

Study on Timing Failures in Cyber-Physical Systems

Joon-Ik Kong

Principal Researcher, Telecommunication Technology Association, Korea
joonik2000@gmail.com

Abstract

Cyber-physical systems (CPSs) can solve real problems by utilizing closely connected resources in the cyber world. Most problems arise because the physical world is uncertain and unpredictable. To address this uncertainty, information pouring from numerous devices must be collected in real-time, and each interconnected device must share the information. At this time, CPS must meet timing-related techniques and strict timing constraints that can deliver accurate information within predefined deadlines in order to interact closely beyond simply connecting the cyber and physical worlds. Timing errors in safety-critical systems, such as automobiles, aviation, and medical systems, can lead to catastrophic disasters. In this paper, we classify timing problems into two types: real-time delay and synchronization problems. The results of this study can be used in the entire process of CPS system design, implementation, operation, verification, and maintenance. As a result, it can contribute to securing the safety and reliability of CPS.

Keywords: *Cyber-Physical Systems, Timing, Real-Time, Safety, Reliability*

1. Introduction

In CPS, various technological elements such as sensing technology, analysis technology, optimization technology, and control technology must work organically and converge [1-3]. In the process, not only will the system grow in size, but the structure may become complex and unintended problems may arise. This increases the probability that there is a potential cause that could cause a glitch or malfunction of the software, which can harm the safety and reliability of the system. A latent defect is not a simple failure due to the nature of CPS but directly affects the real-time changing physical environment, causing enormous damage to human life and property. In fact, an autonomous vehicle, a representative example of CPS, was unable to measure changes in the environment around the vehicle in real-time, resulting in human casualties [4].

CPS timing is the property that connects the cyber and physical worlds in real-time. In the past, it was a system that processed only one function, but recently, to perform one function, it is a structure in which several subsystems perform distributed processing, information sharing through a network, and real-time service provision. It becomes a very important factor. In addition, in CPS, since numerous heterogeneous devices have a complex structure, it is most important for each device to perform the real-time operations in the same time system in order to provide a smooth service.

Although user demand for real-time service of CPS is continuously increasing, research on securing safety and reliability is insufficient. In this paper, problems related to CPS timing errors are dealt with and a case analysis is performed. As a result, the safety and reliability of the CPS can be secured by predicting timing problems that may occur in the process of designing, implementing, operating, verifying, and maintaining the CPS and establishing countermeasures.

2. CPS Timing

2.1 Time Constraints

The components of the CPS should fully consider the following time constraints [5-8]. First, time is a common property of computing and physical systems, but due consideration is needed to enable CPS to operate organically because the concept of time covered by each is different, such as dealing with discrete and continuous times. Second, the components of CPS must be geographically distributed and installed with heterogeneous devices, so that absolute time and relative time can be handled at the same time. If this restriction is not considered, it will be difficult to determine the order of time when producing results by combining data collected from multiple devices. Third, errors should be detected and corrected in advance with preliminary verification of timing requirements so that CPS can complete tasks in a timely manner. Large systems such as CPS cannot be developed by a small number of developers alone and must be collaborated by a large number of developers. Since each developer develops only his or her development module intensively, it is difficult to predict timing issues that arise during interaction with modules developed by other developers. Furthermore, timing problems in the system can be discovered only when all subsystems, including hardware, are integrated into one, and then a complete execution cycle is checked, resulting in huge timing-related error correction costs. Fourth, devices that provide real-time services require shorter processing latency as they are closer to the real world (physical world), and the farther they are, the richer the resources and performance, and the more relaxed the timing constraints. In addition, time constraints according to various situations and conditions should be considered, such as timing elements (finishing time, scheduling, etc.) being perfectly matched like cogwheels to enable smooth information exchange between components.

2.2 Classification of CPS Timing Errors

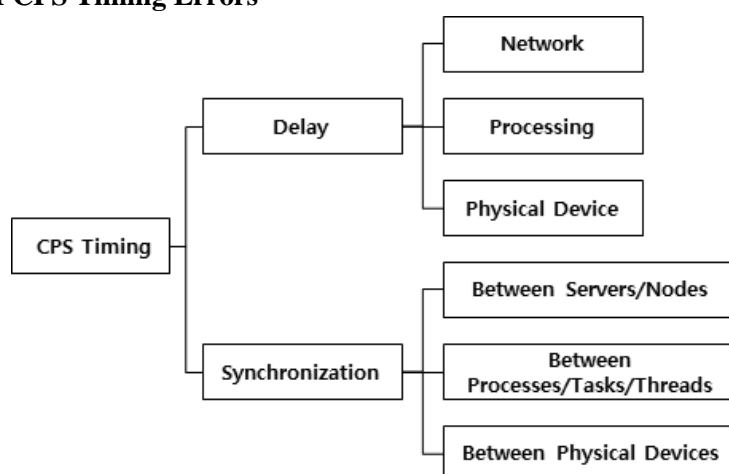


Figure 1. Classification of CPS timing failures

CPS timing errors were classified as shown in Figure 1. This classification helps to detect CPS timing problems that systematic thinking may miss due to user errors and can ensure the safety and reliability of the system. CPS timing varies depending on the domain and system, even if it is the same error, but the range of CPS timing errors follows the classification given. In addition, quantitative timing requirements should be developed according to the domain and system.

2.2.1 Delay

Delay is one of the major threats to accidents. In order to smoothly provide real-time services, it is necessary to comply with the preset deadline. Delay that may occur in CPS is classified into network delay, processing/processing delay, and physical delay, and each is described.

● Network Delay

It refers to a delay error that occurs in a network environment where various subsystems are wired and wirelessly connected. Typically, CPS consists of multiple servers/nodes that interact over the network. This causes network delays due to network environment errors and data transfer errors.

- Network environment errors: Delays due to network equipment errors and operational environments (e.g., bottlenecks, coexistence, network equipment anomalies, interface & protocol errors, network, etc.)
- Data transmission errors: Delay in retransmission due to data transmission errors (e.g., flow control errors, packet transmission errors, control message errors, queuing delays, etc.)

● Processing/Processing Delay

The network means that data processing inside the system is delayed while maintaining a normal state, or delays occur in the process of linking with external systems such as cloud and server-client systems.

- Internal factors: Delay due to internal causes (interrupts, model generation, etc.) of the system (e.g., Interrupt handling errors, memory management errors, calculation delays, etc.)
- External factors: Delay due to external causes (such as interaction of heterogeneous devices) of the system (e.g., Delays between heterogeneous devices, external call delays, etc.)

● Physical Delay

It refers to delays due to physical causes such as people, environments, and machinery other than computing systems.

- Human factors: Delay in decision-making by people interacting with CPS (e.g., Administrator's decision-making delay)
- Operating environment factors: Delay due to failure to optimize the system operating environment (e.g., temperature and humidity that are inappropriate for the system to operate)
- Mechanical factors: Delay due to aging of mechanical devices (e.g., failure to predict the operating time of mechanical devices)

2.2.2 Synchronization

Synchronization of various computing resources, including time shared between subsystems, should be considered. Subsystems that make up large CPS operate in their own time zones and efficiently manage limited resources to achieve the objectives of real-time services in a timely manner. Therefore, CPS timing synchronization errors are classified as time synchronization between servers/nodes, resource synchronization between processes/tasks/threads, and time synchronization between physical devices.

● Time synchronization between servers/nodes

Time synchronization between different devices is required for accurate data processing. If the time synchronization does not match, the same event can be recognized as a different event, causing problems. For time series data, you need to closely process the time and order of the data. CPS describes time synchronization between servers/nodes as important because multiple subsystems can operate in different time zones and time synchronization errors and time measurement errors are described.

- Time synchronization: Time synchronization error between two or more (homogeneous, heterogeneous, domain, etc.) servers/nodes (e.g., Time synchronization errors between homogeneous/homogeneous devices, different time domains, etc.)
- Time measurement error: Server/node self-measured time such as timestamp (e.g., Differences in time measurement methods, clock errors, timestamp errors, etc.)

● Synchronization between Processes/Tasks/Threads

Resource synchronization is required to efficiently use limited resources inside arbitrary devices. Usually, CPUs have very fast processing speed, but most of them are idle because the workload required by users is not large. Multiprogramming allows more tasks to be processed on limited resources using scheduling and so on. However, multiprogramming increases the complexity of the system, reducing its safety and reliability of the system. This section examines the risk by dividing it into resource synchronization errors and health measurement errors.

- Synchronize resources: Synchronization error for sharing limited resources (e.g., Concurrency/parallelism errors, scheduling errors, virtualization errors, contextual exchange overhead, etc.)
- State measurement errors: Error measuring the state of a resource (e.g., Execution control error, cache and memory value mismatch, etc.)

● Synchronization between physical devices

CPS controls physical devices that exist in the real world based on the results analyzed in the cyber world. It ranges from simple motor devices to robotic arms of complex structures used in manufacturing plants. Multiple robot arms in the manufacturing plant must be installed in the assembly line to operate organically. If they are not synchronized with each other, there will be great damage such as collisions. Therefore, it is necessary to measure time synchronization and accurate state so that each device can operate according to the time and order desired by the user.

- Time synchronization: Time synchronization error between two or more physical devices (such as actuators) (e.g., difference in hardware span of physical devices, aging, etc.)

- State measurement error: Physical Device Status Measurement Error (e.g., sensor error, interpretation error of control command, etc.)

3. Case Study

3.1 System Overview

The target system is a smart policing system that utilizes drones for crime prevention and resolution, and performs autonomous flight and policing missions of drones as follows. First, drones must perform autonomous flight missions safely and reliably. If a drone loses control during flight, it becomes a flying weapon, and if it crashes into a person or structure, it causes great damage. Therefore, the autonomous flight of drones is equipped with a function to recognize and analyze the surrounding environment by themselves, avoid obstacles, and respond to unexpected situations. Second, it is necessary to carry out security duties. It collects surrounding environmental information through a camera mounted on a drone, recognizes abnormal behavior, tracks suspects, or arrests them. To this end, image analysis technology using artificial intelligence is importantly used.

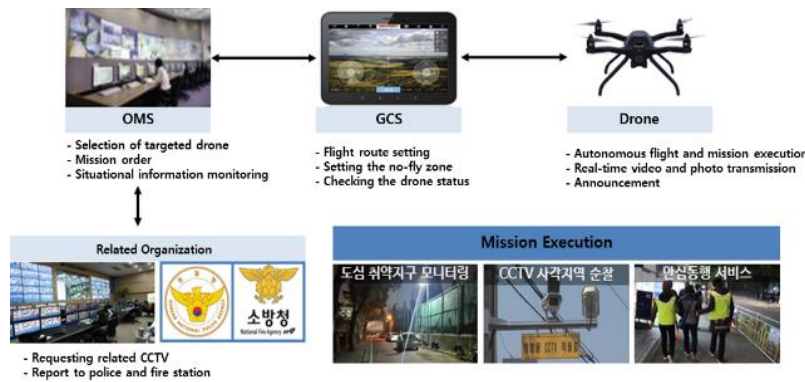


Figure 2. Smart policing system overview

As shown in Figure 2, the target system consists of operational management systems (OMS), ground control systems (GCS), drones, and associated agencies such as police and fire stations.

- **Operation Management System (OMS):** OMS selects the target (drone) necessary to perform the mission and shares various information on mission planning, weather information, and surrounding situation information in the mission area with GCS. When the drone's mission performance and preparation for dispatch are all completed, the GCS instructs the drone to perform its mission.
- **Ground Control System (GCS):** It performs tasks such as flight control, mission planning, real-time control, image processing, and storage for drones. To this end, GCS must have two functions. First, it is a function of receiving and checking the current location and state information of the drone and images photographed by the drone through a wireless communication network. Second, it is a function that can set flight control and mission control based on drone state information. The status information refers to the drone's location, altitude, speed, remaining battery capacity, etc., and shall be free to set flight paths and no-fly zones.
- **Drone:** Patrol the crime scene by flying autonomously or manually along a pre-set route. If abnormalities are found, they immediately switch to the security mission mode to track or suppress suspects. To this

end, drones include the following functions: First, the drone is equipped with a wireless transmission/reception module to check status information (position, speed, remaining battery capacity, etc.), camera image information, and drone flight instructions. In general, Wi-Fi, LTE, 5G, etc. are supported to provide a wireless communication environment. Second, drones can fly autonomously by receiving control signals or acquiring flight status information using various sensors.

- **Associated agencies:** The problem is solved by being dispatched directly through the receipt of reports such as police stations and fire stations.

The operating scenario of the target system is as follows.

- **Scenario 1: Automatic Patrol in Crime Areas**

They use drones to patrol areas where crimes are frequent or likely to occur. The operator establishes a flight plan at the GCS for automatic drone patrol. The flight plan sets the target point at which the drone intends to travel and also sets the no-fly zone to prevent the drone from entering the no-fly zone. The video data collected during the drone's automatic patrol is transmitted to the operator in real-time, and when the crime scene is found, the drone is switched to manual mode to approach the suspected crime area and conduct detailed patrol activities.

- **Scenario 2: Tracking Suspects**

The drone arrives in the crime area or mission area and collects video information. Based on this image information, if a suspect is found, the drone keeps a certain distance from the suspect and tracks him. At this time, various information (location, clothing, etc.) about the suspect is shared in the operator's monitoring system.

- **Scenario 3: Safe Accompanying for Life Safety**

It is a service in which drones fly close to each other to protect the socially disadvantaged and vulnerable, such as children, women, and the elderly. In general, drones are accompanied by women and students who return home late at night, performing tasks such as crime prevention activities, rapid reporting of crimes, and protecting victims when they find them so that they can return home safely to their destinations.

3.2 CPS Timing Analysis of Target System

This section analyzes CPS timing errors that may occur on the target system based on the CPS timing errors classified earlier. In order to secure the safety and reliability of the target system, it shall be developed and operated in full consideration of the following matters:

First, a description of the delay problem of CPS timing is provided.

1) Network Delay

- In a crowded wireless environment, various radio media are delaying drone control commands and data transmission through frequency and interference.
- Data transfer delay due to network failure between GCS and OMS
- Data transfer delay due to network failure on connected systems
- Data transfer delay due to interface and protocol (MAVLink) compatibility issues

- Delay in data transfer due to fluid flow control
- Communication connection between terminals failed (OMS-GCS, GCS-drone, OMS-linked agent)
- Loss of segmented data in drone image data transfer and reconstruction error (timestamp error)
- Suddenly, a large amount of data is received, resulting in a buffer overflow, and the drone's status information is lost.
- Low bandwidth latency and loss of information

2) Processing/Processing Delay

- Loss of control commands due to memory errors in GCS (for example, no memory returned)
- Emergency handling delays (e.g., no minimum battery remaining)
- Delay in image analysis software calculations (such as the complexity of software structures and algorithm faults)
- Drones from different manufacturers fail to collaborate and interact with drones due to different data processing speeds
- Slow processing due to sudden load on the cloud, edge systems

3) Physical Delay

- Delay in sending commands due to absence of OMS administrator or delay in judgment
- Delay due to absence of GCS pilot or late judgment
- Unexpected processing delays due to unpredictable external environmental conditions (rain/wind/obstacle) compared to simulated environments
- Processing delays due to aging and communication equipment failure
- Processing delays due to aging and failure of servers

Next, a description of the synchronization problem of CPS timing is provided.

1) Server-to-node synchronization

- Time synchronization error due to clock errors built into drone and GCS respectively

2) Synchronize between processes/tasks/threads

- OMS and GCS scheduling errors

3) Synchronize between physical devices

- Time synchronization between multiple drones fails to perform incorrect behavior
- The drone and server failed to synchronize the time. The drone does not work at the appointed time.
- Error measuring status information such as drone position, altitude, remaining battery capacity, etc.

4. Conclusion

Understanding time constraints are paramount as CPS' demand for real-time services grows. Since CPS controls physical devices in the direction of analyzing and optimizing physical phenomena that frequently change in real-time, various time constraints occur and appropriate responses are essential. In particular, as the size and complexity of the system grow, the local timing problem can be extended across the system, and it is difficult to find later and the cost of solving the problem is significant without considering the timing problem from the initial stage. Therefore, it is necessary to consider timing problems from the initial stage of system development.

In this paper, we describe the CPS timing problem by classifying CPS timing errors into delay and synchronization. Timeliness must be guaranteed to provide real-time services. Delay and synchronization can be said to be important factors in securing timeliness. Delays are determined by compliance with deadlines, and synchronization supports timely results through time synchronization and resource synchronization. Research on these CPS timing errors helps ensure the safety and reliability of the system and enables sufficient review and countermeasures to prevent safety accidents.

As a future challenge, CPS timing errors described herein should be databased with many use cases. Stakeholders studying CPS can utilize this data as needed and expect it to contribute to ensuring the safety and reliability of CPS.

References

- [1] J. Shi, J. Wan, H. Yan, H. Suo, "A survey of Cyber-Physical Systems", 2011 International Conference on Wireless Communications and Signal Processing (WCSP), Dec. 2011
DOI: 10.1109/WCSP.2011.6096958
- [2] A. V. Jha, B. Appasani, A. N. Ghazali, P. Pattanayak, D. S. Gurjar, E. Kabalci, D. K. Mohanta, "Smart grid cyber-physical systems: communication technologies, standards and challenges", Wireless Networks, 27, Mar. 2021
DOI: <https://doi.org/10.1007/s11276-021-02579-1>
- [3] W. Doghri, A. Saddoud, L. C. Fourati, "Cyber-physical systems for structural health monitoring: sensing technologies and intelligent computing", The Journal of Supercomputing, Jun. 2021
DOI: <https://doi.org/10.1007/s11227-021-03875-5>
- [4] V. A. Banks, K. L. Plant, N. A. Stanton, "Driver error or designer error: Using the Perceptual Cycle Model to explore the circumstances surrounding the fatal Tesla crash on 7th May 2016", Safety Science, Vol. 108, Oct. 2018
DOI: <https://doi.org/10.1016/j.ssci.2017.12.023>
- [5] G. Volkan, P. Steffen, G. Tony, V. Frank, "A Survey on Concepts, Applications, and Challenges in Cyber-Physical Systems", KSII Transactions on Internet and Information Systems (TIIS), Vol. 8, Issue 12, 2014
DOI:10.3837/tiis.2014.12.001
- [6] Edward A. Lee, "Cyber Physical Systems: Design Challenges", Proceedings of the 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), May. 2008
DOI: 10.1109/ISORC.2008.25
- [7] J. C. Eidson, E. A. Lee, S. Matic, S. A. Seshia, and J. Zou, "Distributed Real-Time Software for Cyber-Physical Systems", Proceedings of the IEEE, Vol. 100, Issue 1, Jan. 2012
DOI: 10.1109/JPROC.2011.2161237
- [8] A. Shrivastava, P. Derler, Y. L. Baboud, K. Stanton, M. Khayatian, H. A. Andrade, M. Weiss, J. Eidson, S. Chandhoke, "Time in cyber-physical systems", Proceedings of the 11th IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis, No. 4, pp. 1-10, Oct. 2016
DOI:10.1145/2968456.2974012