



**Katedra  
Inżynierii  
Oprogramowania**

Wydział Elektroniki,  
Telekomunikacji i Informatyki  
Politechnika Gdańska  
ul. Narutowicza 11/12  
80-952 Gdańsk  
tel/fax (058) 3472727

## SEMINARIUM

**Katedry Inżynierii Oprogramowania  
Wtorek, 13 czerwca 2006 r, godz 15:00 sala 633 WETI**

### ***Zastosowanie dynamicznej oceny sytuacji w zapewnieniu bezpieczeństwa pojazdów autonomicznych***

dr. inż. Andrzej Wardziński  
PROKOM Software SA

Zapewnienie bezpieczeństwa dla systemów krytycznych odbywa się zwykle poprzez utworzenie dowodu bezpieczeństwa (*safety case*), w którym poprzez analizę konstrukcji systemu oraz trybów awarii elementów (*failure modes*) określone jest prawdopodobieństwo wystąpienia hazardu (niebezpiecznego wydarzenia). Podejście to bazuje na założeniu, że przyczynami hazardów są awarie elementów oraz kombinacje zdarzeń. Systemy mobilne działające w otwartym środowisku są tu przypadkiem szczególnym, w którym do hazardu może doprowadzić niewłaściwa interakcja z innymi pojazdami lub obiektami, przy czym interakcja ta ma charakter dynamiczny i zmienny.

Podczas prezentacji zostaną omówione zagadnienia architektury systemu sterującego pojazdu autonomicznego istotne w kontekście zapewnienia bezpieczeństwa. Podstawowym elementem jest tutaj wiedza o aktualnej sytuacji (*situation awareness*), będąca podstawą do planowania działania pojazdu. Scenariusze działania są oceniane pod kątem zgodności z misją, spełnienia reguł oraz poziomu bezpieczeństwa. Analiza scenariuszy awarii pokazuje, że istotnymi elementami mającymi wpływ na bezpieczeństwo są również niepewność i niekompletność informacji oraz zaufanie do źródeł informacji oraz innych pojazdów występujących w otoczeniu. Zaproponowany został formalny model obejmujący wiedzę o sytuacji oraz pojęcia niepewności i zaufania. Omówione zostaną wyniki analizy bezpieczeństwa oraz podejście do konstrukcji systemu zapewniającej bezpieczeństwo.