УДК 681.5.01:69.057.3.

Formal Verification of Sino-Russian Regulatory Configuration Switching in an APCS for High-Formwork Monitoring

Pogodaev A.K.[1], Sun C.[1], Yao S.[2], Liu T.[1]
1 Lipetsk State Technical University
Lipetsk, Russian Federation
2 Shenyang University of Chemical Technology
Shenyang, China

Digital construction monitoring links sensors, data processing, configuration records, and supervisory decisions in an automated process control system (APCS). For temporary structures, monitoring values and control logic must remain traceable to the configuration under which they are interpreted [1]. In an international project, this traceability also covers the regulatory and project basis of engineering limits: a numerically valid value may be applied incorrectly if its units, document version, applicability domain, or approval record belong to another configuration.

This study considers a high-formwork monitoring APCS that may operate under Chinese or Russian project/regulatory branches. The branches may reference, for example, GB 55023-2022 and GOST 27751-2014 [2, 3]. The purpose is not to compare which national system is safer and not to establish equivalence between standards. Instead, each branch is treated as a versioned digital configuration object. This follows configuration-management principles of identification, change control, status accounting, and audit [4]. The research object is therefore the supervisory configuration-control algorithm of the APCS rather than the structural calculation of the formwork.

The model contains four software states: CN_ACTIVE, RU_ACTIVE, PROFILE_REVIEW, and CONFIGURATION_HOLD. The first two denote released Chinese and Russian project profiles; PROFILE_REVIEW holds a requested candidate before authorization; CONFIGURATION_HOLD blocks interpretation when configuration integrity is insufficient. Every evaluation receives a requested branch and five binary flags describing configuration-identity validity, comparability of the engineering quantity and units, project approval, candidate-profile release authorization, and an independent adverse-physical-condition signal. The release flag

is evaluated only in PROFILE_REVIEW. After a profile is released, its continued validity is represented by the identity, applicability, and approval flags. Two requested branches and five binary flags give 64 input combinations for each source state.

The transition logic is deterministic. If identity, comparability, or approval is invalid, the next state is CONFIGURATION_HOLD. After integrity is restored, the hold state can move only to PROFILE_REVIEW. A candidate profile can become active from PROFILE_REVIEW only when all release conditions are valid. A request to change directly from CN_ACTIVE to RU_ACTIVE, or in the opposite direction, first enters PROFILE_REVIEW. The independent physical signal passes through unchanged in every state. Thus, a regulatory or configuration problem cannot suppress adverse physical evidence. This separation is compatible with supervisory-control formulations that distinguish controllable and uncontrollable events [5].

Five invariants were checked over the complete state-input space: I1, every incomplete configuration enters CONFIGURATION_HOLD; I2, direct CN_ACTIVE-to-RU_ACTIVE and RU_ACTIVE-to-CN_ACTIVE switching is prohibited; I3, release from PROFILE_REVIEW requires all release conditions; I4, the independent physical output always equals the incoming physical flag; I5, every evaluation generates exactly one audit record containing the source state, requested branch, integrity flags, release decision, physical flag, target state, and reason code. Complete enumeration covers four states and 64 inputs, giving 256 evaluations. Of these, 224 enter CONFIGURATION_HOLD, 20 result in PROFILE_REVIEW, six in CN_ACTIVE, and six in RU_ACTIVE. All 128 cases with an adverse physical signal retain that signal, and no violation of I1-I5 was found.

The zero-violation result establishes conformance of the declared finite-state logic to its own invariants; it is not a statistical reliability estimate, and the 256 evaluations are not construction-site observations. The engineering implication is that Sino-Russian regulatory switching should be implemented as a controlled configuration release rather than by immediate replacement of isolated thresholds. Routing a branch change through PROFILE_REVIEW prevents a mixed-version configuration from being treated as operationally released, while a missing approval or

mismatched identifier remains an information-integrity condition rather than a fictitious physical warning. The contribution is the separation of cross-national regulatory-profile switching from physical risk evaluation and the exhaustive verification of configuration-integrity invariants over the complete declared finite input space. The study remains limited to the software abstraction and requires project-specific mapping review and implementation testing before deployment.

References

1. Yuan X., Anumba C.J., Parfitt M.K. *Cyber-physical systems for temporary structure monitoring* / X. Yuan, C.J. Anumba, M.K. Parfitt // Automation in Construction. - 2016. - Vol. 66. - P. 1-14. - DOI: 10.1016/j.autcon.2016.02.005.
2. GB 55023-2022. General code for scaffold in construction. - Beijing: Ministry of Housing and Urban-Rural Development of the People's Republic of China, 2022.
3. GOST 27751-2014. Reliability for constructions and foundations. General principles. - Moscow: Standartinform, 2015.
4. ISO 10007:2017. Quality management - Guidelines for configuration management. - Geneva: International Organization for Standardization, 2017.
5. Ramadge P.J.G., Wonham W.M. *Supervisory control of a class of discrete event processes* / P.J.G. Ramadge, W.M. Wonham // SIAM Journal on Control and Optimization. - 1987. - Vol. 25, No. 1. - P. 206-230. - DOI: 10.1137/0325013.