付録 1. 研究員らの組織で取り組んでいる品質向上に向けた活動の取り組み状況

活動 1：チェックリスト作成

IPA「組込みソフトウェア向け設計ガイド ESDR」元に，設計上必須となる部分と，過去の不具合事例を含めてチェックリスト化している．

〈課題〉

・項目数が多く，[システム・装置仕様編]と[設計編]で合わせると 80 項目以上ある．仮に 1 項目 3 分で考えるにしても 4 時間かかり労力がいる．

・[はい，いいえ，対象外]の判断基準が明確でないため，熟練者でないと上記の時間でチェックをしていくことは難しい．

・設計者側のセルフチェックの意味合いが濃く，レビューの場でリストのチェック内容を一つ一つ確認することはない．

活動 2：不具合管理票の作成

開発で発生した不具合について，[不具合を作り込んだ工程，内容と原因，今回の対応，恒久対策]を帳票に記入して残す．

〈課題〉

・開発中はレビューの場でその時点での関係者には水平展開されるが，その開発が終了してしまうとその後に積極的に見られることはほぼない．
（チェックリスト見直し時に必要に応じてチェック項目に含めるが，管理表 No との紐づけまではできていない）

・管理表の記録の残し方の粒度も作成者に依存してしまうため，必要最低限の情報のみ記述されているような場合，熟練者とそうでない場合で不具合に対しての理解度の差が大きくなってしまう．
（修正とリリースに追われて，ドキュメントは後回しになりがちな背景もある）

活動 3：QuickDR における DRBFM（Design Review Based on Failure Mode）シートの活用

設計変更内容をレビューで分かりやすく示すために DRBFM シートを活用している．

〈課題〉

・説明者側のためのシートの意味合いが濃く，レビューア側も変更内容が理解しやすく易くはなってはいるが，不具合に気付けるかは結局レビューアのスキルに依存する．

・帳票がハードウェア開発向けのため，ソフトウェアで使う場合，無理矢理帳票に合わせて書かれているため表現が難しい．

活動 4：不具合事例発表会の開催

全社内で発生した不具合事例について定期的に発表会を開催し，情報を共有している．

〈課題〉

・業種的に，機械設計やハードウェア設計関連の発表が多く，ソフトウェアの発表の割合は少ない．（元々外注で対応する場合が多いこともある）

・不具合の改修コストも示されるため，影響をリアルに感じられるはあるが，全社で行う分，出席人数が役職者等に限られてしまい，情報が若手まで伝わりにくい．

付録 2. 勘所集

◆組み込み系ソフトウェア 1(通信機器)

トリガーポイント	サブワード	過去の不具合事例	参照先 (年度, 製品, 不具合管理No.)	影響 (発覚した工程, 改修に要した工数)	指摘観点 (レビューポイント)
外部I/F (通信)	-	・対向機器との送受信タイミングのズレにより, データの欠損が発生	20xx, OOO, DOC*****	リリース後, ○○H	・接続先の機器との送受信タイミングが考慮されているか ・リトライの処理を入れているか
	-	・受信処理前にバッファクリアが行われておらず, ゴミが入った状態で受信してしまう	20xx, OOO, DOC*****	リリース後, ○○H	・受信前にバッファクリアが行われているか ・バッファオーバーフローの対策はされているか
	-	・ポーリング処理で無応答が継続する条件があり, 処理がフリーズ	20xx, OOO, DOC*****	結合試験, ○○H	・ポーリングの場合, 無応答で待機状態のままを回避しているか
	RS232C	・対向機器側とフロー制御のタイミングが合わず, 電文が正常に送れない	20xx, OOO, DOC*****	結合試験, ○○H	・フロー制御は実装しているか
	RS485	・電文データサイズが大きい場合に, 送信終了前に受信切り替えタイミングが来てしまい, 電文データが欠損	20xx, OOO, DOC*****	詳細設計, ○○H	・送受信の切り替えタイミングが全ての送受信処理を考慮しているか
	シリアル通信	・データビットサイズを変更した際に, 最上位bitをマスクしておらず, データが文字化け	20xx, OOO, DOC*****	リリース後, ○○H	・通信仕様変更時のビット読出し状態について考慮しているか
	コマンド・電文	・区切りフォーマットが, 対向機器側と協調がとれておらず, 結合試験で通信失敗	20xx, OOO, DOC*****	結合試験, ○○H	・通信仕様変更時のビット読出し状態について考慮しているか
	設定変更	・装置の接続数が最大の設定の時, 一括操作で正常動作とならないタイミングがあった	20xx, OOO, DOC*****	結合試験, ○○H	・最大数の設定での動作確認できているか
割込み	-	・割込み禁止処理をせずに, タスクとドライバで同時に同じデータにアクセスしてしまい, 状態不一致が発生	20xx, OOO, DOC*****	結合試験, ○○H	・データ更新を行う場合, 他の処理からのデータ参照, コピーのタイミングを同じデータに対して同時アクセスが可能な場合は, 割込み禁止・許可を行う
	-	・割込み禁止後の許可の処理が行われないパターンがあり, 装置がフリーズ→自己リセット	20xx, OOO, DOC*****	結合試験, ○○H	・割込み禁止後に許可されない状態が継続しないか
リセット	-	・リセットの種類によってリセット後の値がレジスタにより異なる	20xx, OOO, DOC*****	詳細設計, ○○H	・レジスタによっては, リセット(ハード/ソフト)の種類が異なると初期化されるものとされないものがあるので注意する
	ソフトリセット	・リセットレジスタを操作する前にプロテクトビットを操作する必要がある場合があるが, リセットレジスタのみを操作しておりリセットがかからない	20xx, OOO, DOC*****	詳細設計, ○○H	・リセット実行時の手順について, ユーザーズマニュアル等で確認したか メーカに対して, 検討した処理手順で問題ないことを確認しておくとよい
メモリ	-	・メモリのアクセスに時間が長く, 連続処理失敗や異常監視リセットが発生した	20xx, OOO, DOC*****	結合試験, ○○H	・異常監視を行っている場合, アクセス時間が監視時間を超えることはないか ・監視時間の設計で, ハードウェアとの兼ね合いで最大値にできない場合は試験等で担保が取れているか
	-	・プログラムデータと記録データの領域をメモリ内に共通で確保している場合, 記録処理による書込み頻度が多く, メモリの書き換えの最大回数に到達した	20xx, OOO, DOC*****	詳細設計, ○○H	・メモリアクセスの頻度が制限回数を超えないようにする (正常系のログを記録する場合などは注意)
	-	・メモリ書込み処理中に停電またはリセットが発生すると, 以降復帰しなくなった	20xx, OOO, DOC*****	結合試験, ○○H	・フラッシュアクセス時と他の処理が重複した場合に双方の処理に影響がないか ・書込み/読出しの途中で停電またはリセットが発生した場合の挙動は考慮されているか
	-	・類似装置のロジックをそのまま適用したことでメモリクリア処理のサイズ誤りに気がつかずに, 意図しないメモリ領域の情報までクリアしてしまった	20xx, OOO, DOC*****	リリース後, ○○H	・スタック, ヒープ用の領域と重複しないか ・流用したソフトがある場合, メモリサイズの確認はできているか
	-	・元の保存データが読み出された時に, 改修後のソフト動作が異常	20xx, OOO, DOC*****	結合試験, ○○H	・変更前のバージョンで外部メモリに書込まれたデータを読出しても異常にならないか
	外部メモリ (EEPROM)	・I2Cアクセス中にリセットが発生すると, 以後EEPROMにアクセスできなくなった	20xx, OOO, DOC*****	リリース後, ○○H	・I2C通信フリーズを考慮してリセットシーケンス処理を入れているか
タイマ	-	・無応答や異常を監視するタイマの場合, 正常応答後のタイマ停止が抜けて, 待ち状態ではない時にタイムアウトイベントが発生	20xx, OOO, DOC*****	結合試験, ○○H	・応答待ちで使用する場合に, タイムアウトと応答のタイミングでどちらが先になっても正常に動作するか
カレンダー	-	・うるう年, うるう秒による動作異常の発生	20xx, OOO, DOC*****	結合試験, ○○H	・カレンダー情報に応じて特定の処理を行う場合に, うるう年, うるう秒の場合に異常にならないように考慮されているか

◆組み込み系ソフトウェア２（制御機器）

トリガーポイント	サブワード	過去の不具合事例	参照先（年度，製品，不具合管理No）	影響（発覚した工程，改修に要した工数）	指摘観点（レビューポイント）
外部I/F（制御）	-	・ノイズを入力イベントと誤検知して，制御を行ってしまう	20xx，〇〇〇，DOC*****	リリース後，〇〇H	・接点入力の場合，チャタリングがあることを考慮した設計になっているか
	-	・制御時間が短く，受け側が認識できない	20xx，〇〇〇，DOC*****	リリース後，〇〇H	・最短制御時間を確認しているか
	入力・操作	・電流の入力で，0mAの時の値と，最大の時の値が共に同じ値（FFFFh）となり，表示エラーとなる 入力が未接続の場合も同様	20xx，〇〇〇，DOC*****	結合試験，〇〇H	・入力範囲の最大時，最小時の値を考慮した設計になっているか ・外部I/Fが未接続時の値を考慮しているか
		・A/D入力において最大値7FFFhをオーバーする演算（16bitADデータに補正をかける場合）があると，演算結果が逆符号となる	20xx，〇〇〇，DOC*****	結合試験，〇〇H	・演算最大値を考慮しているか
		・操作結果のチェック処理で，リレーの挙動によっては期待値と不整合が起きるタイミングがあり，異常を検出	20xx，〇〇〇，DOC*****	結合試験，〇〇H	・ソフトのチェック処理の内容とハードウェア（リレーの挙動）の関係を確認しているか
		・機種設定の組合せパターンによって，A/D変換の乗率を求めていたが組合せによって，計測値がオーバーフロー(スケールオーバー)	20xx，〇〇〇，DOC*****	結合試験，〇〇H	・最大値の設定での動作確認できているか
	出力・表示	・動作回数が，リレーの寿命回数をオーバーし，機器故障が発生	20xx，〇〇〇，DOC*****	リリース後，〇〇H	・ハードウェアによっては，制御回数の寿命を確認し，制限する設計をしているか
		・液晶表示において常時通電（バックライト，液晶表示）し寿命が低下	20xx，〇〇〇，DOC*****	リリース後，〇〇H	・自動消灯機能をつけているか
外部I/F（通信）	-	・対向機器との送受信タイミングのズレにより，データの欠損が発生	20xx，〇〇〇，DOC*****	リリース後，〇〇H	・接続先の機器との送受信タイミングが考慮されているか ・リトライの処理を入れているか
	-	・受信処理前にバッファクリアが行われておらず，ゴミが入った状態で受信してしまう	20xx，〇〇〇，DOC*****	リリース後，〇〇H	・受信前にバッファクリアが行われているか ・バッファオーバーフローの対策はされているか
	RS232C	・対向機器側とフロー制御のタイミングが合わず，電文が正常に送れない	20xx，〇〇〇，DOC*****	結合試験，〇〇H	・フロー制御は実装しているか
	コマンド・電文	・区切りフォーマットが，対向機器側と協調がとれておらず，結合試験で通信失敗	20xx，〇〇〇，DOC*****	結合試験，〇〇H	・通信仕様変更時のビット読出し状態について考慮しているか
	設定変更	・デフォルト値を元に除算を行ってパラメータ設定をする処理で，値を変更したことによって，結果が割り切れない値となり，誤差が発生	20xx，〇〇〇，DOC*****	結合試験，〇〇H	・デフォルト値を元に内部で演算処理を行っている場合，誤差を考慮しているか
割込み	-	・定周期の割込み処理（A/D割込み）で動作するプログラムで，割込み時の処理を増やした結果，シリアル通信の割込み処理が実行されないタイミングがあり，データが欠落	20xx，〇〇〇，DOC*****	結合試験，〇〇H	・割込み処理の処理時間と通信ボーレートの関係を確認しているか ・割込み処理が入るにより，メイン処理の動作が停止することへの影響を考慮しているか
	-	・割込み禁止処理をせずに，タスクとドライバで同時に同じデータにアクセスしてしまい，状態不一致が発生	20xx，〇〇〇，DOC*****	結合試験，〇〇H	・データ更新を行う場合，他の処理からのデータ参照，コピーのタイミングを同じデータに対して同時アクセスが可能な場合は，割込み禁止-許可を行う
リセット	-	・リセットの種類によってリセット後の値がレジスタにより異なる	20xx，〇〇〇，DOC*****	詳細設計，〇〇H	・レジスタによっては，リセット（ハード/ソフト）の種類が異なると初期化されるものとされないものがあるので注意する
メモリ	-	・メモリ書込み処理中に停電またはリセットが発生すると，以降復帰しなくなった	20xx，〇〇〇，DOC*****	結合試験，〇〇H	・フラッシュアクセス時と他の処理が重複した場合に双方の処理に影響がないか ・書込み/読出しの途中で停電またはリセットが発生した場合の挙動は考慮されているか
	外部メモリ（フラッシュ）	・書き換え中の排他処理に不備があり，他処理から書き込みが発生して書き込みデータが破損した	20xx，〇〇〇，DOC*****	結合試験，〇〇H	・フラッシュメモリ領域アクセス時の排他制御を確認しているか ・ガーベジコレクションの発生しにくい設計としたか （OS起動時に大量のファイルを削除している，頻繁にフラッシュへログを記録している場合は注意が必要）
タイマ	-	・タイマのクロック誤差が最大となると処理異常となる	20xx，〇〇〇，DOC*****	結合試験，〇〇H	・タイマの誤差精度は考慮しているか（最悪値で動作しても他の処理に影響しないこと）

トリガーポイント	サブワード	過去の不具合事例	参照先（年度、製品、不具合管理No）	影響（発覚した工程、改修に要した工数・金額）	指摘観点（レビューポイント）
画面	画面デザイン（統一）	－	20xx，○○○，DOC*****	詳細設計，2人日	他画面とのデザインを統一する。 ・開始位置、文字間、文字サイズ
	画面デザイン（表）	－	20xx，○○○，DOC*****	詳細設計，0．5人日	表の接線が未接続・突出がないこと。
		－	20xx，○○○，DOC*****	詳細設計，0．5人日	【表題】枠の左右中央に項目があるか
		－	20xx，○○○，DOC*****	詳細設計，0．5人日	【表題以外】枠の左右中央に項目があるか
	タブ順	－	20xx，○○○，DOC*****	納品後，0．5人日	入力しない項目からのタブ順を考慮しているか
帳票	桁数	－	20xx，○○○，DOC*****	テスト実施，0．1人日	最大桁数で値が重なるが、問題ない旨チェックリストに記載する。 （顧客了承しているため）
共通	変数・定数	－	20xx，○○○，DOC*****	コーディング，0．5人日	変数の先頭文字は小文字にする。 定数の先頭文字は大文字にする。
	コメント	－	20xx，○○○，DOC*****	コーディング，0．5人日	他画面とのコメントを統一する。 ・開始位置、記載内容、空白
	コーディング	－	20xx，○○○，DOC*****	コーディング，2．0人日	他画面とのコーディングを統一する。 ・開始位置、記載内容、空白

付録 3. 勘所集をマインドマップ化した例

勘所集の共有に当たり，マインドマップは表と比較して構造的に全体を把握しやすいというメリットがあるため，参考までに付録 2 のエンタープライズ系ソフトウェアをマインドマップ化した例を示す.