SECRET/`.

[3] K. Wu and M. Chen. JTCP: Jitter-based TCP for Heterogeneous Wireless Networks. *IEEE Journal on Selected Areas in Communications*, 22(4):757–766, 2004.

[4] M. Al-Kuwaiti, H. Kyriakopoulos, and S. Hussein. A Comparative Analysis of Network Dependability, Fault-tolerance, Reliability, Security, and Survivability. *IEEE Communications Surveys & Tutorials*, 11(2):106–124, 2009.

[5] United Nations General Assembly. Development and International Co-operation: Environment; Our Common Future, Chapter 2: Towards Sustainable Development. Commission on Environment and Development: Our Common Future, Document A/42/427, `http://www.un-documents.net/ocf-02.htm`, 1987.

[6] J. Knight and E. Strunk. Achieving Critical System Survivability through Software Architectures, Architecting Dependable Systems. In *Architecting Dependable Systems II, LNCS 3069*, pages 51–78. Springer-Verlag, 2004.

[7] J. Bowen and V. Stavridou. Safety-Critical Systems, Formal Methods and Standards. *Software Engineering Journal*, 8(4):189–209, 1993.