GENERIC CONTROL SYSTEM ARCHITECTURE FOR CRITICAL INFRASTRUCTURE PROTECTION

Hrvoje Sagrak[1]

Introduction

In an interconnected world that we live in, protection of our societies and values relies highly on critical infrastructures. The more we are developed, the higher is the dependency on critical infrastructures, the higher are the stakes and risk impacts of threat to it. From the perspectiive of an EU member country, the approach in protection of the critical infrastructures takes into account the national, regional and EU level with respective aligned regulattory frameworks and policies. Due to the multi dimensional character of CI's, embedded interdependency among it from the sectoral point of view and territorial (national, regional, supra-national) a comprehensive, hollistic approach not only to security but also to the overall model of protection needs to be developed at the national level and integrated at the supra-national level. Therefore, taking into account the main regulations and legal base at the EU and Croatian level, this article explores in brief and on a high level the Generic Control System Architecture for CIP to be presented as a model upon which knowledge based, process event control information systems for CIP could be designed and built in order to enhance the effectiveness and efficiency on a member state and EU level of the critical infrastructure protection.

[1] Hrvoje Sagrak is a Public Sector Solution Sales Director in InfoDom, Zagreb, Croatia. He has a University of Zagreb Degree in Law and Executive MBA from Cotrugli Business School.

Regulatory Framework – EU and Croatian level

Main sources of the regulatory framework at the EU level are the following http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm):

a. European Programme for Critical Infrastructure Protection (2006)

   - EPCIP Action Plan.
   - ERNCIP - The European Reference Network for Critical Infrastructure Protection forms part of the European Programme for Critical Infrastructure Protection and aims at providing a framework within which experimental installations will share knowledge and expertise throughout Europe leading to improved protection of critical infrastructure against all hazards.

b. Directive on European Critical Infrastructures 2008/114/EC

   Sets up a procedure for identifying and designating European critical infrastructures. It provides a common approach for assessing these infrastructures, with a view to improving them to better protect the needs of citizens.

c. Proposal for a Council Decision on a Critical Infrastructure Warning Information Network (CIWIN) {SEC(2008)2701} {SEC(2008)2702}

   The proposal aimed at assisting Member States and the European Commission to foster exchange information on shared threats, vulnerabilities and appropriate measures and strategies to mitigate risk in support of Critical Infrastructure Protection (CIP). A Commission owned protected public internet based information and communication system, offering recognized members of the EU's CIP community the opportunity to exchange and discuss CIP-related information, studies and/or good practices across all EU Member States and in all relevant sectors of economic activity. The CIWIN portal is in production since mid-January 2013.

d. 8/08/2013 - Commission staff working document on a new approach to the European Programme for Critical Infrastructure Protection. The document emphasized the need for a systems approach to CIP issues rather than the sectoral that had been mostly used before. Interdependency between CI's, industry and state actors is taken into account in the new approach.

e. 22/06/2012 - Commission staff working document on the review of the European programme for critical infrastructure protection (EPCIP);

f. 31/03/2011 - Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security' (COM(2011) 163 final);

g. 30/03/2009 - Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (COM(2009) 149 final).

In **Croatia**, the main legislative framework on the topic of CIP is sublimated in the following:

a. Law on Critical Infrastructures (2013)

b. Decision on determining the sector from which the central government bodies identify national critical infrastructure and lists the order of the critical infrastructure sectors (2013)

c. Rules on the methodology for a risk analysis of critical infrastructures conduct of work (2016). It has been aligned with ISO 31000 Risk Management standard and replaced the previous Rules from 2013.

CIP Value Chain

From the methodology point of view, to present a model for CIP from the national/state perspective we shall take into account two main situational statuses: pre-accident (Figure 1

– blue) and post-accident (Figure 1 – red) with hazardous impact to the critical infrastructure.

Namely, due to the main characteristics in an occurence of a harm to the critical infrastructure, e.g. energy supply (due to the limited frame of this article, we consider here events that do significant harm to the CI) the respective processes should be aligned to the expected envvironment in such an accident, that is: elements of surprise, sudden occurence and disruption of normal life, great public and media attention, national security at risk (terrorism). Such environment requires that the reaction aimed at recovery needs to be very fast (automatic), mostly with limited resources, less than planned, while decision making is constrained with limited available or confusing information.In order to have automated standard operating procedures and reactions in place when needed, simulations with respect to risk assessment have to be conducted and the system tested at a level that is feasible.

In order to enable such rapid and comprehensive reaction for recovery that makes the risk of harm acceptable, Communication among all stakeholders to ensure Awareness of CIP and Prevention measures that ensure Readiness (Figure 1) in the case of need, should be developed. Moreover, CIP awareness and readiness, as desired outputs, should be comprehensively transmitted horizontally and vertically through all stakeholders in order to enable proper Crisis Management and desired Reaction as output after Hazardous Incident occurs. Rapid Recovery processes that would follow (based on standard operating procedures) aim to stabilize the situation after the accident and should trigger suggestions for Improvements, as lessons learnt.

Figure 1: CIP value chain

Above described view requires understanding of the elements of the CIP Governance Value Chain - Figure 2.CIP governance structure has to be set up in order to conduct the Assessment and Planning, which process group outputs are used by the overall System of critical infrastructure protection. Such system generates, according to risk assessment, control functions to inspect readiness for reactions on accidents. As needed, corrective measures shall be applied as a result of control processes. In the case of Accident, as an undesired event, processes based on Protection Action Rules are triggered for recovery purposes. The cycle ends through knowledge management concepts of lessons learnt and new strategic initiatives to be employed in the overall CIP governance structure.

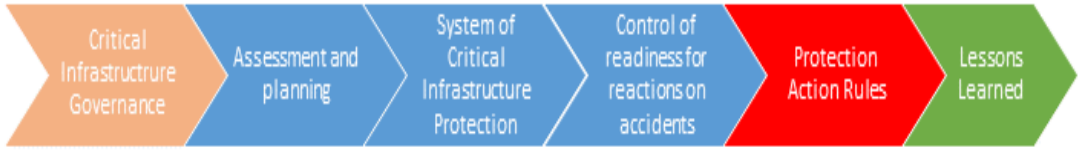

Figure 2: CIP Governance value chain

CIP Stakeholders

The complexity of the concept of Generic Control System Architecture illustrate the multidimensional stakeholders that are concerned with the CIP procedure at the EU and national level, as part of the CIP network:

- EU - DG HOME; DG ENERGY, DG CONNECT...
- CIWIN – Critical Infrastructure Warning Information Network
- ERNCIP – European Reference Network for Critical Infrastructure Protection ...
- National Government
- Government Bodies

- National Protection and Rescue Directorate (in Croatia)
- CI Owners
- Regulatory Agencies
- Certified Suppliers/private companies
- Business/Citizens

Central National CIP Management System

In order to set up a Critical Infrastructure Protection Management System at a national level, both the CIP Governance value chain along with stakeholders and their respective roles is put in a relation, as by the following Figure 3, which may demonstrate the interdependency of responsibilities and decision making of different levels of stakeholders and group of processes in the governance structure. Just for illustrative purposes, an example is put for outcomes from the central government point of view/role, through the whole value chain and roles of all the stakeholders and key outcomes in establishing the CIP Governance structure. The main aim of the Figure is to emphasize,in such a very complex and adaptive system, the interrelationship in a national CIP management system that requires interagency cooperation and coordination, which is seen as one of the key challenges in operating an effective and efficient critical infrastructure protection process, contrary to the immanent culture of centralized decision aking within strict hierarchies. (Bordas & Tomolya, 2014[2]).

[2] Critical Infrastructure Protection, M. Edwards (Ed.), IOS Press 2014

H. Sagrak: **Generic control system architecture for CIP**

Organization/ Stakeholders						
Government	CIP Policy	Action Plan	CIP Budgeting	Inspection Procedures	Standard Operating Procedures	Strategy alignment
Government Bodies	Administers competencies					
CI owners	Ownership responsibilities					
National Protection and Rescue Directorate	Establish Governance					
Regulatory Agencies	Administer Policy					
Certified Suppliers	Apply Policy through the supply chain					

Figure 3: Central national CIP management system

CIP Monitoring and Inspection System Functions

Regular conduct of Inspection functions are critical to maintain the desired standards of operations, procedures, activities and respective results. The overall CIP System Architecture has to contain the monitoring and inspection functions. The Government acts through its bodies and competent agencies in order to assure that compliance is maintained and procedures checked. Inspections shall cover the whole supply chain of the CI's, taking into account the results of risk management, especially risk assessment. Therefore, inspection shall target all the stakeholders in the CIP management system, their key processes and outcomes related to CI operations, correction measures to assure prevention of accidents, desired readiness to accidents level and proper recovery after incident. Inspection functions should not be seen as coercive only, but also through knowledge and practice sharing as part of self-assessment procedures by particular stakeholder.

Generic Control and Management System Architecture for CIP

The complexity of CIP concepts, its multidimensional character, local, regional, national and supra-national level and necessary systems approach, rather than sectoral, put demanding requirements to the overall Critical Infrastructure Protection Generic System Architecture – containing elements/building blocks that each per se can be considered as a complex information system.

The proposed architecture, as put in Figure 5, aims to explore the possibilities of combining concepts of process driven and process event control/intelligent control systems along with elements of artificial intelligence based on knowledge management. The CIP system technological infrastructure, therefore, would entail business activity monitoring system in real time, business process and workflow management systems, shared inspection management system, interoperability system (Government Service Bus), community and collaboration system with intelligent control mechanisms. The Industry 4.0 provides new technologies as means to empower the CIP system, e.g. drones, robots, big data analytics, Internet of Things, AI, energy storage.

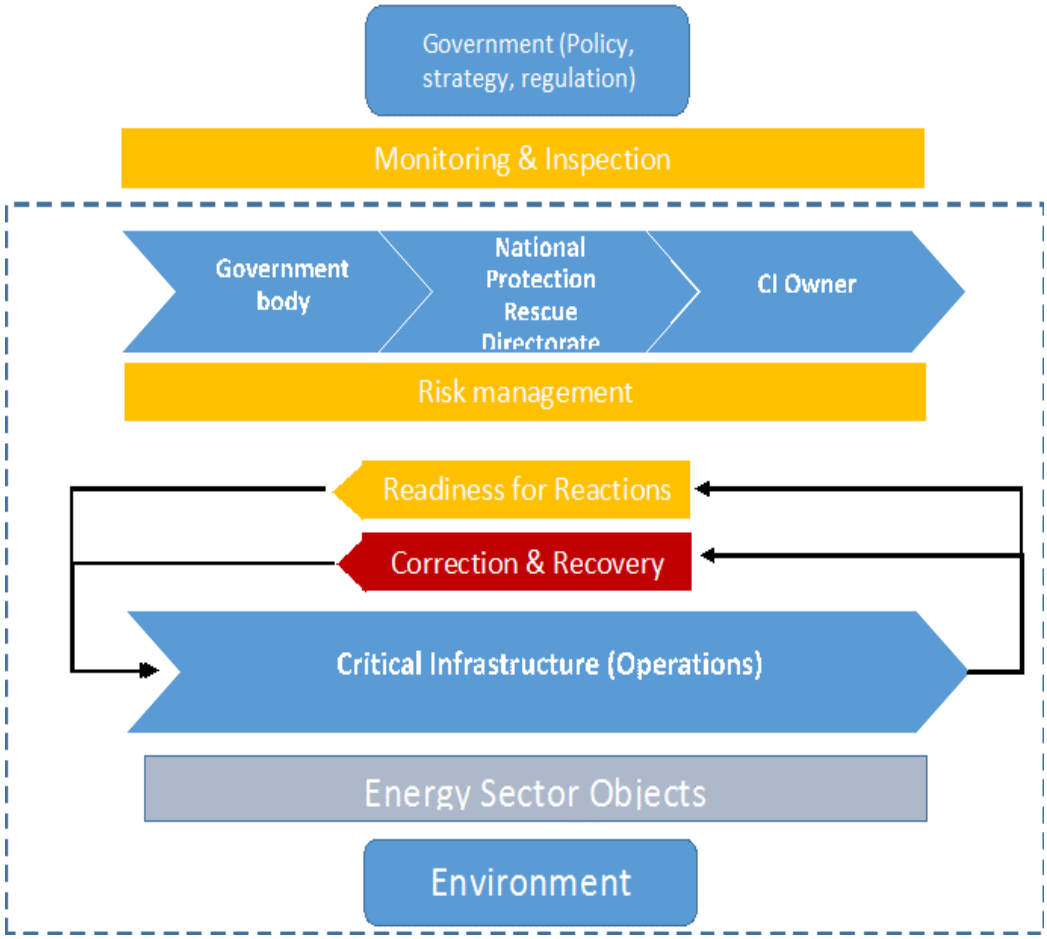

Figure 4: CIP Monitoring & Inspection functions –

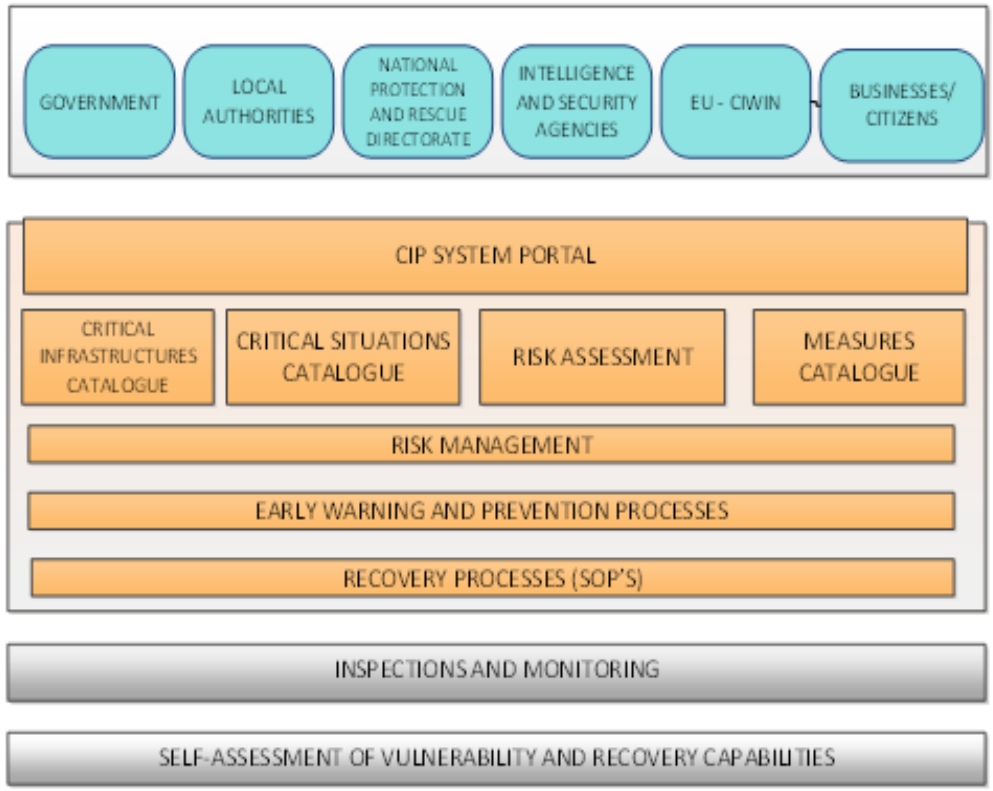

Figure 5: Generic control and management system architecture for CIP

Conclusion

Such system is multilayered and should encompass all the stakeholders with respective roles. In the Figure above, elements from the Croatian regulatory framework where taken into account, with a specific competency of the National Protection and Rescue Directorate. Such system should be integrated with the EU CIWIN (Critical Infrastructure Warning Information Network) in real time or for NON-EU countries respective regional alliance network. Interoperability is assumed through all of the functions and process management system components, as well as with shared inspections. The concept of catalogues would allow intelligent controls through the system. Several main groups of process driven systems cover respective events/situations that are managed.

Due to the complexity, this architecture is aimed to address challenges that are initiated by the Critical Infrastructure Protection regulatory requirements and demonstrate possible responses. It should be explored in practice further, with hope that this article triggers new ideas.

References

1. European Programme for Critical Infrastructure Protection (2006)
2. Directive on European Critical Infrastructures 2008/114/EC
3. Proposal for a Council Decision on a Critical Infrastructure Warning Information Network (CIWIN) {SEC(2008)2701} {SEC(2008)2702}
4. 8/08/2013 - Commission staff working document on a new approach to the European Programme for Critical Infrastructure Protection.
5. 22/06/2012 - Commission staff working document on the review of the European programme for critical infrastructure protection (EPCIP)
6. 31/03/2011 - Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security' (COM(2011) 163 final);
7. 30/03/2009 - Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (COM(2009) 149 final).
8. Law on Critical Infrastructures (Croatian Public Journal, 56/2013)
9. Decision on determining the sector from which the central government bodies identify national critical infrastructure and lists the order of the critical infrastructure sectors (Croatian Public Journal 108/2013)
10. Rules on the methodology for a risk analysis of critical infrastructures conduct of work (Croatian Public Journal 47/2016)
11. Critical Infrastructure Protection, M. Edwards (Ed.), IOS Press 2014