Deep Science Publishing, 2026
https://doi.org/10.70593/978-93-7185-896-0_4

DeepScience
Open Access Books

Chapter 4: Designing Control Mechanisms for Infrastructure Operations

4.1. Introduction

Control mechanisms direct the behavior of complex systems and help maintain system states within desirable bounds. Control mechanisms for power grids, water and wastewater infrastructure, and transportation systems are often tightly integrated with group operation, management, and business control mechanisms. Although set at a higher level, control mechanisms for public organizations, regional economies, society, and the planet typically influence the behavior of such infrastructure systems. The various control mechanisms for different infrastructure systems alter a subset of the inputs into, outputs of, and constraints on the systems under their purview.

Formal control mechanisms are fundamentally monitoring, sensing, decision-making, actuation, and enforcement functions. Control operation covers the procedures used to conduct individual monitoring, sensing, decision-making, actuation, and enforcement activities. Special-purpose monitoring and sensing systems, such as those that cover power consumption instead of production, projection of consequences rather than historical situations, or local instead of global interaction, augment actuator states, information, and logical instructions at other levels.

4.1.1. Power Grid Control Mechanisms

Every power grid is subject to Random and Deliberate disturbances. Control mechanisms design architecture and behavior in a way that the system remains Safe-Operational in the Normal and some other Appropriate states to formalize these concepts in the context of Infrastructure Operations. The identification of Random and Deliberate incidents and Failures and intended behavior (or Coverage of CRFs) therefore precedes defining control architectures, or what the control mechanisms of the considered Infrastructure System are.

Control mechanism operability is at Risk from Random and Deliberate incidents, e.g., fires or floods, hysteresis, traffic accidents, deliberate acts, equipment Faults, and operator errors. The control mechanisms' implementation are however not affected by such incidents (in particular when considering high-impact steep-dip random incidents), nor is their Safe-Operational state (except when communication links are broken), nor the required Behavior when Random Disturbances occur (side events), as this Dependability property refers only to the CRFs Coverage of these commulative disturbances. The combination of Threats and design requirements is the basis for the Threat Model of the Control Mechanism and a first-level design tool within the Security and Risk Management step of Infrastructure Operations.

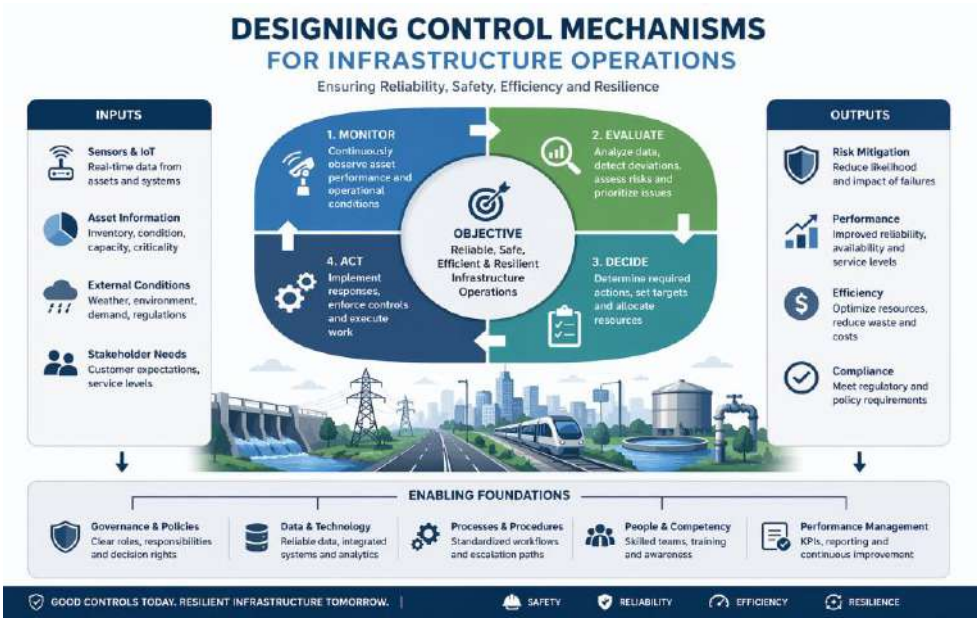

Fig 4.1: Designing reliable infrastructure control systems

4.1.2. Water and Wastewater Infrastructure

In the water and wastewater infrastructure domain, control perspectives have been overwhelmingly on process control at the plant or facility level. Supervisory control systems have been proposed to coordinate the control of geographically-distributed, coupled water supply control and treatment systems across a region, driven by water demand patterns or moving threats such as contaminants or floods. At a higher management level, modeling supported by decision support systems has been suggested to provide guidance for a portfolio of operational decisions over a longer time horizon. Many important tasks require such coordination across facilities: large-scale water quality monitoring and monitoring systems, risks from climate change and urbanization,

management across a portfolio of water delivery and treatment facilities, including water quality development; and the exploration of potential benefits from port facility cooperation in new situations.

In recent years, there have been efforts to conceptualize control of urban flooding and water in general from an integrated, holistic, system-of-systems perspective; to study control of wastewater systems from this same perspective, such as watershed-based integrated flood risk management encompassing urban drainage, or to begin developing a control and management layer for water systems from such a perspective. No literature currently synthesizes these control perspectives of the many facets of water and wastewater infrastructure as a whole, but synthesis becomes essential to the realization of control that provides, ultimately, improved public safety, sustainability, quality of life and national security from flood-driven hazards.

4.1.3. Transportation and Urban Mobility Systems

Control mechanisms are equally important for transportation systems, particularly for mobility. This involves providing information to users so they can behave in a way that optimizes the system's performance. These mechanisms must be designed as a system-of-systems that takes into account not only the traffic network but also transit and freight transport. Users can behave optimally if they know the expected state of the system and can easily exchange that information. This is particularly true for traffic where localized congestion can be very dynamic and where optimal response times are very sensitive to current and predicted conditions.

Providing a model of optimal behavior requires a prediction of the state of the system, and short-term prediction relies heavily on real-time information. When a small part of the traffic network is congested, the drained traffic generally re-routes quickly. In this context, the predictive model must include an estimation of the response time of the last user. However, the performance is better if warning signals are given to the user. On longer time scales, transit and freight services should be included within the same control mechanisms that provides guidance to all users. These entities are requested to run in the most efficient way possible, but without the traffic congestion their operation is not optimal. Thus, new models that analyze the system from a whole perspective are required and should be included too.

4.2. Foundational Concepts in Infrastructure Control

Infrastructure control mechanisms are a central aspect of operations. Such mechanisms direct, regulate, and facilitate infrastructure and system-of-systems operation and

interact with user- and provider-operations. This section proposes a brief vocabulary for discussing these mechanisms, outlines key stakeholders and their roles, and describes technical management, operational management, and business management from a system-of-systems perspective.

Two sets of definitions are relevant: the first describes the concepts of monitoring and control, while the second describes the activities of management B. Monitoring and control are the pulsation of complex technical systems. Operations are activation and the use of the monitored multilayerized technical system by an operator that realizes the actual functioning processes of the monitored objects through a controlled actuation of a wide variety of actuating subsystems embedded into a monitoring system itself. Different layers of monitoring and management of the transport system and the state of highest importance and responsibility are termed management, operations management, and technical operations management, respectively.

4.2.1. Definitions and Scope

Infrastructure operates and delivers services based on complex process models, leveraging characterizations of the domain space for planning, monitoring, and control. Internal control mechanisms implement condition monitoring, anomaly detection, localization and identification of failures and perturbations, decision-making regarding corrective actions or adaptive behavior, and enforcement. These are common and sometimes mandatory for many technical systems. Additional requirements emerge when considering infrastructure, wherein constituent systems and systems of systems must deliver services for supporting economic and social activities. System control constitutes an area of active ongoing research, and forming a clear and comprehensive definition is challenging due to field-specific peculiarities. Control mechanisms are about how systems behave when everything is okay, whereas safety mechanisms deal with controlling when everything is not okay.

Infrastructure control mechanisms can be described by their functional and non-functional requirements, the architectural patterns they conform to, and the interfaces they provide. These control mechanisms are commonly formalized as a set of functions that provide monitoring and sensing, decision-making and automation, actuation and enforcement, performance avoidance, and behavioral uniformity of the system through suitable control-oriented models. Control mechanisms relative to safety and security are special cases of such functions that ensure the infrastructure can continue to provide its service without putting system users or third parties at risk, particularly when such behavior is essential.

4.2.2. Key Stakeholders and Roles

Several key stakeholders are directly involved in the design of a control mechanism for a collective infrastructure operation, namely the infrastructure operators, the infrastructure users, and a Federal authority governing the infrastructure operation. Other stakeholders, such as the service providers (for transport services, etc.), the insurance companies, etc., may also play an indirect role in specifying the control mechanism.

Infrastructure operators. These are public or private entities that own, operate and maintain the infrastructure networks (in transport, for example, rail, air, urban transit, etc.). Some of them act as monopolies (despite being regulated), and they have an incentive to optimize the operation of their own infrastructure, but not necessarily of the whole infrastructure system. For this reason, they may or may not support (or invest in) the creation of a control function. Some operators are privatised (air transport) and thus their main objective is profit maximization, which can lead to less-than-optimal outcomes from an overall infrastructure point of view.

Infrastructure users. These are the individuals and corporations (including logistics and transport companies) that use one or multiple mode(s) of transport. Each of these users may express preferences about quality of service, and may decide to choose one service over another based on these preferences. Typically, users are willing to pay more for better quality of service. Consequently, users are key stakeholders in the design of a control system for collective infrastructure operations. These users benefit from the avoidance of the tragedies of the commons (e.g., a too-long queue at an airport that leads a user to miss a flight, or congestion at a transport medium that leads to excessive delays at a particular leg of the journey), and they are also ready to pay to avoid that. The users may also select a service provider, in the case of air transport, and their adherence to a particular airline may help in bridging over a trade-off between time and cost.

4.2.3. System-of-Systems Perspective

Infrastructure systems are characterized by a high degree of interrelatedness of their components and the external environment. Water distribution infrastructure is intertwined with energy grids, transportation and mobility systems, wastewater systems, and telecommunication networks. The interactions and interdependencies of such systems reach a level of complexity that leads to their classification as a system of systems. The relationships among different systems are classified into three categories.
• User-relation: different systems are usually managed by different authorities, but the users are usually the same. Their behavior, e.g. traffic flows on different roads, is correlated and has serious consequences on the efficiency of each system. • Environmental-relation: a particular system is indeed the solution for other systems that

are poorly behaving. Roads can be flooded, but the transport can rely on airplanes; airports can be connected with the telecommunication system, bypassing the problems of the transportation system. • Geographical-relation: different systems are usually built in the same area and is natural to use the same area to accommodate different infrastructures. At a geographical level, more than one point of view is needed, to optimize the positioning of each system, for example the position of airports and harbors are strongly correlated.

4.3. Architectural Patterns for Control Mechanisms

Several architectural patterns have been observed when designing control mechanisms for different types of infrastructure operation. First, centralized- control elements are a proven concept that, if recognized as appropriate to the task at hand, allow for development with minimal customization. Yet potential drawbacks, such as single points of failure, concentration costs, or lack of adaptability need to be accounted for at design time. The state of centralization of the observed control element, whether being a pure central control, or such centrally coordinated sub-controllers operating in a federated manner need to be clear in the design. For instance ticket sales for urban public transportation can easily be centralized in a finite capacity manner, online, and distributed in a mobile capacity manner, thus can serve to reduce congestion on the local ticket booths. However management of traffic lights, public transport priority systems, traffic accidents and such within a specific area would require a more distributed or federated approach. For autonomous driving vehicles, provided the roads are clear, an easy direct control mechanism is to allow the vehicle to travel to its destination without input. Such a central command when allowed to be at each vehicle would then run in a federated mode. But should the road become congested, a more centralized infrastructure coordination of these vehicles to reduce congestion should come into play.

Second, there are many established control elements that react automatically to the observed state of the infrastructure. These event-driven mechanisms can be combined with centralized, decentralized, or federated approaches, further increasing the contextual build and use of the mechanism.

4.3.1. Centralized Control Architectures

Centralized control approaches are based on a single, dedicated control platform where monitoring, decision-making, and actuation functionalities are designed to be implemented. Depending on the application domain, centralized control mechanisms can also coordinate related operations across multiple infrastructures. Unlike conventional SCADA systems, modern implementations are expected to support a rich set of quality

attributes, including performance, security, scalability, and resilience. The system is expected to provide primitives for continuous, real-time, and continuous-time operation, as well as event-driven capabilities to be invoked in emergency situations.

Conceptually, their architecture resembles the layered structure of an information system, where monitoring and actuation functionalities are typically associated with the lower layer, decision-making functions with an intermediate layer, and the infrastructure being controlled with the upper layer. On the one hand, this structure reflects management hierarchies of infrastructural operations event-driven and emergency functions typically involve the highest tier of management and human-aided decision-making on whether to act, while primitive and replanning functions are usually delegated to lower tiers. On the other hand, it also reflects the temporal evolution of structurally dichotomous primitive and replanning functions, which can be solved in parallel and are encapsulated in the notion of system dynamics.

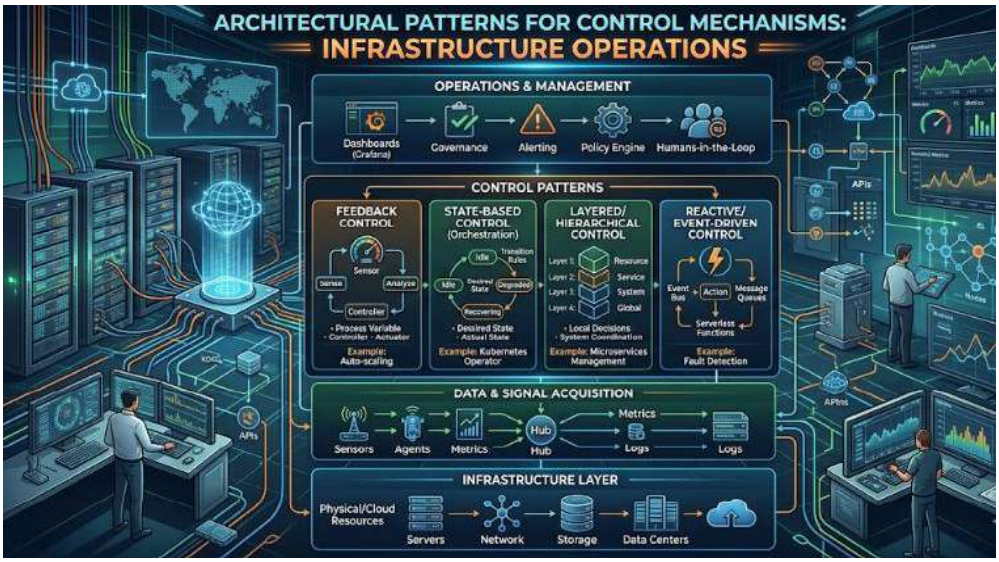

Fig 4.2: Control mechanisms architectural

4.3.2. Distributed and Federated Control

Two decisive factors underline the limitations of centralized control systems in large-scale infrastructure facilities. First, the existence of multiple independent authorities or owners, whose assets may need to be managed in coordination with other entities. A prime example is the transportation infrastructure of every metropolitan region. Dedicated operators control the networks of roads, railroads, subways, airports, and sea ports, and sometimes the operation of the corresponding vehicles; but major events in one sub-system can cause significant disturbances in the others. The case of a major

storm at a metropolitan region during holiday seasons, forcing a significant reduction of air traffic in and out of the area, is emblematic for the types of coupling among the sub-systems.

Second, the scarcity of real-time information for the entire process, or that of a single authority that can accurately visualize the state of the whole process. A similar event causing disturbances in the travel time of a road segment can go unobserved by the operator of the transportation system, either because their area of operations extends beyond those in which the situation is taking place.

4.3.3. Hybrid and Event-Driven Models

Hybrid control architectures combine elements of centralized and distributed solutions as appropriate, leveraging the advantages of both approaches while minimizing their disadvantages. Event-driven architectures seamlessly integrate active management and regulation, triggering responses to deviations from normal operation even in the presence of self-organizing components.

Event-driven management in infrastructure systems relies on two key components: the ability to detect significant deviations from normal state or behavior, and the capability to automatically implement necessary corrective actions. These capabilities can be expressed together as a declarative specification of control or management rules, monitored and enforced through a rule engine. Although this approach is especially useful in open dynamic environments, it does not supersede other forms of infrastructure management. Event-driven control is applied alongside, rather than instead of, a centralized view. A well-defined set of exception scenarios, which may arise in highly stable conditions but with a low probability, is continually monitored. Response rules are defined, either as a one-off operation for simple scenarios, or using model-checking or similar mechanisms for complex scenarios.

4.4. Functional Requirements for Control Systems

Control mechanisms help steer data and actuation through the infrastructure system-of-systems in a safe, secure, and resilient manner to meet operational objectives for the individual infrastructures and for the infrastructure portfolio as a whole. The three principal classes of functional capabilities that control mechanisms must support are monitoring and sensing, decision-making and automation, and actuation and enforcement.

The control mechanism must monitor the data streams flowing into and through the control mechanism, and it must ensure that these data streams are properly fed by

adequate sensing or monitoring within the infrastructures. Major hazards, security threats, and resilience risks can often be detected only on the basis of infrastructure system behavior, that is, by modeling or simulating likely effects, and the control mechanism must therefore support such monitoring, where possible. Infrastructure systems are complex, interconnected, and highly engineered; they are constantly generating and responding to data, but they usually lack true intelligence and situation or command awareness. Innovations in machine learning, artificial intelligence, and analytics therefore offer promise for developing real-time or near-real-time automated decision-making and operational support capabilities within individual infrastructures and portfolios of infrastructures alike, and the control mechanism must serve as a platform for these innovations. Suffering infrastructure systems provide multiple opportunities for such automated decision-making and for supporting humans in the decision-making loop, but such opportunities must also be fed back into the infrastructure systems in order to continue to operate within acceptable risk envelopes even under stressful conditions.

4.4.1. Monitoring and Sensing

Monitoring and sensing are foundational functions of any control mechanism. An effective monitoring subsystem must be able to identify system events and states that are relevant to the decision-making process of the control mechanism and can trigger the initiation of the control logic. This typically requires a set of different types of sensors and monitors that can infer along different dimensions. Collectively the deployed sensing and monitoring system must ensure that the hazards and events that could lead to safety, security, performance, and resilience violations can be detected within a time frame that supports timely decision and actuation.

Monitoring and sensor data is often uncertain or incomplete. Uncertainty can arise from the sensor, algorithm, or process itself. Distributed judgment methods, such as the Dempster–Shafer theory of evidence, can help fuse data from multiple imperfect and uncertain sources for making better assessments. Missing data can also complicate decision processes. A model can suggest the expected values when data is missing, thus improving the decision-making process in such cases. The failure of components in a critical monitoring path may hinder the ability of the control mechanism to initiate fast decision making. Therefore redundancy in critical paths can improve system operation and support a high level of reliability and performance.

4.4.2. Decision-Making and Automation

Appropriate decisions, made at the right time, have a significant impact on the effectiveness and cost of operating systems. Decisions can be planned (made periodically, e.g., optimal sensor allocation and selection of sampling frequencies) or in real-time with less anticipation of future disturbances. Control mechanisms may provide full (automated) actuation, or a degree of human-in-the-loop interactions where suggestions or options are presented to the operator without any guarantee that they will follow these suggestions.

In many cases, operating decisions require both human and automated inputs. Virtual supervisors, either single agents or, more frequently, part of a multi-agent environment, can interact with human operators and other supervisory entities of other infrastructure systems. Basic control strategies such as proportional-integral-derivative (PID) control have a long history in the literature. More advanced predictive and optimal control solutions have received increasing attention. Event-driven automation solutions allow supervisory control only on specific situations (e.g., under certain disturbances), reducing the load on operators while keeping a high-level supervision.

4.4.3. Actuation and Enforcement

In addition to the monitoring and analysis functions described in previous sections, control mechanisms need direct means to reliably enforce actions in the real world. In sociotechnical systems, enforcement mechanisms typically achieve this by coordinating the activities of professionals and companies that operate the physical infrastructure or provide the supporting services. For example, traffic-light regulation requires close cooperation between traffic planners and regulatory agencies, which decide the timing of red lights based on historical patterns of congestion. In emergencies, e.g., at the outbreak of floods, natural disasters, major accidents, etc., traffic authorities may take decisions to prevent access to certain parts of the city.

Important requirements pertain to competency, preference and capability. Individual actors are best suited to making decisions when those decisions are in their own self-interest. But some actors not only need to make decisions that go against their self-interest, they may even need to shoulder an unfair burden for the common good. For example, during an epidemic, the government may close schools not only for health-safety reasons but also to allow a reduction in the street congestion created by the rush hours (several families dropping/picking the kids at school). Similarly, although tourism authorities may dislike a regulation ordering to prohibit tourism for specific periods, it may still be justified for the prevention of greater losses. The decision to authorize such

an exceptional regulation is therefore likely to be in the best hands when a set of actors (the government) with a strong sense of common-good, can take such decisions.

In more complex systems, where individual situations tend to have both strong localized effects while at the same time coupling with other systems, decision support for timely and coordinated decisions can be useful. These situations tend to be rare and short, but can benefit from a rapid response (e.g., major accidents). Decision support can also help where actors should collaborate to improve the result for all but are normally tempted to consider only their local gain. For instance, a temporary admission restriction in the touristic areas during peak periods may inconvenience tourists and local economies, triggering opposition from both groups, even if the overall gain makes the interference positive. In these cases, providing a decision support that improves the net effect for the entire city (with the actors participating in the decisions) may help achieving an overall better performance.

Two main aspects should also be considered in the decision-making process during emergencies. On one hand, changes taking place across cities or airport areas and their mutual relationships can influence the situation (e.g., a storm or a strike in a central city may indeed force to close all airports, even though the event might last hours in just one city). On the other hand, the solution developed for a local area may also be transferred to main neighbouring cities. A temporary stop of flights to certain Turkish areas during the last war evidenced that some decisions can be made very quickly by neighbouring cities participating in a solution pool for those exceptional events.

4.5. Non-Functional Requirements and Quality Attributes

The functionality of control mechanisms for infrastructure operations is assessed not only in terms of capability. Non-functional requirements encompass a diverse spectrum of qualities, such as usability, performance, reliability, resilience, and security, which apply to all forms of digital systems. Infrastructure control systems incorporate a set of unique attributes that have critical importance for the safety, security, and resilience of vital economic and social systems. Systems must remain secure, available, and operational possibly in degraded mode even under extraordinary operational conditions associated with natural catastrophes or terrorist attacks. To achieve this, responsibility and accountability must be assigned to specific organizations. Operators need to devise and enforce policies involving the execution of emergency plans by other stakeholders throughout the system-of-systems.

Infrastructure control systems must enhance monitoring, detection, and response capabilities, while increasing mission assurance and risk management in the event of an attack, accident, or failure. Continuous operation must be guaranteed even in the

aftermath of such incidents. Occasional reconfiguration or a switch between primary and backup operations should maintain functionality with minimal disturbance, focusing on organizational procedures, logistics, and risk assessment, rather than additional redundancy in hardware and software. Sustainable public-private partnerships are also crucial; external support can enable rapid recovery from failure, while private-sector expertise can enhance security without losing focus on the underlying infrastructure operation and maintenance business.

Fig 4.3: Non-functional requirements for control mechanisms

4.5.1. Reliability and Availability

Systems that support infrastructure operations need to meet high availability and reliability requirements. They are usually critical systems that must continuously operate. However, outages do happen due to failure in data collection, analysis, or generation, or due to communication problems preventing the transmission of warnings or decisions. These outages need to be managed. For example, when a failure happens, operators or automated processes may have to rely on alternative or redundant data sources or revert to a manual control mode. Nevertheless, the outage windows need to be small: automated processes may perform manual tasks but with lower quality and at greater costs.

Reliability is the ability of a system to perform a required function under stated conditions for a specified period of time. Aspects related to reliability and availability that are of particular relevance for control mechanisms include: (1) requirements that explicitly define acceptable levels of reliability and availability, as well as maximum tolerable downtime; (2) failure modes and effect analysis (FMEA) for communications

to assess the effects of outage of the various data sources (sensors, models, and historical data) and decision outputs; and (3) evaluation through simulation or modeling of the system operations of the directives issued by the control mechanism in the event of failure of one or more data sources.

4.5.2. Performance and Scalability

How a control system's ability to manage traffic may degrade when a network is saturated, and how this spatially non-uniform performance can hinder functioning across geographically distributed systems.

A major problem for the management of critical infrastructure is that the observed behaviour of a control system may change depending on traffic load. For example, in transportation systems, when traffic load is low, a large control reserve exists, so that the control algorithms can keep each of the roads at its nominal load ratio level, thus optimizing the entire traffic and providing a globally low travel cost (delays). On the contrary, when the traffic load is near maximum, the control management approach often turns helpless. Notably, this important criterion can be missed when several road networks in different cities are considered as a whole. Indeed, the performance of a city's traffic control can be studied separately, and hence an excellent performance can be confirmed for all cities when analyzed in isolation. However, when the attention is shifted to the entire area of operation, the conclusion may change because the combination of the traffic-control systems of the individual cities may not suffice to ensure that no city experiences an excessive level of inhabitants' discomfort.

The concept of performance as a quality attribute indispensable for assessing the suitability of the control mechanisms that regulate the operation of any critical infrastructure is thus essentially interconnected with another concept of a criticality strongly linked to the safety level. Both are closely related to the quantification of the probability of failure of the overall infrastructural network when a disturbing event occurs. In fact, if the software evenly distributes the offered load during normal conditions in the monitored area, all critical infrastructure can be safely downgraded and robustly managed under a joint management methodology.

4.5.3. Interoperability and Standards

Interoperability between component-software systems is a major enabler of modularity, composability, plug-and-play capability, integration and repairability. It is driven by multiple factors, including technical, market and political factors. Standards address both formal and de facto requirements for interoperability.

A standard in computer science is a prescriptive document that describes interconnections, interfaces and formats, encoded behaviors of one or more operation specification, the information and data exchange that can appear on those interfaces. Standards deal with terminology and words for the description of issues and technology and describe the expected behavior of the different systems. Standards provide reference models and architectures. Standards are normally made available to the entire developer community. Standards are a result of a multilateral consensus and offer a declaration from the community about how things should interoperate. Standardization enables the creation of a product family, integration, fast development and installation, and a cost-effective evolutionary approach.

Standards may affect the following references: public policy, creation of products and services, establishment of reference models, market coverage, migration across generations or products, efficient communication and implementation of technologies. For large complex systems, de facto or formal standards exist for key middleware technologies, e.g. sensors and actuator networks, telecom integration and internetworking technology.

4.6. Data Architecture and Analytics

The design of control mechanisms for efficient operation of critical infrastructure systems relies heavily on the availability, quality, and analytical treatment of data. Data architecture covers the creation, collection, and storage of such data, and encompasses the associated processes for preparing it for control operations. The quality of the collected data directly affects the accuracy of predictive modeling, in turn impacting the performance of the control mechanisms.

The monitoring and control of infrastructure systems requires the collection data from distributed environments, often using a variety of sensors. The resulting data are monitored for quality and accuracy throughout the process of data preparation, from assimilation, cleansing, and integration, to storage and utilization by control systems. For predictive control functions, both generalized and specific models are generated through simulation-supported data analytics, and then updated in real-time operations using feedback from Kalman filters or other statistical techniques.

4.6.1. Data Collection and Quality

Designing control mechanisms for major infrastructure operations power, water, wastewater, and urban transportation requires the use of new digital technologies and software, as well as key function patterns. A supporting resource is a taxonomy of

system-of-systems (SoS) architecture for real-time monitoring, decision-making, and automated enforcement of safety and operational requirements.

Control systems must assure the quality and utility of the data they exploit. Control invariants define the required properties of the system-of-systems, with major events triggering data-collection patterns that assure the quality needed for both real-time and long-term operational decisions. Control-modelling solutions can augment operational models that concentrate on short-term events, while real-time data-analysis solutions can assess safety and security at all times, even in the presence of uncertainty. North American electrical technology and telecommunications standards provide examples of control-data quality for SoS-type applications.

Control mechanisms for major infrastructure operations confront research design based on new digital technologies and methodologies that improve resilience, availability, and performance. Recent responses to control-response requirements exploit digital technology attributes that permit resources to function as decision-making and decision-acting mechanisms. Examples include power grid-information events that record and detect unsafe conditions. Resilience ensures service availability during natural physical disasters, avoided through interoperation with complementary services. Other requirements apply control to enhance performance, such as daily traffic management to minimize journey time. Transport SoS control technology directly supports performance-requirement fulfilment by permitting vehicular access to cities with scheduled travel windows.

4.6.2. Modeling and Simulation for Control

Effective functioning of infrastructure depends heavily on the support from actuators and devices contained within the infrastructure operation domain and their capabilities to detect system-wide emergencies and performance-degrading situations. These devices support real-time data acquisition on the current operational state of narrow subsets of the infrastructure. However, the information collected is not sufficient to make adequate real-time decisions and the strategic planning decision-making activities. Performance-degrading situations tend to have a broad impact on the functioning of the infrastructure and need to be reliably predicted before the symptoms become evident. The overall operational state of the infrastructure system cannot be optimally represented solely by the monitoring capabilities of the actuators and devices of the operation domain, and it is essential to recover the missing information from data-driven, agent-based, and/or dynamical-system simulation models. Agent-based and dynamical-system simulation models need to be complemented by data of a high volumetric resolution and quality to enable their effective use and to deliver qualitative and/or quantitative declaration of

developing performance-degrading situations that incorporates transient, progressive, and near-catastrophic condition phases.

Real-time analytics applied to the high-frequency volumetric data is essential for rapid and accurate diagnosis of actual system states and for expeditious support-system decision-making activities in critical situations. Up-to-date information about the actual operation state is necessary to feed the hardware/software resources that constitute the various control mechanisms supporting the preventive, predictive, and corrective control paradigms. The manner in which real-time operational data conditioning is performed influences the response time of the centralized system, and dynamic calibration, tuning, or retraining and assessment of the models forming the various control mechanisms is mandatory.

4.6.3. Real-Time Analytics and Feedback

The ability to sustain real-time functioning at the system level requires support for real-time analytics and feedback of real-time information. To control a complex and dynamic system of systems in stressed or emergency states, real-time analytics are essential. Control and operation mechanisms for such systems need richer datasets for real-time analytics, including support for high-volume, high-velocity data from facing infrastructure, such as traffic monitoring systems for the road network, monitoring the charging status for vehicle charging stations, and monitoring other "fast" services in the road mobility region. Such datasets eventually aid transport engineers in monitoring incidents and forecasting congestion.

Real-time analyses require timely data, inferring monitoring states of the complex system of systems and subsequently driving contingency safety measures. Real-time analyses are not only beneficial but indispensable for safety when a system shifts to risk zones. Historical and lower-velocity datasets support higher-level analysis for critical monitoring and control push of control actions. Automation plays a role in detecting when the critical alarms are reached for manually supervising system states; otherwise, it should be a human supervisor decision.

4.7. Security and Risk Management

Critical infrastructure operations demand effective security risk and privacy management strategies. This is particularly true for control mechanisms. Cyber-physical systems, which are an increasingly important class of systems for critical infrastructure, utilize the Internet not only for monitoring and command and control applications but also to control physical and alternative resources that have real consequences in the

physical world. Consequently, the risks associated with management of critical infrastructure become of utmost importance.

Threat modeling identifies the potential areas of risk within a system that may lead to an exploitable vulnerability. Consequently, threat modeling is a requirement of the control mechanisms of any critical infrastructure ecosystem engaged in governance and operation as well as any data and analytics capability implementing real-time control. Risk and privacy management involves both establishing privileged roles within data systems and control for critical infrastructure and developing methodologies to limit access to sensitive personal data. Access control methodologies and systems connect users to services offered by a data source such that a user is granted access only to resources to which he is authorized for a defined purpose while preventing unauthorized data breaches.

4.7.1. Threat Modeling for Control Mechanisms

In the design of any control mechanism, threat modeling is an essential early step in laying the groundwork for an effective security posture. Control mechanisms include sensing, actuation, decision-making, and enforcement. In functions that range across multiple infrastructure systems (e.g. cascading failure), threats should be modeled collectively. In functions with a dual role, like human operators, common threat models can significantly simplify security engineering. For example, the human operator function is both a threat (a malicious insider) and a responsibility (accidental misuse, etc.). Behavioral ethos and professionalism of such users should be explicitly accounted for in design.

Although the control function generally has access all areas (of infrastructure), a policy of least privilege can be applied. For example, if the control mechanism is temporary as in the case of a flooding warning system, then during normal operation it should not have access to the flood control channel. Sensitive actions should also be temporally restricted to reduce the chance of the clandestine qualification of all controls.

4.7.2. Access Control and Identity Management

The concepts of identity management and authorization have received considerable attention in the literature, and the task of creating a control structure with the focus of identity management, authorization, and enforcement in a distributed setting, where different organization participate to a common goal is a fundamental requirement. Such task is crucial in transport systems, where different infrastructures are managed by

different authorities that do not necessarily share same technology but execute a main track and signally also transversal operations.

4.8. Conclusion

Systems of infrastructure for mobility, water distribution and treatment, and electric power are now entering a new phase of operation. The latest generation of real-time operating systems for these installations has been designed to enable proactive performance during routine operation, and to facilitate operational control and intervention when major disturbances occur. Such coordinating and control capabilities are desirable and essential for the safety, health, and welfare of citizens and the effective functioning of the economy. These systems, often viewed as “control mechanisms” for the operation of the constituent infrastructures, comprise the end-to-end collection of sensors, software, and hardware that detect threats and instabilities to system performance, and effect the responses needed to return the combined systems to their preferred operating conditions.

A systematic analysis of these control mechanisms in support of infrastructure operations furnishes functional requirements for their design. Monitoring and sensing capabilities provide the information needed to assess the state of the constituent infrastructures. Decision-making and automation functions identify and activate the appropriate corrective response. Actuation and enforcement capabilities activate response measures ranging from system restoration following a major disturbance to routine functions such as traffic signal switching for congestion mitigation that are implemented within and across the constituent infrastructures.

4.8.1. Future Trends

Important trends in these systems indicate an intensification, a greater interest, or enhanced influence of a given phenomenon. The most significant of these trends are presented below.

Infrastructure systems are receiving greater attention and support from governments and funding agencies. Investments for new infrastructure are essential to keep pace with community growth, urbanization, and economic development. At the same time, existing facilities are aging and require sustained capital for operations, maintenance, and replacement. Communities need to manage these assets over their life cycle; to do so efficiently, infrastructures must be adequately operated, monitored, and maintained.

Consequently, the need arises for control mechanisms to assist operators in their daily tasks. Control mechanisms can be defined as the set of procedures, hardware, and

software involved in the sensing, decision-making, and actuation of the infrastructure system in order to achieve predefined goals such as reliable operation or reduced cost. Control mechanisms can also be viewed as the control structures of the large-scale engineering systems that are deployed to serve the needs of society and to fulfil the missions of stakeholder agencies and organizations..

References

Karl J. Åström, K. J., & Richard M. Murray (2010). Feedback Systems: An Introduction for Scientists and Engineers. Princeton University Press.

Gene F. Franklin, J. David Powell, & Abbas Emami-Naeini (2015). Feedback Control of Dynamic Systems (7th ed.). Pearson.

National Research Council (2012). Disaster Resilience: A National Imperative. National Academies Press.

Henry Petroski (2012). To Forgive Design: Understanding Failure. Harvard University Press.

ISO (2018). ISO 55000: Asset Management Overview, Principles and Terminology. ISO.

Erik Hollnagel (2014). Safety-I and Safety-II: The Past and Future of Safety Management. Ashgate Publishing.

Paleti, S., Kummari, D. N., Garapati, R. S., Sheelam, G. K., Adusupalli, B., & Singireddy, J. (2025, December). Building a Cyber-Resilient Payment Infrastructure: Transforming Payment Security with Zero Trust Architecture. In 2025 3rd International Conference on IoT, Communication and Automation Technology (ICICAT) (pp. 1-7). IEEE.

Andrew Haldane, A. G., & Robert May (2011). Systemic risk in banking ecosystems. Nature, 469(7330), 351–355.

Mahesh Recharla, (2020), "Targeted Gene Therapy for Spinal Muscular Atrophy: Advances in Delivery Mechanisms and Clinical Outcomes", International Journal of Science and Research (IJSR), 9(12), 1921-1934. https://dx.doi.org/10.21275/SR20126161624, https://www.ijsr.net/getabstract.php?paperid=SR20126161624

National Institute of Standards and Technology (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). NIST.

Agrawal, S., Kumar, S. N., Singh, D. K., Sai Niharika, D., Nandan, B. P., & Asati, D. (2025). Dynamic Access Management and Authentication Mechanisms for Enhancing 5G Security Against Heterogeneous Adversaries. In 2025 IEEE 5th International Conference on ICT in Business Industry & Government (ICTBIG) (pp. 1–6). IEEE. 2025 IEEE 5th International Conference on ICT in Business Industry & Government (ICTBIG). https://doi.org/10.1109/ictbig68706.2025.11323683

Elena P. Paté-Cornell (2012). On “black swans” and “perfect storms”: Risk analysis and management when statistics are not enough. Risk Analysis, 32(11), 1823–1833.

Martin van Creveld (1985). Command in War. Harvard University Press.