Agent Build System

Version 1.5.1

Commit:	https://github.com/aleonal/ABS.git
Language:	Python 3.8
Libraries:	PyQt5 PyInstaller PyAutogui
OS:	Linux Windows

The Agent Build System software is a tool designed to generate an agent template that can be modified through a graphical user interface.

The main goal of this system is to create the following: a script or set of runnable scripts that can reproduce captured user actions based on stimulus from various sources; and a packaged file that contains virtual machines and project files that can be transferred, imported, and executed on other computers.

The system consists of four modular components:

- Causation Extractor
- Runner
- Builder
- Packager

Causation Extractor

The Causation Extractor is responsible for:

■Extracting potential causal relationships (observations that lead to user actions), within data captured using the ECELd-netsys tool.

■ Saving the data into a JSON file that will be loaded into the Builder component.

Data collected: System calls
Network traffic
Keystrokes
Timed screenshots (at a given time interval)
Mouse clicks (collected on each click)

Builder

The Builder provides a graphical representation of the causal relationships produced by the CE. This allows the user to view and modify causal dependencies.

This module allows the user to:

- Manually select relationships and create a dependency list.
- Specify dependencies from a sequence of observations to a user action.
- Specify the dependency values.
- Search values in user input.
- Generate an executable script that will be used by the Runner.

Runner

The Runner is responsible for:

- Coordinating the processes for data collection and Builder output script.

- Reproducing the user actions based on system observations.

- Loading and running the script.

- Stopping the script at any given time.

Packager

The Packager is responsible for:

- ■ Allowing the user to export and import all elements that are part of the Agent Build System project including:
  - ✓ VMs
  - ✓ Scripts
  - ✓ Other files

- ■ Working with VirtualBox.