

Информационные технологии. Лекция 12. Функциональная безопасность

Студент группы 2305 Макурин Александр

22 мая 2023

Виды проблем (сбоев) в ИБ:

- сбой
- отказ
- нарушение

Места сбоев:

- органы управления
- датчики
- переход от СУ к ОУ

Здесь должна быть картинка

$S^{t+1} = S^t + U^*$, где U^* — реально полученное управляющее воздействие.

$U^* = f(K_P P + K_V V) + U$. $K_{P,V}$ — передаточные коэффициенты. U — то, что хотим сделать (запланированное воздействие). P — погрешность анализа. V — «словарь», обычно неизменный (const). $f(\dots)$ — поправки.

Проблема — в данной формуле не заложена возможность сбоя.

На примере датчиков:

- $\bar{P} = AP$ — сбой. A — случайный ряд.
- $\bar{P} = \text{const}$ — отказ.
- $\bar{P} = AP + l$ — нарушение. l — смещение.

Здесь должна быть картинка

$U^* = G(K_P P + K_V V) + U$

$G = \begin{cases} I \\ \text{diag}(0_i) \end{cases}$ — если элемент функционирует неверно, то соответствующий элементы диагональной матрицы равен 0.

Когда элемент j вышел из строя, его состояние неизвестно и требуется вносить поправку в управляющее воздействие с учётом этого: $\bar{U} = U^* + \Delta U_j$.

Порядок действий при взаимодействии с отказом (сбоем/отказом/нарушением):

1. Обнаружить отказ и зафиксировать время обнаружения и предыдущее состояние системы ($t_{\text{обн}}$ и $U_{t_{\text{обн}}-1}$).
2. Локализовать отказавший элемент j .
3. Противодействовать отказу компенсацией управляющего воздействия $\Delta U_j = U_{t_{\text{обн}}} - U_{t_0}$.

Здесь должна быть картинка

$|\{j\}| > |\{\bar{j}\}|$

τ — разница между тем, что должно было быть и тем, что есть.

$S^{t_0} = S^{t_0-1} + K_P^{\text{Камер}} P_{\text{Камер}} + K_P^{\text{Сенсоров}} P_{\text{Сенсоров}} + K_V V + U$

$S^{t_1-\delta} = S^{t_0} + K_P^{\pi} P_U + U$

$S^{t-1} = S^{t_0} + K_P^{\pi} P_U + K_P^{\text{Сенсоров}} P_{\text{Сенсоров}} + U$

$K_r = \frac{\delta U(t_0, t_1, \frac{\delta U(t_0)}{\delta U_j})}{\delta U_j} \cdot \frac{\delta U(t_0)}{\delta U_j}$ — коэффициент чувствительности (чем он выше, тем важнее датчик).

$U(t_0, t_1, \Delta U) = K_r \cdot \Delta U_j(t_\alpha)$. $\Delta U = \begin{cases} 0 & \text{— сенсор был не нужен} \\ \alpha & \text{— сенсор был нужен} \end{cases}$ — коррекция.

Если на участке времени сенсор был не нужен, то его можно не корректировать на этом участке.

1. $t_{\text{поиска}} |\text{Гипотеза}| = |\{j\}|$ – строим графики гипотез для $U_{\text{реал}_j}$.

2.1. $\tau_\alpha = \arg \min \phi_j(\tau)$

$$\phi = \arccos \frac{\Delta U \frac{\delta U}{\delta U_j}}{\|\Delta U\| \left\| \frac{\delta U}{\delta U_j} \right\|}$$

$\phi_j(\tau) \leq \overline{\phi_j}$ – порог, который мы назначим

2. $j^* = \arg \min \phi(\tau_j)$

$$\Delta U_j = \frac{\delta U}{\delta U_j} \cdot \Delta U$$

Здесь должна быть картинка

Тоже самое повторяем для K_P , K_V и P .