Résumé Cette étude porte sur la *conception sûre* de systèmes automatisés de production (SAP). Nous nous focalisons principalement sur un sous ensemble temps réel des SAP : ceux où les contraintes temporelles doivent être strictement respectées et où le contrôle est prédominant. Notre approche repose sur des modèles synchrones : le modèle *synchrone fort* des langages ESTEREL, LUSTRE ou SIGNAL et le modèle *synchrone faible* (retard unité pour la communication). Cette dichotomie synchrone fort/synchrone faible, intimement liée aux notions de communications locales/distantes, assure un comportement déterministe au système réparti tant d'un point de vue logique que temporel. Cette approche introduit un biais dans le comportement en regard de son équivalent centralisé. Cependant, nous donnons un sens à ce type de comportement en introduisant une nouvelle notion d'équivalence. La *validation a priori de contraintes temporelles* est un des objectifs de notre étude. Cette validation est rendue possible par l'approche synchrone, s'appuyant sur un temps global (horloges synchronisées). La vérification des contraintes repose sur la technique des « observateurs ». Les modèles sous-jacents permettent d'établir une correspondance simple entre temps physique et temps logique. Nous avons développé la plate-forme R-PORTS (Rapid Prototyping Of Real-Time Systems) chargée d'automatiser la répartition du contrôle d'un SAP sur une architecture cible donnée, communiquant via réseaux de terrain industriels. Dans nos travaux, R-PORTS est dédiée aux réseaux CAN/VAN. Une couche *Middleware* a été développée afin de donner le caractère synchrone à ces bus. Cette couche d'interface entre le processus d'application et le profil de communication intègre également des politiques de tolérance aux pannes. Le concept de *sensibilité booléenne* que nous introduisons permet de caractériser l'impact d'un signal d'entrée erroné sur l'évolution du système.

Mots-clés : synchrone fort/faible, réseaux de terrain industriels, synchronisation d'horloges, validation.

Abstract We study safe design of automated production systems (APS). More specifically, we focus on a subset of APS : those with strict temporal constraints and where control is predominant. Our approach relies on synchronous models. We use both the strong synchronous model of the ESTEREL, LUSTRE and SIGNAL languages, and the weak synchronous model, where communications take a unit delay. We use the strong synchronous model for local communications and the weak synchronous one for distant communications. Such a distinction guarantees deterministic behaviour for the distributed system, from a logical perspective as well as from a temporal one. This approach introduces a bias between the resulting behavior and its centralised equivalent. However, we formalize this kind of behaviour by introducing a new equivalence relation. A priori validation of temporal constraints is one of our goals. Such validation is possible within the synchronous framework because of its global time view (synchronized clocks). For properties checking, we use the verification by observer technique. Underlying models allow us to construct a simple correspondence between logical time and physical time. We have developed the R-PORTS platform – Rapid Prototyping Of Real-Time Systems –, for automating the distribution of APS control onto fieldbus target architectures. In this work, R-PORTS is dedicated to CAN/VAN buses. A Middleware layer was developed to provide these buses with a synchronous interface. This interface between the application process and the communication profile also integrates fault-tolerant policies. We introduce the concept of boolean sensitivity to characterise the influence of erroneous signal input onto system evolution.

Keywords : strong/weak synchronous, fieldbus, clock synchronization, validation.