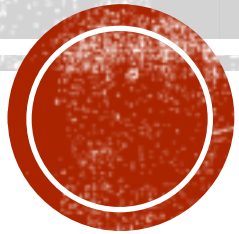
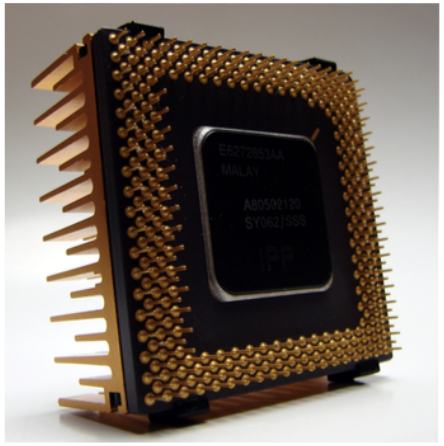
SOFTWARE MODEL CHECKING

Sylvain Conchon, Sébastien Bardin, Fatiha Zaïdi

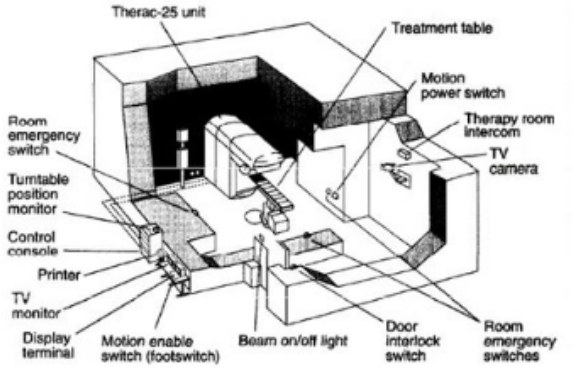


CONTEXTE

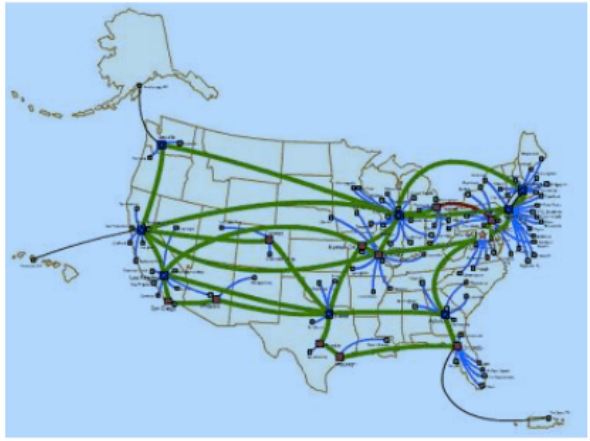
Des bugs célèbres ont mis en lumière le besoin de vérifier la correction des logiciels



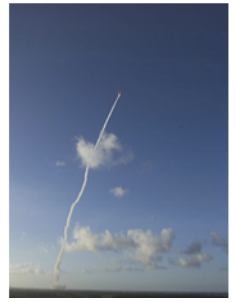
Bug Pentium FDIV 1994



Radiation Therac 1985-87



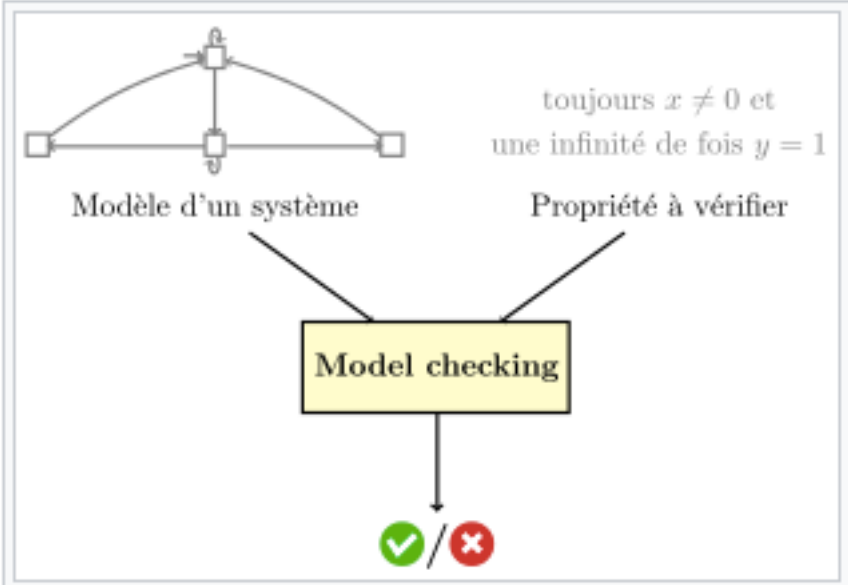
AT&T Interruption du réseau 1990



Crash d'Ariane 5 1996

QU'EST-CE QUE VERIFIER UN LOGICIEL?

- La Vérification consiste à vérifier si le modèle d'un système satisfait une propriété
- Elle permet de vérifier différents types de propriétés : l'absence de blocage, propriétés de Safety, Liveness, les problèmes liés aux accès concurrents, etc.
- La vérification doit être faite tôt dans le cycle de développement d'un logiciel
- La vérification est une technique outillée (disponibilité de model checkers)
- Technique utilisée dans l'industrie car très utile pour des systèmes ayant beaucoup d'interactions



BUT : Découvrir les erreurs de conception en phase amont de développement du logiciel

CONTENU DU COURS

- Introduction au Model Checking (1 cours)
- Techniques de Model Checking basées sur des algorithmes d'accessibilité et des propriétés exprimées en logiques temporelles (3 séances – 1 séance TP avec SPIN)
- Model checking paramétré – prouver une propriété de Safety pour un nombre quelconque de processus (3 séances – utilisation de l'outil CUBICLE)

- MCC : 2 TP notés.